Federal Voting Assistance Program (FVAP) Technology Projects

FVAP.GOV
FEDERAL VOTING ASSISTANCE PROGRAM

Recommendations for the UOCAVA Pilot Program Testing Requirements (UPPTR)

Prepared For:
Federal Voting Assistance Program
Department of Defense
4800 Mark Center Drive
Mailbox 10
Alexandria, VA 22350-5000

Prepared By:
CALIBRE
6354 Walker Lane, Suite 300
Metro Park
Alexandria, Virginia 22310-3252
www.calibresys.com

Contract No.:
GS-35F-5833H

[redacted]

RECOMMENDATIONS FOR THE UOCAVA PILOT PROGRAM TESTING REQUIREMENTS (UPPTR)

CONTRACT # GS-35F-5833H
Task # 2.4.3
Final Report
Version # 1
02 November 2012

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 (collectively known as the UOCAVA population) during the voting process. The MOVE Act mandated that the U.S. Election Assistance Commission (EAC) and the National Institute of Standards and Technology (NIST) provide FVAP with best practices or standards to support the pilot programs.

The EAC published the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) UOCAVA Pilot Program Testing Requirements (UPPTR) on August 25, 2010. The UPPTR are relevant both for any future FVAP pilot projects, and potentially for an electronic voting demonstration project mandated by Congress in the 2002 and 2005 National Defense Authorization Acts (NDAA). Following the publication of the UPPTR, FVAP initiated the following programs to evaluate the accessibility and security of electronic voting technologies:

- FVAP sponsored testing on the usability and testability of the UPPTR. Two EAC-accredited Voting System Test Laboratories (VSTL) conducted these tests on seven electronic voting systems. These tests focused solely on Sections 2 (Functional Requirements) and Section 5 (Security) of the UPPTR.
- FVAP collaborated with the U.S. Air Force Institute of Technology (AFIT) to carry out penetration testing of three electronic voting systems.
- FVAP began exploration of internet-based kiosk voting systems for use by military and overseas voters via the Voting Operations Testing and Evaluation (Operation VOTE) project. Six electronic voting systems under went testing for usability, accessibility, and privacy considerations.

As part of each test program, the test participants submitted comments and recommendations for updates to the UPPTR to increase the readability, usability, and testability of the requirements.

This report summarizes UPPTR-related comments FVAP received during the execution of these three programs. Section 1 provides background information regarding the UPPTR, and describes relevant legislation and federal entities, while Section 2 details FVAP's three testing programs. In the fall of 2012, FVAP, the EAC, and NIST conducted a series of joint meetings to review and address the submitted comments. Section 3 of this document summarizes discussion at these meetings and details the final accepted recommendations from the three test programs. FVAP is presenting this report to the EAC and NIST as part of the process to improve the UPPTR and any future electronic voting demonstration project guidelines.

Table of Contents

List of Figures

1 Introduction

1.1 Background

Under UOCAVA of 1986, 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 legislation became law before the advent of today's global electronic communications technology. At that time, the absentee voting process relied on U.S. domestic and military mail systems, as well as foreign postal systems for the worldwide distribution of election materials. By the mid-1990s, it became apparent that the mail transit time and postal delivery logistics posed significant barriers for many UOCAVA citizens, thus preventing them from successfully exercising their right to vote. Over the next decade, businesses, governments, and the public widely adopted the internet for a variety of communication and data transfer services. Therefore, it was a natural development for FVAP and the states to consider the potential of electronic communication as an alternative to the "by-mail" UOCAVA voting process.

In 2002 the NDAA mandated by Congress that FVAP carry out an electronic voting demonstration project in the 2002 or 2004 general elections, using a statistically significant number of absent uniformed services members. The 2005 NDAA amended this mandate, allowing FVAP to delay the implementation of the demonstration project until the EAC had established electronic absentee voting guidelines and certified that it would assist FVAP in carrying out the project. In 2009, Congress passed the MOVE Act, authorizing FVAP to run pilot programs testing the ability of new or emerging technologies to better serve uniformed and overseas citizens (collectively known as the UOCAVA population) during the voting process. The MOVE Act required that the EAC and the NIST provide FVAP with best practices, or standards, in accordance with electronic absentee voting guidelines to support the pilot programs.

The EAC operates a voting system testing and certification program, via accredited VSTL, using the 2005 Voluntary Voting System Guidelines (VVSG). These guidelines received input and guidance from both the EAC and NIST. The EAC's program certifies, decertifies, and recertifies voting system hardware and software and accredits test laboratories. While states are not required to participate in the program, many have enacted laws that require some level of participation, providing a level of assurance that voting systems offer required functionality and operate reliably and securely.

While the EAC has yet to publish guidelines for the mandated demonstration project, the EAC, NIST, and FVAP cooperated to create the UPPTR for use with MOVE Act-authorized pilot projects. In these testing requirements, the three agencies considered the differences between such pilot projects and regularly certified voting systems used in traditional polling places. Pilot projects are small in scale and short in duration. Consequently, certification for pilot systems should be quicker and less expensive than the process currently used for conventional systems with an expected life of over 10 years. Nevertheless, pilot voting systems may allow voters to cast actual votes and the certification process must retain sufficient rigor to provide reasonable assurance that these systems will operate correctly and securely.

The EAC published the UPPTR on August 25, 2010. This document defines requirements for conformance of kiosk-based remote electronic voting systems, intended for use in UOCAVA pilot programs, and specifies minimum requirements for functional capabilities, performance characteristics (including security), documentation, and test evaluation criteria. The UPPTR also provides the framework, procedures, and requirements followed by VSTL and manufacturers responsible for the certification testing of such pilot program systems. The intended use of the requirements is for the following groups:

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

1.2 Scope

After the UPPTR publication, FVAP initiated a number of projects to evaluate the accessibility and security of electronic voting systems. These efforts resulted in the following reports detailed below:

- Voting System Testing Laboratory Functionality and Security Testing
  This report detailed the testing of five electronic ballot delivery systems against Section 5 (Security) of the UPPTR, and the testing of two internet voting systems against Sections 2 (Functional Requirements) and Section 5 (Security) of the UPPTR.
- Voting Operations Testing and Evaluation (Operation VOTE)
  This report detailed accessibility, usability, and privacy testing of three electronic ballot delivery systems and three internet-voting systems. Although not a full conformance test against the UPPTR, this testing provided comments on Section 3 (Usability) of the UPPTR.
- Penetration Testing of a Simulated Election
  This report detailed the penetration security testing of three internet-voting systems and provided comments on all security-related portions of the UPPTR.

The primary goal of these projects was to assess the adequacy and testability of the UPPTR. There is no scheduled revision of the UPPTR by the EAC in the near future. These requirements are relevant to the congressionally mandated electronic voting demonstration project since they speak to similar architectural features. Recommendations to improve the UPPTR while considering the context of required electronic absentee voting guidelines for this project are essential. Chapter 2 of this report briefly describes FVAP's programs, while Chapter 3 summarizes the resulting recommendations for improvements to the UPPTR, as suggested by test engineers, security analysts, VSTL, and end-users. Appendix A contains all UPPTR-related recommendations submitted over the three projects.

2 FVAP Testing Programs

Efforts to evaluate the security and accessibility of electronic voting technology are predicated on the assumption that FVAP will be involved in the direct funding and testing of pilot programs or a demonstration project. Direct experience organizing testing efforts, evaluating testing requirements, interacting with VSTL and voting technology manufacturers, and assessing security and accessibility feedback from experts will thus be critical to FVAP in its future efforts in this domain. The initial testing programs described in this section sought data on the usability and testability of the UPPTR, which is likely to form the basis of future guidelines for an electronic voting demonstration project.

2.1 VSTL Functionality and Security Testing

Following the publication of the UPPTR, FVAP initiated a test project of the UPPTR using electronic voting systems as tools to aid in the testing. FVAP sought a testing effort to provide insight into:

- The security and functionality of electronic ballot delivery and internet voting systems currently in marketplace;
- Methodologies and results across different VSTL; and
- The suitability of the UPPTR to serve as a baseline for future standards related to the electronic voting demonstration project.

2.2 VSTL Functionality and Security Testing Methodology

We understand that the UOCAVA Pilot Program Testing Requirements design is for testing a traditional manned kiosk voting system; therefore, some of the requirements would not translate well into a completely web-based system. This reality aided us as we developed the methodology and analyzed the results of the test.

In order to stay within the UPPTR testing scope desired by FVAP, the VSTL 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.

EAC Certification Requirements

In standard voting system certification, registered voting system vendors, and VSTL must adhere to the EAC Voting System Testing and Certification Program Manual. The primary purpose of this manual is to provide clear procedures to VSTL for testing and certification of voting systems. VVSG Section 1.4, Volume II requires the VSTL to follow the specific 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.

VSTL Methodologies

At the time of the initial research, SLI and Wyle were the only two active VSTL accredited by the EAC for voting system certification. The VSTL's 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 require 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 communicated to the system vendor throughout the process.[i] Each VSTL has an established standard methodology that is traceable to the activities in Section 1.4 of the 2005 VVSG. Prior to testing, each VSTL submits a formal test plan for approval and the EAC provides clarifying guidance for any ambiguities. This formal environment for both a test plan and EAC guidance was not included within this research.

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 all hardware, consumables, source code, and applications; a technical data packages (TDP); a declaration of the functionality supported by the system; and documentation of how the system is employed by a jurisdiction.

Details of the seven phases of SLI's standard testing model are described below.

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;
- TDP review;
- Vendor training on the various aspects of their system;
- A comparison of the documentation against applicable requirements to verify that all required information is appropriately conveyed;
- A source code review; and

i 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

- A test plan created at the end of this phase that details the system variations to be tested, and how the test suites[ii] 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.

SLI Second Phase - System Familiarization & Readiness

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

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 the modules determines how well individual requirements have been met.

SLI Fourth Phase - Test Validation

During the fourth phase, each test module incorporates the respective suites. The correctness of each module under goes validation within each suite.[iii] 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 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.

SLI Fifth Phase - Test Execution

The fifth phase encompasses the formal execution of each test suite, as prescribed in the test plan. Test modules are created for each vendor and once validated become the platform for testing. If there was insufficient documentation to create test cases, the possibility for ad-hoc testing exists.

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.

[ii] 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.

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

SLI Seventh Phase - Finalization

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

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.

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.

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 employ 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 to run during the penetration test.

Source code testing for compliance to Sections 5 and Section 7 (Volumes I and II) of the EAC 2005 VVSG conducted. 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. After successful review of all source code and install packages in order to confirm their compliance with the EAC 2005 VVSG, trusted build of the code is completed.

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.

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 then defined with a written script. The test consists of executing each step of the script, recording observations and relevant data as each step completes. During testing 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 tested for functionality, strength, and NIST compliance. Systems that generate cryptographic keys internally tested for key management. This includes the generation method, security of the generation method, seed values, and random number generation. Individual test cases for the system 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 provided to a certified security professional, who will analyze the results and determine the best method and types of attacks to perform during the exploratory phase of testing.

The exploratory phase of the penetration test will have specific test cases designed and executed. Test cases include 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.

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

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 Electronic Ballot Delivery Systems (EBDS).

FVAP Approach

FVAP established a modified testing scope to encourage the broadest possible participation from the vendors. The EAC Voting System Pilot Program Testing and Certification Manual was not followed in its entirety because 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 VSTL's standard methodologies that the scope omitted from the testing.

Inclusions:

- Security testing against UPPTR Section 5 EDBS;
- Full system testing against UPPTR Sections 2 and 5 for two Internet Voting Systems (IVS);
- 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";
- The 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

- The final test report includes the VSTL 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 VSTL 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 VSTL testing campaign are identified for those activities not performed.

Impact of FVAP Approach

In accordance with the inclusion and exclusion list above, both VSTL made deviations to their standard methodologies. Figure 1 outlines the VVSG activities, FVAP modification / deviation from standard procedures, the impact on the VSTL, and VSTL differences. The most significant of these exclusions was not requiring the vendors to provide a TDP to the VSTL and not requiring source code reviews, these activities are not required by the EAC. These two exclusions resulted in major adverse impacts on the VSTL's ability to develop and execute test cases. The changes made to the methodology of each VSTL were driven by the insertion of the new UPPTRs and the actual scope of the testing events. FVAP decided to exclude TDPs and code review to meet the required schedule and constrain its focus on the viability of the UPPTR as well as develop experiences in terms of working with VSTL's which will likely be a future requirement for any future pilot projects or the conduct of the electronic voting demonstration project.

Figure 1: VSTL Standard Methodology for EAC Certification and Deviations

VVSG Activities	FVAP Approach	Impact on VSTL	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 VSTL could not complete Phase One of their Test Methodology	
b. Examination of the vendor's Quality Assurance Program and Configuration Management Plan	Not Required	VSTL 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)		VSTL 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	VSTL did not perform this activity	
e. Witnessing of a system 'build' conducted by the vendor to conclusively establish the system version and components being tested	Not Required	VSTL did not perform this activity	
f. Operational testing of hardware components, including environmental tests, to ensure that operational performance requirements are achieved	Not Required	VSTL 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	VSTL did not perform this activity	

VVSG Activities	FVAP Approach	Impact on VSTL	VSTL Differences
h. System installation testing and testing of related documentation for system installation and diagnostic testing	Not Required	VSTL 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	VSTL did not perform testing of the Operational Manual	
k. Examination of the system maintenance manual	Not Required	VSTL 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.	VSTL does 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	VSTL did not perform this activity	

2.3 VSTL Functionality and Security Testing Results

During execution of a typical certification test, the EAC requires an approved test plan prior to initiation of the test effort. Without this approved test plan and the specific EAC guidance that accompanies it, the testing project found that the UPPTR requirements, as written, allow for variations in interpretation. For example, the two VSTLs interpreted the number of UPPTR requirements differently – while both evaluated all of Section 5.6, Wyle based their results on 17 requirements, while SLI broke the requirements down to include individual bullets, creating 70 requirements. In UPPTR Section 2, SLI recommended that 36 of the requirements enumerated be, split, modified, or deleted for clarification and testability. In UPPTR Section 5, SLI and Wyle recommended that 65 of the requirements to be enumerated, split, modified, or deleted for clarification and testability.

Both VSTLs reported significant limitations in the testing due to exclusions established for these tests. Two major areas influencing the VSTL's testing were the lack of TDP and the availability of source code for the voting systems. The VSTL reported that the lack of sufficient information and technical documentation limited their ability to define test cases and identify the testable requirements. In addition, due to the lack of source code the VSTL could not perform UPPTR-required 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).

2.4 Operation VOTE

As part of a broad initiative to evaluate potential systems for remote voting electronic pilot projects, FVAP coordinated with the Office of Wounded Warrior Care and Transition Policy (WWCTP) and the EAC to address the voting related needs of Wounded Warriors. The Operation Vote project assessed the usability, accessibility, and privacy of electronic voting systems.

This targeted test evaluated six electronic voting systems, using Wounded Warrior participants as testers, and as practicable, assessing Section 3 (Usability) of the UPPTR. This was the first exercise of its kind performed by FVAP, and the first evaluation of the UPPTR to use voters with disabilities in a mock election process. At its highest level, Operation VOTE served as a trial to show that such a test was feasible. The objectives of this testing was to assess both IVS and EBDS in a potential kiosk environment, in order to identify:

- Wounded Warrior needs;
- Usability, accessibility, and privacy deficiencies in the platforms; and
- Deficiencies in Section 3 of the UPPTR.

Section 3 of the UPPTR describes usability, accessibility and privacy issues related to voting systems. The requirements in this section address a broad range of usability and accessibility factors, including physical abilities, language skills, and technology experience across various disabilities, comprising cognitive, vision, hearing, dexterity, and mobility challenges. The third goal of Operation VOTE was the creation of meaningful recommendations for the EAC, enabling improvements to Section 3 of the UPPTR with regard to persons with disabilities generally, and Wounded Warriors specifically.

2.4.1 Usability and Accessibility

Operation VOTE attempted to replicate a personal absentee voting experience using either an IVS or EBDS system, while allowing volunteer participants to be observed in a manner that could provide insight into the usability, accessibility, and privacy of the voting platforms. All vendors were provided a standard ballot for use during the exercise (see Appendix D for the sample ballot found in the original report). All volunteers gave informed consent prior to participating in Operation VOTE, and the data collection carried out in accordance with Department of Defense policies, under the Washington Headquarters Service Report Control Symbol DD-P&R (OT)-2483.

Operation VOTE took place as follows:

Upon arrival at the Brooke Army Medical Center, participants were welcomed by FVAP representatives, read the consent form, and were handed a unique number that would allow for their voting experience and system documentation while maintaining their anonymity. Vendor representatives then showed the participants a 3-5 minute overview of the voting system and reviewed any specific accessibility features. At the conclusion of the demonstration, FVAP staff escorted each voter to the voting machine where they completed their ballot. If necessary, a "poll worker" (voting system vendor representative) was available to assist the participants during the voting process, just as a poll worker would offer help in an actual voting environment. See Appendix E for a detailed picture of the layout of the testing space used during Operation VOTE.

A trained member of the project team observed each participant advancing through the voting process. Participants received instructions to ignore the observers in their latter assessments of the privacy of the systems. Observers recorded their evaluations of the participants' voting experiences on an observer checklist (see Appendix B). The checklist was used by the observers to assess issues relating to usability, accessibility, and privacy as well as the effectiveness and efficiency of the voting process for the participants.

Upon completion of the voting process, FVAP interviewed each voter to assess their satisfaction with the particular voting system that they used (see Appendix C). Questions dealt with the accessibility, usability, and privacy features of the voting system, including physical system configuration, visual display settings, audio features, tactile controls, instructions, navigation, voting selection, help features, error messages, ballot summary, and ballot submission. Participants were asked about their previous voting experiences and their medical situation, including current difficulties with vision, hearing, mobility, dexterity, cognition, and emotion.

Inclusions

Section 3 of the UPPTR provides specific guidelines related to the usability, accessibility, and privacy of voting systems (see Appendix A). However, not all aspects of the requirements apply to the IVS and EBDS voting systems, and many of the requirements were not testable outside of a lab environment. For the purposes of this project, only the aspects of Section 3 UPPTR that were clearly testable and observed in a simulated voting environment were included in this evaluation.[iv] A summarization of these aspects can be found in the sections below, and a full requirement-by-requirement listing can be found in Appendix G .

Usability

The following table summarizes Section 3 usability requirements (including privacy) observable during Operation VOTE.

Figure 2: Observerable UPPTR Usability Requirements

Section 3.2: Usability			
3.2.1	Privacy	.1 a & b	The ability of the voting system to prevent people other than the voter from determining the content of the ballot during the voting process.
		.1 c	The audio interface is audible only to the voter.
		.1 d	Any alerts and/or warnings given by the voting system preserve the privacy of the voter.
		.1 e	The vote capture device does not issue a receipt to the voter that would

[iv] Some portions of the UPPTR Section 3 were not tested due to unclear language.

Section 3.2: Usability			
			provide proof to another of how the voter voted.
3.2.2	Cognitive Issues	a	The voting system includes valid instructions for all operations.
		b	The voting system provides a means for the voter to get help directly from the system.
		d	The voting system supports a process that does not introduce a bias for or against any ballot choices.
		e	There is a capability to design a ballot with a high level of clarity and comprehensibility.
		f	Any use of color agrees with common conventions.
		g	When an icon is used to convey information, indicate an action, or prompt a response, it is accompanied by a corresponding linguistic label.
3.2.3	Perceptual Issues	b	System performs an automatic reset to standard default settings upon completion of individual voting session.
		c	System contains a mechanism to allow the voter to reset all settings to default values while preserving current votes.
		e	The voting system is capable of showing all information in at least two defined font sizes.
		g	Reading assistance is provided for any paper verification records.
		j	The system supports correct perception by voters with color blindness.
		k	Color coding is not used as the sole means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.
3.2.4	Interaction Issues	a	No page scrolling is required by voters.
		b	There is unambiguous feedback regarding the voter's selection.

Accessibility

The following figure details Section 3 accessibility requirements observable during Operation VOTE.

Figure 3: Observable UPPTR Accessibility Requirements

Section 3.3: Accessibility			
3.3.1	General	b	When the provision of accessibility for the voting system involves an alternative format for ballot presentation, then all information presented to non-disabled voters, including instructions, warnings, error and other messages, and contest choices are presented in the alternative format.
		c	The support provided to voters with disabilities is intrinsic to the voting system and it is not necessary for the voting system to be connected to any personal assistive device of the voter in order for the voter to operate it correctly.
3.3.2	Low Vision	a	Black text on white background and white text on black background are provided as display options.
		b	Buttons and controls on the voting station are distinguishable by both shape and color.
		c	Synchronized audio output is available to convey any information displayed on screen; there is a means by which the voter can disable either the audio or video output; and the system allows the voter to switch among the three modes

Section 3.3: Accessibility			
			throughout the voting session while preserving current votes.
3.3.3	Blindness	a	There is an audio-tactile interface that supports the full functionality of the visual ballot interface.
		b	Voting stations that provide audio presentation of the ballot do so in a usable way.
		c	If the voting system supports ballot activation for non-blind voters, then it also provides features that enable voters who are blind to perform this activation.
		d	The support of ballot submission or vote verification for non-blind voters is also provided for voters who are blind.
		e	Mechanically operated controls or keys, or any other hardware interface on the voting system available to the voter is tactilely discernible without activating those controls or keys.
		f	The status of all locking or toggle controls or keys for voting system are visually discernible, and also discernible through either touch or sound.
3.3.4	Dexterity	a	There is a mechanism to enable non-manual input that is functionally equivalent to tactile input.
		b	Features are provided that enable voters who lack fine motor control to perform ballot submission and/or vote verification.
		c	Keys, controls, and other manual operations are operable with one hand without requiring tight grasping, pinching, or twisting of the wrist.
		d	The system does not require direct bodily contact or the body to be a part of any electrical circuit.
3.3.5	Mobility	c	Labels, displays, controls, keys, audio jacks, and other parts of the voting system necessary to operate the voting system are legible and visible to a voter in a wheelchair with normal eyesight.
3.3.8	English Proficiency	a	There are features designed to assist voters who lack proficiency in reading English.

Exclusions

FVAP considered voting system features and functionality that do not affect voting usability, accessibility, and privacy out of the scope during Operation VOTE testing. No portions of UPPTR Sections 2, 4, 5, 6, 7, 8, or 9 received evaluation in this exercise. Furthermore, portions of the UPPTR Section 3 that were not easily observable during a simulated election process, that were not applicable to IVS and EBDS voting systems, or that were ambiguously worded were not evaluated. Ballot design usability not evaluated during Operation VOTE.

Systems Tested

Six voting systems from six different voting system vendors participated in testing during Operation VOTE. Three IVS systems participated on Day 1 and three EBDS systems on Day 2. IVS and EBDS platforms are usable on any PC or laptop, have the capability to display an unlimited number of different ballots, and potential candidates for use in an overseas kiosk voting environment. In addition, an IVS system has obvious usability benefits based on its original architecture in support of an electronic voting transaction. Figure 4 summarizes the voting systems and vendors who participated in Operation VOTE. Selection of these particular systems were based either on vendor experience in real-world elections or prior participation in FVAP's Electronic Voting Support Wizard (EVSW) program and identified those

IVS systems registered with the EAC.[v] Direct Recording Electronic (DRE), optical scan, digital scan, Ballot Marking Devices (BMDs) and other voting technologies were not included in this voting system evaluation.

Figure 4: Voting System Manufacturers

Type	Manufacturer	System Name	Selection Criteria
IVS	Dominion Voting Systems www.dominionvoting.com	Democracy Suite IVS	Dominion Voting is the second largest election vendor in the U.S.* and its IVS solution has been used in Canada.
IVS	Everyone Counts www.everyonecounts.com	eLect Platform	Everyone Counts participated in FVAP's EVSW program and has deployed internet voting technology around the world.
IVS	Scytl www.scytl.com	Scytl Pynx	Scytl participated in FVAP's EVSW program and has deployed internet voting technology around the world.**
EBDS	Democracy Live www.democracylive.com	LiveBallot	Democracy Live participated in FVAP's EVSW program.
EBDS	Konnech www.konnech.com	Konnech EVSW	Konnech participated in FVAP's EVSW program.
EBDS	Credence www.credence-llc.com	Credence EVSW	Credence participated in FVAP's EVSW program.

**Election Systems & Software (ES&S) is the largest.*
***Scytl is now in a marketing arrangement with ES&S to market Scytl's technology in the United States.*

The following paragraphs contain more detailed descriptions of each of the systems as configured for Operation VOTE. It should be noted that other configurations of these systems might be possible, including configurations that allow election officials to set pop-up versus verification screen warnings, and configurations for some EBDS systems to electronically cast the ballots. However, only the configurations specified here received assessment during Operation VOTE.

Democracy Suite IVS

The Democracy Suite IVS is an interactive internet voting solution developed by Dominion Voting, and provides a web-based voting interface that allows voters to electronically receive, complete, and cast their ballots. The system presented the Operation VOTE ballot as one race per screen. Voters received notice of any over or under-votes on a verification screen after the last race. The system allowed voters to make changes from the verification screen before casting their ballots, but security and privacy implementation required them to restart a blank ballot from the beginning to allow changes to the ballot.

eLect Platform IVS

The eLect Platform IVS is an interactive internet voting solution developed by Everyone Counts, and provides a web-based voting interface that allows voters to electronically receive, complete, and cast their ballots. The system presented the Operation VOTE ballot as one race per screen. Voters received notification of under-votes on a verification screen after the last race. The system prevented over-votes

[v] The EVSW program was an FVAP funded and managed EBDS tool employed in collaboration with state election officials on a pilot basis during the 2010 election.

on each race by requiring participants to deselect their choices prior to selecting new candidates. The system allowed voters to make changes from the verification screen before casting their ballots, and provided a "change selection" link under each choice that would take the voter directly back to each individual contest needing correction, such that voters did not have to restart the ballot.

Pnyx IVS

The Pnyx IVS is an interactive internet voting solution developed by Scytl, and provides a web-based voting interface that allows voters to electronically receive, complete, and cast their ballots. The system presented the Operation VOTE ballot as one race per screen. Voter's received notification of under and over-votes by an immediate pop-up message. The system allowed voters to make changes from the verification screen before casting their ballots, but returned the voter to the first race and required them to click through the ballot from the beginning to make changes (voter selections were preserved).

LiveBallot EBDS

The LiveBallot EBDS is an interactive electronic ballot delivery system developed by Democracy Live, and provides a web-based voting interface that allows voters to receive, complete, and print the ballot for postal mailing. Voters could choose whether the Operation VOTE ballot would present as one race per screen or all races on one screen. Voters received notification of over-votes by an immediate pop-up message on the screen, while under-votes did not receive an error message until the verification screen after the last race. The system allowed voters to make changes from the verification screen before printing their ballots, and the verification screen provided links to take voters directly to the individual contests needing correction, such that voters did not have to restart the ballot. Voters followed on-screen instructions to print the ballot and then secured it in an envelope to be mailed for tabulation.

Konnech EBDS

The Konnech EBDS is an interactive electronic ballot delivery system, and provides a web-based voting interface that allows voters to receive, complete, and print the ballot for postal mailing. The system displayed all Operation VOTE races on one screen. Voters received notification of under-votes by a pop-up message at the bottom of the screen, which stated that not all selections were made and the voter had not completely voted, but it did not specify in which race the vote(s) were missing. The use of radio buttons prevented over-voting in races where voters could choose only one candidate.[vi] After completing the ballot, the voter converted the ballot to a PDF file. The voter then printed the PDF file and secured it in an envelope to be mailed for tabulation. After printing the ballot, a new browser window appeared confirming the votes were cast. If voters found an error, they were required to restart the process with a blank ballot to correct the error.

Credence EBDS

The Credence EBDS is a web-based electronic ballot delivery system, which delivers the PDF ballot and allows it to be electronically filled and printed for postal mailing. The system delivered all Operation VOTE races on one screen, just as the entire ballot was one PDF file. The use of the PDF interface meant that the system did not provide notification or warning messages about under or over-votes, and did not provide a verification screen. However, the use of radio buttons prevented over-voting in races where voters could choose only one candidate. Voters used the Adobe Acrobat interface to print their ballot and then secured it in an envelope for mailing and tabulation.

[vi] Radio buttons, also called option buttons, are a type of graphical user interface that allow the user to only choose one option from a predefined set.

Participants

Participants in Operation VOTE consisted of volunteer Wounded Warriors and Warrior in Transition Unit staff stationed at Brooke Army Medical Center (BAMC). Based on previous research evaluating Wounded Warrior voting challenges,[vii] Wounded Warriors with vision, hearing, mobility, dexterity, cognitive, and emotional impairments were asked to participate in the exercise. Staff members who regularly work with the Wounded Warriors were invited to volunteer to ensure the broadest possible testing of system accessibility features. See Appendix F

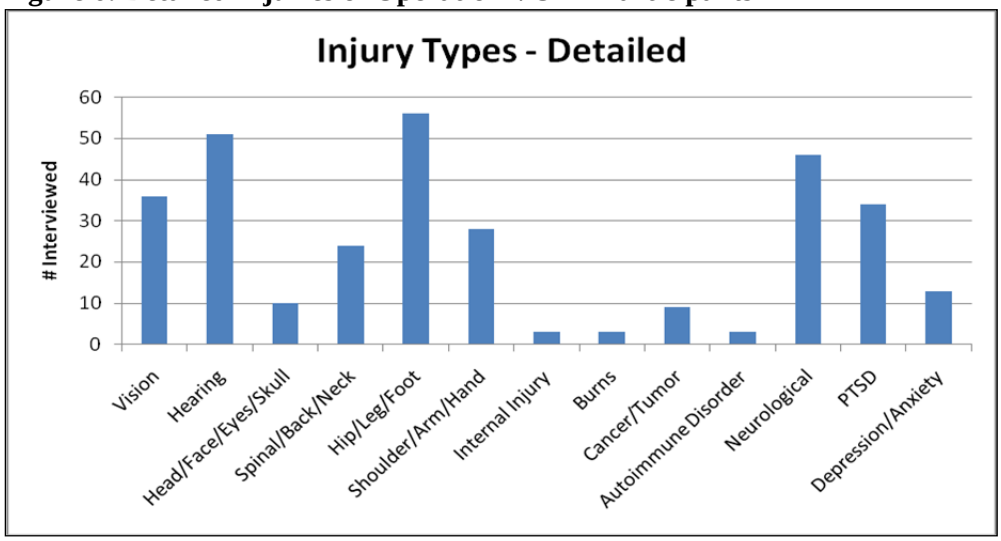
A total of 127 Wounded Warriors, family members, and Brooke Army Medical Center staff participated in Operation VOTE. Figure 4 below represents the breakdown of voters by platform and participant type.

Figure 5: Participant Numbers by Platform

Platform	Participant Type	Number
IVS	Wounded Warrior	61
	Staff	6
EBDS	Wounded Warrior	39
	Staff	21

A robust number of Warriors with a variety of injuries and illnesses participated in Operation VOTE. The following figure demonstrates the variety of injuries and illnesses reported by the Wounded Warrior participants in Operation VOTE. It should be noted that this figure represents only the injuries of personnel interviewed during Operation VOTE, and should not be generalized to all Wounded Warriors.

Figure 6: Detailed Injuries of Operation VOTE Participants

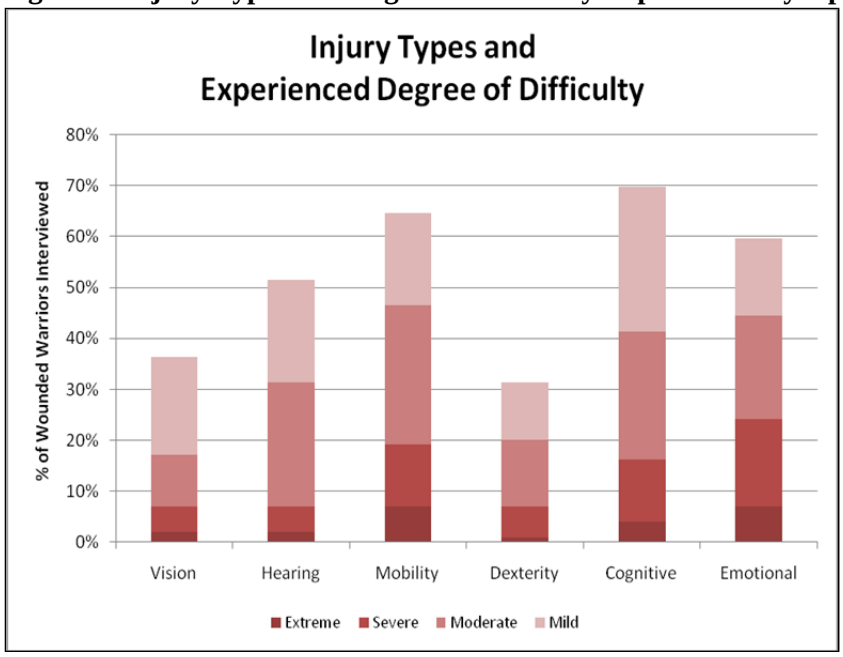


The detailed injuries aligned into six domains: vision, hearing, mobility, dexterity, cognitive, and emotional. The following figure shows that most interviewed Wounded Warriors reported difficulties in multiple domains, with over 60% reporting mobility and cognitive impairments, and over 50% reporting

[vii] Department of Defense. Federal Voting Assistance Program. CALIBRE Systems, Inc. 2011. Combat-Related Disabilities and Voting Challenges.

hearing and emotional impairments. When asked about the degree of difficulty they experienced in each domain, Wounded Warriors generally reported mild or moderate difficulties, although significant percentages also experienced severe or extreme difficulties, especially in mobility, cognitive, and emotional areas.

Figure 7: Injury Types and Degree of Difficulty Experienced by Operation VOTE Participants



Previous FVAP research has shown that injured service members may have special voting-related requirements related to reading forms and instructions, completing forms and ballots, and travelling to their local polling place and voting in-person. This research suggested the following accommodations relevant to electronic voting systems:

- access to voting assistance online;
- simplified forms and written instructions with a large type;
- voting website assistance and tools that are compatible with screen readers;
- the ability to magnify information;
- dual auditory and visual versions of registration and ballot materials;
- availability of headphones with adjustable volume for audio; and
- voting technology that is accessible and compatible with assistive devices for dexterity impairments.[viii]

2.4.2 Operation VOTE Results

A review of Section 3 of the UPPTR found these requirements to be generally robust, comprehensive, and applicable to either the IVS or EBDS systems. However, the Operation VOTE test team suggested revisions to the UPPTR to remove ambiguity and maximize testing efficiency and efficacy. The final

[viii] Department of Defense. Federal Voting Assistance Program. CALIBRE Systems, Inc. 2011. Combat-Related Disabilities and Voting Challenges.

report contained a series of recommendations designed to clarify, clearly organize, and enhance the content of the UPPTR. These recommendations included suggestions for consistent numbering, condensing redundant requirements, separating out distinct requirements, and adding additional requirements for voting system features to assist users with disabilities. Based on the data obtained during the Operation VOTE program, meaningful recommendations were made to the EAC, enabling improvements to Section 3 of the UPPTR with regard to persons with disabilities generally, and Wounded Warriors specifically.

The Operation VOTE test team recommended two UPPTR changes related to accessibility issues:

- Several Wounded Warriors who tested the systems explained that while accessibility features were present in the systems, they had no way of knowing how to access or operate these features without poll worker assistance. There is currently no specific language in Section 3 of the UPPTR, which describes a requirement for prominent, understandable instructions about how to operate accessibility features. Requirement 3.2.2 (a) does state: "The vote capture device SHALL provide instructions for all its valid operations." However, it is not clear from the context whether accessibility features or adjustable aspects of the vote capture device are specifically included in the words "valid operations." The Operation VOTE test team felt that such specific language added to the above requirement, or to a new, additional requirement is necessary.
- Another deficiency in Section 3 of the UPPTR related to requirement 3.3.7(a) which states: "The accessible voting station should provide support to voters with cognitive disabilities." This requirement is not prescriptive, presumably because this section does not describe any specific, testable features of the accessible voting station that could assist voters with cognitive disabilities. However, guidelines for such assistance are present in many prominent usability and accessibility-related resources, including the Web Content Accessibility Guidelines (WCAG) and the Illinois Center for Information Technology Accessibility (iCITA) HTML Best Practices. The Operation VOTE test team recommended that specific, testable requirements be adapted from available resources and added to section 3.3.7 of the UPPTR.

2.5 Penetration Testing of a Simulated Election

To address security issues, FVAP collaborated with AFIT to carry out penetration testing of three electronic voting systems.

Penetration testing is an integral form of security testing which challenges online system security using techniques similar to those used by criminals and other hostile entities intent on inflicting genuine harm. However, in an authorized penetration test, all parties agree to the testing; and the testing conducted for the benefit, not the harm, of the system vendors and all stakeholders. The findings of the penetration test then evaluated so that mitigation strategies can be developed and applied to manage security risks to acceptable levels.

FVAP's penetration testing consisted of a 72-hour period in in August 2011 using online voting systems developed by three major online voting system vendors whose systems successfully used by jurisdictions throughout the world to conduct online elections. The intent of this penetration testing and subsequent analysis was to provide FVAP with usable information about the security posture of current online voting systems, and to provide data that supports decisions regarding FVAP's future congressionally mandated

demonstration project. Additionally, the testing intended to assess if the UPPTR requirements were sufficient as written or are in need of revision

2.5.1 Penetration Testing Methodology

We understand that the UOCAVA Pilot Program Testing Requirements are more relevant to testing a traditional manned kiosk voting system. This lead to assumptions that some of the requirements would not translate well into a web-based system. FVAP considered this as we developed the methodology and analyzed the results of the test. The penetration testing covered Section 5 and Section 9 of the UPPTR.

The following text describes the methodology used to conduct the PenTest and outlines the design of the experiment, the test environment, the teams involved in the test, and how ballots were cast. Also outlined is what was *not* undertaken for this mock election PenTest.

We understand that the UOCAVA Pilot Program Testing Requirements are more relevant to testing a traditional manned kiosk voting system. FVAP assumed that some of the requirements would not translate well into a web-based system. This was considered as we developed the methodology and analyzed the results of the test.

In designing the methodology for penetration testing, FVAP developed a list of assumptions given that this penetration test would serve as an initial "proof of principle" which further penetration tests could be built and improved upon. The list of assumptions is listed below:

- All vendors will have some security built into their systems.
- The PenTest will show some weaknesses in the vendors' systems.
- There would be insufficient time to complete a source code review.
- The vendors may not have all the needed information for a complete TDP so a minimum of technical data requested from the vendors.

The AFIT students received training from Mr. Rossi on network security concepts. They also received three separate PenTesting training sessions provided by the RedPhone team. This training provided the students with actionable knowledge on how to construct a test plan, execute the plan, and properly format and report the team's findings. Additionally, the students received hands-on training using many "hacker" tools. Examples of these tools include Metasploit, Nessus and NMAP. Each training session provided a logical information progression on each vendor, the tools (and how to use them), and how to build a successful PenTest. FVAP provided to the students templates for constructing their test plan and the final report format for their findings. The graphic in Figure 3 provides a systematic explanation of how the voter cast a ballot and at what point the PenTest teams attempted to penetrate the systems.

A student lounge used by AFIT students served as the polling place for the mock election portion of the PenTest. The area selected was easily accessible by the AFIT students, and they were frequently in the area during breaks and lunch. Since the students were the volunteer voters for the experiment, it was essential that the area was convenient for them to access. AFIT provided each vendor one laptop computer with only the operating system, Internet Explorer and Firefox installed. The voting computers became part of the AFIT network and provided Internet access without going through any firewalls or other security devices. Figure 2 below, graphically depicts the AFIT test system environment.

AFIT assigned each computer a static IP address and these IP addresses given to each hacking team. The systems were operational for the entire 72-hour period. The student lounge was accessible by the

volunteer voters at any time to cast their ballots; however, traffic through the lounge did abate after normal duty hours, which are 0730–1700 Monday through Friday. Although the AFIT facility is located on a secure military installation, there were no specific physical security precautions taken to protect the machines; no locks or security cables installed to secure the systems to the shelf; and no guards posted to protect the voting machines. The systems did not time out nor did they allow a screen saver to pop up after a certain amount of time.

The volunteer voters walked up to the system of their choice—most voted on all three—and cast their ballots. The three vendors supplied any necessary logon credentials, and the voters used these credentials to access each vendor's Internet voting site. These credentials varied from vendor to vendor, were not complicated, easily used, and allowed the voter to logon to each system's home page. Each vendor's system had a different way to cast an online ballot, but the systems were all intuitive and clear instructions provided on the screen. Each vendor was given one ballot to load into their system. Every voter had the opportunity to vote on each ballot, and voters prompted if they had under voted or over voted on a particular ballot. Two of the races on the ballot allowed the choice of a single candidate. One race allowed the voter to pick up to three of six possible candidates.

Both the AFIT student and the RedPhone penetration teams had direct access to each voting computer, and they did approach each machine and cast ballots. The RedPhone team worked mostly off site, but they did approach the machines in the student lounge and cast ballots. As this was a cooperative test, both the AFIT and RedPhone PenTest teams were given voting computer and voting system server IP addresses. This allowed more time for penetrating the voting systems without necessarily jeopardizing other AFIT production systems.

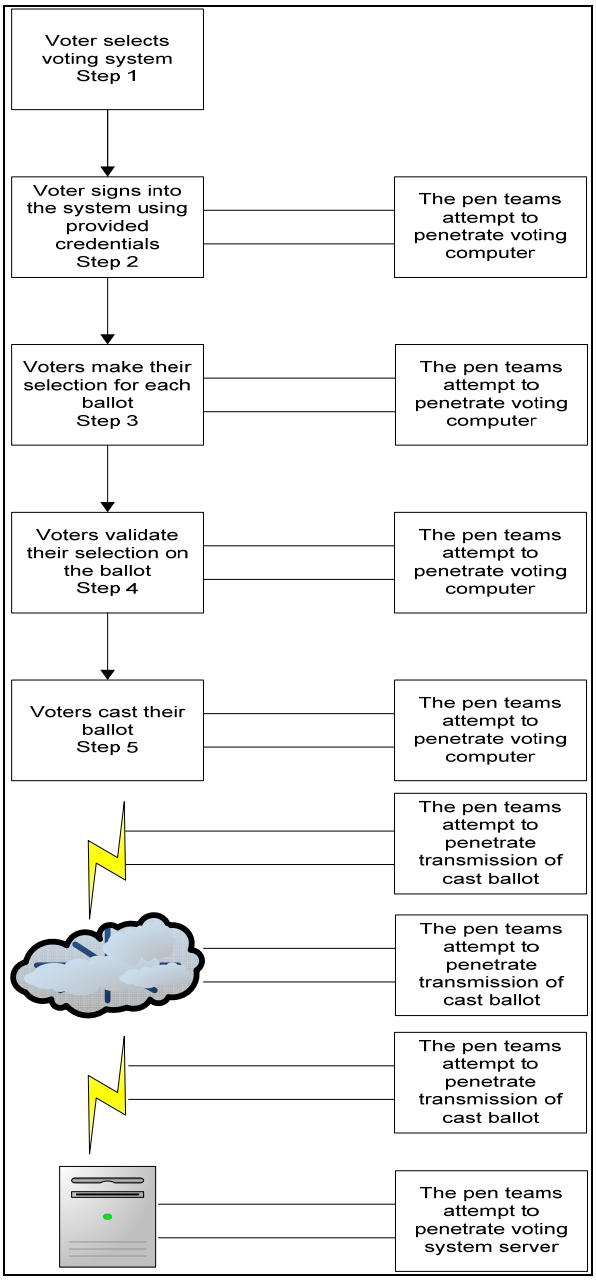


Figure 3. Voter Actions and Penetration Attempts

The PenTest teams were actively attempting to enter the vendor online voting system to change, alter, or delete a vote, or votes, beginning at Step 2 and continuing until after the ballot reached the voting system server. These servers were not physically located at AFIT, but geographically dispersed, with one server located outside the continental United States. Similar to the voting computers, the IP addresses of the voting systems servers were given to the penetration testing teams.

2.5.2 Penetration Testing Results

Most UPPTR changes recommended by the penetration testing effort were related to the development of a program manual specifically for VSTL, rather than manufacturer, use. For example, requirement 5.9.2

(Penetration Resistance Test and Evaluation) describes the scope of penetration testing, the test environment, the focus, and priorities for the testing, the composition of the test team, and the level of effort of the testing. All these requirements are oriented for the VSTL that performs the testing, and not for the manufacturer creating the system.

The requirement lends itself to a pre-programmed set of tests and events, which are describable in the program manual. This manual would provide guidance to the VSTL on how the requirements should be set-up and tested in a lab environment. The particular events needing action on each individual voting system would then be documented against the requirement for the task. Any changes needed to accommodate the particular voting system would be documented and the change in methodology recorded.

It is important to note that a balance between structured and non-structured security testing is currently the recommended industry best practice. Any guidance provided by the program manual should therefore also include guidance for non-structured and constrained penetration testing.

3 Recommendations for UPPTR Improvement

As part of each test program, the test participants submitted comments and recommendations for updates to the UPPTR to increase the readability, usability, and testability of the requirements. These comments are presented in Appendix A.

On October 03, 2012, FVAP led a meeting to review and address the submitted comments. The participants at this meeting were the EAC, NIST, and FVAP. The participants reviewed the submitted comments and either agreed with the comment, disagreed with the comment, or tried to address the comment in a manner acceptable to all three stakeholders. The following sections summarize discussion at this meeting and the final accepted recommendation from the three test programs.

Revision of the UPPTR is a long process that requires a period of public comment and is impossible without a quorum of the EAC Commissioners for approval. Thus, some recommendations affect the usability and readability of the UPPTR, but not its testability, this is accepted by all participants as useful for any potential revision of the UPPTR, but not for immediate modification.

3.1 Clarification

FVAP's test program participants submitted specific comments on three requirements that all stakeholders agreed could use additional clarification. These requirements are listed below, followed by a statement on what additional clarification is needed:

- Section 5.2.1.5 Password reset – The voting system SHALL provide a mechanism to reset a password if forgotten, in accordance with the system access/security policy.
    - The comment on this requirement was that it specifically states "password." However, system architecture could use other forms of authentication so this is too limiting
- Section 5.6.1.4 Logging events – The voting system SHALL log logging failures, log clearing, and log rotation.
    - The comment on this requirement was that logging failures are a system function, while log clearing and log rotation are administrative functions.
- Section 5.6.2.1 General – All communications actions SHALL be logged.
    - The comment of this requirement was that "all" is a very broad term and guidance given as to communications should be more specific.

FVAP recommends that NIST research the intent of these requirements and provide clarity to the intended scope of the requirements.

3.2 Specific Level or Degree

Throughout the test projects test participants made recommendations requesting specification of a level or degree to which a requirement was to be tested. This is difficult, as the UPPTR was developed to be broad enough to cover multiple pilot programs. Specifying degrees or levels would make the requirements more testable, but also less flexible.

For a pilot or future electronic voting demonstration project, stakeholders recommend that all stakeholders including the manufacturers, EAC, FVAP, VSTL, and NIST hold a series of design meetings to agree to which level or degree the system should be tested. The factors to consider in these design meetings are cost, time, and risks. These factors need to be identified and mitigated to complete a successful pilot program. The meetings should result in a test strategy that can be incorporated into a test plan, which would allow other stakeholders to review and comment on the intended strategy and approach.

3.3 Readability and Usability of the UPPTR

Many of the recommendations submitted by participants in FVAP's testing projects pertained to the organization and presentation of the UPPTR:

- High level requirements in the UPPTR currently contain prescriptive SHALL statements instead of "should" statements. FVAP testing participants felt that in most cases, the higher level requirement would be met by testing the sublevel requirements and that many high level requirements should be changed to contain "should" statements only.
- The UPPTR currently contains a number of requirements with multiple SHALL statements. Testing participants recommended that any requirement containing more than one unique SHALL statement should be divided into separate requirements, and that any requirement containing redundant SHALL statements should be changed to contain one clarifying "should" statement and one prescriptive SHALL statement.

The test program participants also found the numbering and level structure of the UPPTR somewhat confusing, and recommended changes to sublevel requirement numbering for consistency. FVAP believes that these types of comments are valuable and constructive suggestions, but they do not increase the testability of the requirements. FVAP understands that the revising of these requirements is a long process that requires a period of public comment and is impossible without a quorum of the EAC Commissioners to approve the revisions. Since these recommendations do not affect the testability of the UPPTR, the team recommends that the EAC and NIST examine these issues during the next revision.

3.4 Disposition of Recommendations

The specific dispositions of recommendations submitted to FVAP are contained in the table below.

Requirement	Comment	Disposition
Multiple	The test method should be changed.	The selected test method was determined by all parties involved in the development of the UPPTR. Factors such as time, cost, and resources were discussed during the development. No update recommended.
Multiple	Split the requirements with multiple "shall" statements into multiple requirements.	These comments might make the requirements more readable, but do not affect the testability. No update currently recommended. Should be considered at any potential revision of the UPPTR.
Multiple	The use of the word "shall" versus "should" in high level (first order) requirements.	On a case-by-case basis remove the word shall and replace with should for all first order requirements that have prescriptive sub-requirements. No update currently recommended. This will be considered at the next revision of the UPPTR.
Multiple	Add definitive authoritative documents (NIST and DoD) to clarify various requirements.	Authoritative documents should be cited when the requirement requires more clarity. References will be added at the next revision of the UPPTR.
Multiple	Enumerate requirements which are currently listed in tables.	Should be considered at any potential revision of the UPPTR.
Multiple	Requirement does not apply to voting system (e.g., the requirement is for ballots or other associated processes).	Should be considered at any potential revision of the UPPTR.
Multiple	The requirement does not define if this configuration is to be web-based or operating system configurable.	The requirement is satisfied whether the configuration in question is web-based or operating system configurable. No update currently recommended.
Multiple	All graphic file formats should be tested for corruption from malformed packets. Known vulnerabilities exist with almost all graphic file formats. Appropriate patches to operating systems must be tested.	It is recommended that during development of the test plan for any pilot program that all stakeholders agree on the types of files that must be examined for malicious content.

Requirement	Comment	Disposition
Multiple	Application scanning tools should be used to identify source code vulnerabilities.	The current version of the UPPTR has no software assurance tool requirements listed. It is recommended that during development of the test plan for any pilot program that all stakeholders agree on a combination of static and dynamic software assurance tools to be used during the test program.
2.2.1	This requirement does not provide acceptable minimums.	The requirements need to be flexible to accommodate systems of different sizes and capacities; therefore, the minimums were not stated. No update recommended.
2.4.2.1	The feasibility of this requirement would be determined by where the power failure occurred.	In any type system a backup power supply is required for the voting system to allow the voter to finish the voting session and successfully shutdown. If the voting session is on a device, it must have a backup power supply. If the voting session is remote the server must have a backup power supply. No update recommended.
3.3.7	Specific, testable requirements should be adapted from available resources and added to subsection 3.3.7 of the UPPTR (support for cognitive disabilities).	This comment could not be addressed during the disposition of all the comments because a subject matter expert was not present at the disposition meeting. An expert should be engaged and this comment considered at any potential revision of the UPPTR.
5.1.1.1	These requirements need a specific level or degree to be determined to increase testability.	It is recommended that once the system architecture is selected for a pilot program, all stakeholders agree on the level or degree to which these requirements will be tested.
5.1.1.3		
5.1.2		
5.1.2.1		
5.1.2.2		
5.1.2.6		
5.1.2.7		
5.1.2.9		
5.3.1.1		
5.2.1.5	This requirement covers only passwords and does not consider alternative methods of authentication.	It is recommended that during the next revision of the UPPTR this requirement be reworded to include other authentication methods.
5.6.1.4	This requirement contains both application level logging and administrative functions.	It is recommended that during the next revision of the UPPTR this requirement be reworded or split into different functional levels.
5.6.2.1	This requirement does not define the level of communication that must be logged (i.e.: hardware level, transport level, application level, etc.).	It is recommended that during the next revision of the UPPTR a discussion or examples be provided. Until such time, it is recommended that during the development of the test plan for any pilot program all stakeholders agree what communications are required to be logged.

Requirement	Comment	Disposition
5.6.3.3	This requirement does not provide a definition of the term critical.	It is recommended that during the development of the test plan for any pilot program that all stakeholders agree on the critical events that must be logged.

Appendix A: All Recommendations for UPPTR Changes

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
2.1 Accuracy	The voting system SHALL achieve a target error rate of no more than one in 10,000,000 ballot positions, a maximum acceptable error rate in the test process of one in 500,000 ballot positions.	"Shall" should be removed from header.			
2.1.1.1 Component accuracy	Memory hardware, such as semiconductor devices and magnetic storage media, SHALL be accurate.	1) Standards are recommended to specify appropriate component accuracy. 2) This is better suited to Inspection, viewing the results overall of the testing, as well as review of hardware manufacturer specifications.			
2.1.1.2 Equipment design	The design of equipment in all voting systems SHALL provide for protection against mechanical, thermal, and electromagnetic stresses that impact voting system accuracy.	This should be Inspection / Review of hardware test reports and/or hardware specifications.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
2.1.1.3 Voting system accuracy	d. Include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the voting system has been designed for accuracy;	1) Recommend this as Inspection. 2) Best suited for a source code review and environment specification, in particular for data at rest.			
2.1.1.3 Voting system accuracy	e. Provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected.	1) Recommend this as Inspection. As written, this requirement is only looking to verify that the monitoring software is provided. 2) Would recommend that the "…and how they were corrected." portion be broken out to another requirement, as this looks to be more of an event log.			
2.1.2 Environmental Range	All voting systems SHALL meet the accuracy requirements over manufacturer specified operating conditions and after storage under non-operating conditions.	This should be Inspection / Review of hardware test reports and/or hardware specifications. As written this requirement seems to be written more for a traditional voting system than a UOCAVA internet based system.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
2.1.3.1 Election management system accuracy	Voting systems SHALL accurately record all election management data entered by the user, including election officials or their designees.	As written, this requirement contains a high degree of vagueness. Each type of Election Management data should be enumerated.			
2.1.3.2 Recording accuracy	b. Accurately interpret voter selection(s) and record them correctly to memory; c. Verify the correctness of detection of the user selections and the addition of the selections correctly to memory; d. Verify the correctness of detection of data entered directly by the user and the addition of the selections correctly to memory; and e. Preserve the integrity of election management data stored in memory against corruption by stray electromagnetic emissions, and internally generated spurious electrical signals.	Our assumption here is that this requirement is testing write-ins as opposed to selecting choices, as in b and c. This requirement (b, c, and d) need to be clarified as to their specific intents, with any redundancies removed. e. would be covered under EMC testing. This should be Inspection / Review of hardware test reports and/or hardware specifications.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
2.1.4 Telecommunications Accuracy	The telecommunications components of all voting systems SHALL achieve a target error rate of no more than one in 10,000,000 ballot positions, with a maximum acceptable error rate in the test process of one in 500,000 ballot positions.	For telecommunications, if TCP/IP protocols are used all transmissions are guaranteed to be accurate. The discussion of one in ten million and one in half a million is somewhat obfuscated, the requirement should be more clearly defined.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
2.1.5 Accuracy Test Content	Voting system accuracy SHALL be verified by a specific test conducted for this objective. The overall test approach is described in Appendix C.	For a true internet voting system, that uses a web browser implementation for capturing votes, the accuracy test is whether or not the election is coded correctly. The technologies involved are mature, proven and robust. For a true internet voting system that employs physical devices such as a touch screen, the accuracy test would be similar to that of a ballot delivery system, in that the touch screen is dependent on the prescribed maintenance cycle of the device. For a ballot delivery system, where the cast ballot is potentially returned in any of a number or ways (fax, email, printed/scanned), the accuracy is dependent on the device used, within the confines of the prescribed maintenance cycles of the device.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
2.1.5.1 Simulators	If a simulator is used, it SHALL be verified independently of the voting system in order to produce ballots as specified for the accuracy testing.	Not a voting system requirement.			
2.1.5.2 Ballots	Ballots used for accuracy testing SHALL include all the supported types (i.e., rotation, alternative languages) of contests and election types (primary, general).	Question as to the applicability of the ballot type to accuracy testing. Accuracy testing concerns itself with accuracy with regard to the scanning/ reading of each possible ballot position on a given size ballot. The ability of the system to correctly handle the various supported voting variations is addressed in other specific tests.			
2.1.6 Reporting Accuracy	Processing accuracy is defined as the ability of the voting system to process stored voting data. Processing includes all operations to consolidate voting data after the voting period has ended. The voting systems SHALL produce reports that are consistent, with no discrepancy among reports of voting data.	In general this is a bit high level, would like to see some specific metrics called out to ensure reporting accuracy. Similar v1.0 VVSG volume 1, sections 2.4.2. and 2.4.3.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
2.2.1 Maximum Capacities	The manufacturer SHALL specify at least the following maximum operating capacities for the voting system (i.e. server, vote capture device, tabulation device, and communications links): - Throughput - Memory - Transaction processing speed and - Election constraints: o Number of jurisdictions o Number of ballot styles per jurisdiction o Number of contests per ballot style o Number of candidates per contest o Number of voted ballots	Recommend that this section look at capacities more in terms of minimums that need to be met (as specified by NIST/FVAP), rather than as stated maximum capacities that a manufacturer claims they can accommodate. Many times a manufacturer will list an unrealistically high number for many of these categories. A minimum standard will create a consistent baseline for all manufacturers.			
2.2.1.1 Capacity testing	The voting system SHALL achieve the maximum operating capacities stated by the manufacturer in section 2.2.1.	Recommend making the Test Method for this item Inspection/Functional. Some instances can be impractical to functionally validate within a reasonable cost/benefit ratio.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
2.2.2 Operating Capacity notification	The voting system SHALL provide notice when any operating capacity is approaching its limit.	Recommend making the Test Method for this item Inspection/Functional. In some instances it can be impractical to functionally validate within a reasonable cost/benefit ratio.			
2.2.3 Simultaneous Transmissions	The voting system SHALL protect against the loss of votes due to simultaneous transmissions	Recommend making the Test Method for this item Inspection/Functional. In some instances it can be impractical to functionally validate within a reasonable cost/benefit ratio.		Recommend that the following guidance be referenced and followed. NIST SP800-52 provides guidance on protecting transmission integrity using TLS. Other NIST documents include SP800-81, 800-44, 800-45, 800-49, 800-57, 800-58, 800-66, 800-77 and 800-81. FIPS 198 also discusses transmission quality.	

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
2.3.1.1 Import the election definition	b. Provide the capability to import or manually enter ballot content, ballot instructions and election rules, including all required alternative language translations from each jurisdiction;	Enumerate the activities.		Recommend that all graphic file formats be tested for corruption from malformed packets. Known vulnerabilities exist with almost all graphic file formats. Appropriate patches to operating systems must be tested.	
2.3.1.2 Protect the election definition	The voting system SHALL provide a method to protect the election definition from unauthorized modification.			No recommendation. However, the requirement does not specify how this is to be accomplished.	
2.4.2 Casting a Ballot	The voting system SHALL: successfully accomplish sub-requirements a-I	There should be a sub-requirement that deals that the system allows the voter to change their selection within a contest prior to casting their ballot (similar to (g) for undervotes).			
2.4.2.1 Record voter selections	b. Record the voter's selection of candidates whose names do not appear on the ballot (if permitted under state law) and record as many write-ins as the number of candidates the voter is allowed to select;	Recommend splitting sub-requirement so that one validates the ability to enter a write-in, and the other verifies the correct number of write-ins is allowed.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
2.4.2.1 Record voter selections	f. Indicate to the voter when no selection, or an insufficient number of selections, has been made for a contest (e.g., undervotes);	Recommend that this requirement is made more specific by notifying the voter of potential undervote prior to casting the ballot (as opposed to when going from one contest (or screen) to another).			
2.4.2.1 Record voter selections	j. In the event of a failure of the main power supply external to the voting system, provide the capability for any voter who is voting at the time to complete casting a ballot, allow for the successful shutdown of the voting system without loss or degradation of the voting and audit data, allow voters resume voting once the voting system has reverted to backup power.	This may not be feasible in a remote session environment. Depending on where the power failure occurs, as well as the duration, will dictate if a ballot can be recorded within the voting system without loss or degradation of voting/audit data. The "… allow voters to resume voting… "clause would inherently cause some kind of voter data to be resident on the vote capture device, which would potentially violate other Security requirements (5.4.1.3).			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
2.4.2.2 Verify voter selections	a. Produce a paper record each time the confirmation screen is displayed;	Would recommend that a paper record is generated only when the ballot is cast and not each time the confirmation screen is accessed.			
2.4.2.2 Verify voter selections	c. Allow the voter to either cast the ballot or return to the vote selection process to make changes after reviewing the confirmation screen and paper record; and	Recommend removing "… and paper record", see comment to "a" above.			
2.4.2.3 Cast ballot	The voting system SHALL:	Recommend renaming requirement to "Post Cast Ballot Process."			
2.4.2.3 Cast ballot	b. Notify the voter after the vote has been stored persistently that the ballot has been cast;	Recommend defining "persistently" in more detail. In a full electronic system, "persistently" would indicate that the central server has received the vote record and stored it. In a ballot delivery system, "persistently" would indicate the printing of a physical ballot, or creation of a pdf.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
2.4.2.3 Cast ballot	c. Notify the voter that the ballot has not been cast successfully if it is not stored successfully, and provide clear instruction as to the steps the voter should take in order to cast his ballot should this event occur; and	Recommend enumerating this requirement to c.i and c.ii			
2.4.3.1 Link to voter	The voting system SHALL be capable of producing a cast vote record that does not contain any information that would link the record to the voter	In the Glossary, cast vote record needs a better definition, so that it is differentiated from the cast ballot more explicitly. It should indicate that it is the record stored in the voting system, as opposed to the cast ballot that is produced by the vote capture device. In the Absentee model the cast ballot contains links to the voter's identity, where the cast vote record should not.			
2.4.3.2 Voting session records	The voting system SHALL NOT store any information related to the actions performed by the voter during the voting session.	Audit logs would record when the voter accessed the ballot, as well as when they cast the ballot, but no information would be stored that would link information to individual voter			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
2.5.1 Ballot Box Retrieval and Tabulation		An additional requirement is recommended that explicitly deal with the encryption of the electronic ballot box upon closure of the voting period, in order to prevent voter data (private information and vote data) from being exposed in even a read only manner. "Seal" in 2.5.1.1 may be used to cover this concept. But then should be broken out to a separate requirement from the "sign."			
2.5.1.1 Seal and sign the electronic ballot box	The voting system SHALL seal and sign each jurisdiction's electronic ballot box, by means of a digital signature, to protect the integrity of its contents.	Recommend that the term "seal" be more explicitly defined. "Seal" is historically more of a physical concept, whereas in this instance it is a logical concept. May want to define as making the electronic ballot box "read only," with a corresponding time stamp or something similar.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
2.5.1.3 Electronic ballot box integrity check	The voting system SHALL perform an integrity check on the electronic ballot box verifying that it has not been tampered with or modified before opening.	See comments in 2.5.1 and 2.5.1.1, as would pertain to this requirement.			
2.5.2.1 Tabulation device connectivity	The tabulation device SHALL be physically, electrically, and electromagnetically isolated from any other computer network.	Enumerate the activities.			
2.5.2.2 Open ballot box	The tabulation device SHALL allow only an authorized entity to open the ballot box.	Recommend adding "voting system" in front of "authorized entity."			
2.5.2.3.1 Adjudication	The tabulation device SHALL allow the designation of electronic ballots as “accepted” or “not accepted” by an authorized entity.	1) See comment in 2.5.2.2 2) "Electronic ballots" is not a defined term. Recommend using the term "Cast Ballot."			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
2.5.2.4 Ballot decryption	The tabulation device decryption process SHALL remove all layers of encryption, breaking all correlation between the voter and the ballot, and thus producing a record that is in clear text.	Decryption process may be different than what is used to break all correlations between the voter and the ballot. This requirement should be broken out. The breaking of the correlation should only be done after the adjudication is completed. The decryption process may be involved at multiple points of this overall process.			
2.6 Audit and Accountability		Assumption is that 2.6.1 and 2.6.2 are "header" sections that should not have any actionable events. The "Shall" in 2.6.2 should be removed.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
2.6.2 Electronic Records	In order to support independent auditing, a voting system SHALL be able to produce electronic records that contain the necessary information in a secure and usable manner. Typically, this includes records such as: - Vote counts - Counts of ballots recorded - Paper record identifier - Event logs and other records of important events- Election archive information	1) Recommend using appropriate NIST standard, and/or VVSG section 2.1.5, in place of "secure and usable manner." 2) Recommend removing "Typically", and rephrasing to something similar to, "this includes, but is not limited to:" 3) Enumerate bullets so they are referenceable. 4) Remove "Shall" as it causes need for actionable event. Recommend more explicitly defining "important events."			
2.6.2 Electronic Records	The following requirements apply to records produced by the voting system for any exchange of information between devices, support of auditing procedures, or reporting of final results:	Enumerate in relation to above subsection.			
2.6.2 Electronic Records	a. Requirements for electronic records to be produced by tabulation devices; and b. Requirements for printed reports to support auditing steps.	The pertinent requirements associated to this sub requirement should be explicitly called out. A vague reference will only create gaps in coverage.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
2.6.2.2 Ballot images	The voting system SHALL have the capability to generate ballot images in a human readable format.			Recommend that all graphic file formats be tested for corruption from malformed packets. Known vulnerabilities exist with almost all graphic file formats. Appropriate patches to operating systems must be tested.	
2.6.2.3 Ballot image content	The voting system SHALL be capable of producing a ballot image that includes:	Does this requirement need a complementary requirement, similar to how 2.6.3.2 has 2.6.3.3 Privacy?		Recommend that all graphic file formats be tested for corruption from malformed packets. Known vulnerabilities exist with almost all graphic file formats. Appropriate patches to operating systems must be tested.	
2.6.2.4 All records capable of being printed	The tabulation device SHALL provide the ability to produce printed forms of its electronic records. The printed forms SHALL retain all required information as specified for each record type other than digital signatures.	Should be enumerated or split out.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
2.6.3 Paper Records	The vote capture device is required to produce a paper record for each ballot cast. This record SHALL be available to the voter to review and verify, and SHALL be retained for later auditing or recounts, as specified by state law. Paper records provide an independent record of the voter's choices that can be used to verify the correctness of the electronic record created by the vote capture device.	Need to remove "Shall" from header.			
2.6.3.2 Paper record contents	Each paper record SHALL contain at least:	2.6.2.3 and 2.6.3.2 test for the same thing, but one is a Test Method Inspection and the other is a Functional. These should be consistent. Recommend making both Inspections.			
2.6.3.4 Multiple pages	When a single paper record spans multiple pages, each page SHALL include the voting location, ballot style, date of election, and page number and total number of the pages (e.g., page 1 of 4).	Enumerate the activities.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
2.6.3.7 Linking the electronic CVR to the paper record	b. Identify whether the paper record represents the ballot that was cast.	Recommend replacing "Identify" with "Validates."			
2.7.1.1 Network monitoring	The system server SHALL provide for system and network monitoring during the voting period.	More detail should be added as to what level of monitoring should be taking place. This could be as minimal as, "the light is green, and the system is up."		Recommend that IDS/IPS system(s) SHALL be used that actively monitors, detects, and notifies system administrators of any potential malicious activity.	
3.2.2 Cognitive Issues	a. The vote capture device SHALL provide instructions for all its valid operations.				It is recommended that either requirement 3.2.2-a be modified to specifically mention accessibility features as valid system operations that require instructions, or that an additional requirement discussing this topic be added to the UPPTR.

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
3.2.2 Cognitive Issues	e. The voting system SHALL provide the capability to design a ballot with a high level of clarity and comprehensibility. ii. The ballot SHALL clearly indicate the maximum number of candidates for which one can vote within a single contest.				It is recommended that requirement 3.2.2-e(ii) be deleted from Section 3 of the UPPTR, as it pertains to ballots and not the voting system.

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
3.3.7 Cognition	These requirements specify the features of the accessible voting station designed to assist voters with cognitive disabilities. a. The accessible voting station should provide support to voters with cognitive disabilities.				It is recommended that specific, testable requirements be adapted from available resources and added to subsection 3.3.7 of the UPPTR. These requirements may detail features such as: consistent navigation (placement, display, and functionality); avoidance of unnecessary time-outs or short time limits; confirmation features for correctly casting the ballot; and alerts for users to errors or possible errors.

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.1 Access Control	This section states requirements for the identification of authorized system users, processes and devices and the authentication or verification of those identities as a prerequisite to granting access to system processes and data. It also includes requirements to limit and control access to critical system components to protect system and data integrity, availability, confidentiality, and accountability. This section applies to all entities attempting to physically enter voting system facilities or to request services or data from the voting system.	Manufacturer shall clearly define what level users, roles and groups are defined on, whether that be at the operating system or the voting system level.			
5.1.1.1 Definition of roles	The voting system SHALL allow the definition of personnel roles with segregated duties and responsibilities on critical processes to prevent a single person from compromising the integrity of the system.		Specific roles should be defined to facilitate true segregation of duties.	Recommend the use of application scanning tools such as Fortify 360, Nessus, Lumension etc. to identify source code vulnerabilities.	

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.1.1.2 Access to election data	The voting system SHALL ensure that only authorized roles, groups, or individuals have access to election data.			Recommend the use of application scanning tools such as Fortify 360, Nessus, Lumension etc. to identify source code vulnerabilities.	
5.1.1.3 Separation of duties	The voting system SHALL require at least two persons from a predefined group for validating the election configuration information, accessing the cast vote records and starting the tabulation process.	Enumerate the activities.		Recommend that passwords conform to DOD minimum requirements.	
5.1.2 Voting System Access	The voting system SHALL provide access control mechanisms designed to permit authorized access and to prevent unauthorized access to the system.	"SHALL" should be removed, as it designates an actionable item. The header of a section is validated when all of its sub requirements are validated.	This requirement does not define at what minimum level this security should be implemented.		
5.1.2.1 Identity verification	The voting system SHALL identify and authenticate each person, to whom access is granted, and the specific functions and data to which each person holds authorized access.	This requirement should be split out. It covers both authentication and authorization.	This requirement does not define at what minimum level this security should be implemented.		

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.1.2.2 Access control configuration	The voting system SHALL allow the administrator group or role to configure permissions and functionality for each identity, group or role to include account and group/role creation, modification, and deletion.	Enumerate the activities.	This requirement does not state whether this should be a system OS level or at a web based administration application level.		
5.1.2.5 Operating system privileged account restriction	The voting system SHALL NOT require its execution as an operating system privileged account and SHALL NOT require the use of an operating system privileged account for its operation.	Should enumerate the activities.			
5.1.2.6 Logging of account	The voting system SHALL log the identification of all personnel accessing or attempting to access the voting system to the system event log.	This is tested in 5.6.3.3.	This requirement does not define what information should be logged.		

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.1.2.7 Monitoring voting system access	The ((voting system)) SHALL provide tools ((or shall be provided)) for monitoring access to the system. These tools SHALL provide specific users real time display of persons accessing the system as well as reports from logs.	Should enumerate the activities. Concern for this requirement is if it is realistically feasible to monitor a globally distributed system, with potentially a very large set of users.	This requirement does not define what information should be logged. This requirement also does not state if the tool is to be accessible via the Web based administration application or at an OS Level.		
5.1.2.8 Login failures	The vote capture devices at the kiosk locations and the central server SHALL have the capability to restrict access to the voting system after a preset number of login failures.	1) "SHALL" should be removed, as it designates an actionable item. The header of a section is validated when all of its sub requirements are validated. 2) Enumerate activities. 3) This requirement is too specific, should use the term "voting system" so that all areas are covered.	This requirement does not define if this needs to be at a Web application level or at OS level. Reactivation of an account should not require utilization of anything but the web-based application.		
5.1.2.8 Login failures	b. The voting system SHALL log the event.	Covered in 5.6.3.3.			
5.1.2.9 Account lockout logging	The voting system SHALL log a notification when any account has been locked out.	Covered in 5.6.3.3.	This requirement does not define what information should be logged.		

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.1.2.10 Session timeout	Authenticated sessions on critical processes SHALL have an inactivity time-out control that will require personnel re-authentication when reached. This time-out SHALL be implemented for administration and monitor consoles on all voting system devices.	Enumerate activities.	This requirement does not define how this function should be configured.		
5.1.2.11 Screen lock	Authenticated sessions on critical processes SHALL have a screen-lock functionality that can be manually invoked.	Should mention need for re-authentication in order to re-access.			
5.2.1.1 Strength of authentication	Authentication mechanisms supported by the voting system SHALL support authentication strength of at least 1/1,000,000.	This should be referring to appropriate NIST SP, NIST 800-63 Electronic Authentication Guideline Standards.			
5.2.1.2 Minimum authentication methods	Voter Not required	Assuming voter authentication is performed "outside" the scope of the voting system, by kiosk worker/ Election Official.			
5.2.1.3 Multiple Authentication mechanisms	The voting system SHALL provide multiple authentication methods to support multifactor authentication.		This requirement does not define what minimum level is required.		

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.2.1.5 Password reset	The voting system SHALL provide a mechanism to reset a password if it is forgotten, in accordance with the system access/security policy.	Covers passwords only. What if there are alternative methods of authentication?	This requirement does not define if this function is to be web-based.		
5.2.1.6 Password strength configuration	The voting system SHALL allow the administrator group or role to specify password strength for all accounts including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters per NIST 800-63 Electronic Authentication Guideline Standards.	Should specify the authentication level as defined in reference NIST SP.	This requirement does not define if this configuration is to be web-based or OS configurable.		
5.2.1.7 Password history configuration	The voting system SHALL enforce password histories and allow the administrator to configure the history length when passwords are stored by the system. NIST Special Publication 800-57		This requirement does not define if this configuration is to be web-based or OS configurable.		

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.2.1.10 Device authentication	The voting system servers and vote capture devices SHALL identify and authenticate one another using NIST - approved cryptographic authentication methods at the 112 bits of security.	Tested in 5.3.1.2.	This requirement does not define which NIST standard or level to use.		
5.2.1.11 Network authentication	Remote voting location site Virtual Private Network (VPN) connections (i.e., vote capture devices) to voting servers SHALL be authenticated using strong mutual cryptographic authentication at the 112 bits of security. Cannot be fully verified in lab; Testing at remote voting location(s) at operational Level.	Tested in 5.3.1.2.			
5.2.1.12 Message authentication	Message authentication SHALL be used for applications to protect the integrity of the message content using a schema with 112 bits of security.	1) Need to define what a "message" is. 2) Tested in 5.3.1.2.		Recommend that authentication schema SHALL be commensurate with the highest level technically feasible, as this will constantly change as new schemas become available.	

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.2.1.13 Message authentication mechanisms	IPsec, SSL, or TLS and MAC mechanisms SHALL all be configured to be compliant with FIPS 140-2 using approved algorithm suites and protocols.	1) Is the intent here to use current certified communication methodologies? If so, would be better suited as an Inspection test method. 2) Tested in 5.3.1.1 and 5.3.1.3 and 5.3.2.4.			
5.3 Cryptography		1) "SHALL" should be removed, as it designates an actionable item. The header of a section is validated when all of its sub requirements are validated. 2) Note quantify "Strong Authentication," this term is too vague, should reference a standard.			
5.3.1 General Cryptography Requirements		This section needs additional requirements that handle the situation of keys purchase from a Certificate Authority.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.3.1.1 Cryptographic functionality	All cryptographic functionality SHALL be implemented using NIST-approved cryptographic algorithms/ schemas, or use published and credible cryptographic algorithms/ schemas/ protocols	"… or use published and credible cryptographic algorithms / schemas/ protocols " is something that should be qualified by FVAP/NIST. The preference is to not leave it to a VSTL to determine, or to leave it as a loophole for a manufacturer to argue.	This requirement does not define what minimum NIST level is required.		
5.3.1.2 Required security strength	Cryptographic algorithms and schemas SHALL be implemented with a security strength equivalent to at least 112 bits of security to protect sensitive voting information and election records.			Recommend that authentication schema SHALL be commensurate with the highest level technically feasible, as this will constantly change as new schemas become available.	
5.3.1.3 Use NIST-approved cryptography for communications	Cryptography used to protect information in-transit over public telecommunication networks SHALL use NIST-approved algorithms and cipher suites. In addition the implementations of these algorithms SHALL be NIST-approved (Cryptographic Algorithm Validation Program).	These requirements should be split out to discrete items.	This requirement does not define which NIST standard or level to use.		

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.3.2.1 Key generation methods	Cryptographic keys generated by the voting system SHALL use a NIST-approved key generation method, or a published and credible key generation method.	See comment on 5.3.1.1, as it is applicable here as well.	This requirement does not define which NIST standard or level to use.		
5.3.2.3 Seed values	If a seed key is entered during the key generation process, entry of the key SHALL meet the key entry requirements in 5.3.3.1. If intermediate key generation values are output from the cryptographic module, the values SHALL be output either in encrypted form or under split knowledge procedures.	These requirements should be split out to discrete items.			
5.3.2.4 Use NIST-approved key generation methods for communications	Cryptographic keys used to protect information in-transit over public telecommunication networks SHALL use NIST-approved key generation methods. If the approved key generation method requires input from a random number generator, then an approved (FIPS 140-2) random number generator SHALL be used.	1) These requirements should be split out to discrete items. 2) Unless key is purchased from a Certificate Authority.	This requirement does not define which NIST standard or level to use.		

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.3.4.1 Key storage	Cryptographic keys stored within the voting system SHALL NOT be stored in plaintext. Keys stored outside the voting system SHALL be protected from disclosure or modification.	These requirements should be split out to discrete items.			
5.3.4.3 Support for rekeying	The voting system SHALL support the capability to reset cryptographic keys to new values.	What is the acceptable level of effort to reset the cryptographic keys to new values? Is it acceptable to have to redefine the election? Or should the jurisdiction be able to just replace the keys.			
5.4 Voting System Integrity Management	This section addresses the secure deployment and operation of the voting system, including the protection of removable media and protection against malicious software.	Would work better to have 5.4.1 be specific to vote capture devices, then have a section 5.4.2 that pertains to vote capture devices and ballot delivery systems.			
5.4.1 Protecting the Integrity of the Voting System		May need an additional requirement for nonrepudiation issues.			
5.4.1.4 Electronic ballot box integrity	The integrity and authenticity of the electronic ballot box SHALL be protected by means of a digital signature.	Additional detailed definition of "electronic ballot box" is needed.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.4.1.5 Malware detection	The voting system SHALL use malware detection software to protect against known malware that targets the operating system, services, and applications	More definition is needed to quantify the level of protection needed. Potentially a hardware/software malware detection solution, instead of just software.			
5.4.1.6 Updating malware detection	The voting system SHALL provide a mechanism for updating malware detection signatures.	A follow on requirement to this one would be to have the manufacturer specify in their documentation (i.e. an Inspection test method) the recommend interval for requiring updated signatures.			
5.4.1.7 Validating software on kiosk voting devices	The voting system SHALL provide the capability for kiosk workers to validate the software used on the vote capture devices as part of the daily initiation of kiosk operations.	This requirement needs to be expanded to cover all associated devices at the kiosk location. Some systems contain additional devices.			
5.5 Communications Security	This section provides requirements for communications security. These requirements address ensuring the integrity of transmitted information and protecting the voting system from external communications-based threats	Some of the requirements in this section appear to explicitly call out specific communication protocols, which could be interpreted to exclude all other like communication protocols.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.5.1.1 Data integrity protection	Voting systems that transmit data over communications links SHALL provide integrity protection for data in transit through the generation of integrity data (digital signatures and/or message authentication codes) for outbound traffic and verification of the integrity data for inbound traffic.	Recommend that this requirement be broken out to handle outbound versus inbound separately.			
5.5.1.3 Virtual private networks (VPN)	Voting systems deploying VPNs SHALL configure them to only allow FIPS-compliant cryptographic algorithms and cipher suites.	Tested in 5.3.1.1 and 5.3.1.3. As this appears to be a specific instance of the above mentioned requirements, recommend removing in order to reduce redundancy.			
5.5.1.5 Mutual authentication required	Each device SHALL mutually strongly authenticate using the system identifier before additional network data packets are processed.	Recommend referencing appropriate NIST publication (SP 800-63) to more clearly define "mutually strongly authenticate."			
5.5.1.6 Secrecy of ballot data	Data transmission SHALL preserve the secrecy of voters' ballot selections and SHALL prevent the violation of ballot secrecy and integrity.	1) This requirement should be split out. 2) Recommend more clearly stating that voter data is to be encrypted. "Preserve the secrecy …" creates ambiguity.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.5.2 External Threats	Voting systems SHALL implement protections against external threats to which the system may be susceptible.	"SHALL" should be removed from header.			
5.5.2.2 Minimizing interfaces	The number of active ports and associated network services and protocols SHALL be restricted to the minimum required for the voting system to function.	Need to define test method "Inspection/ Vulnerability."			
5.5.2.3 Prevention of attacks and security noncompliance	The voting system SHALL block all network connections that are not over a mutually authenticated channel.	Make this 5.5.2.4 need to define test method "Functional/ Vulnerability."			
5.6.1.1 Default settings	The voting system SHALL implement default settings for secure log management activities, including log generation, transmission, storage, analysis, and disposal.	1) This should be split to more discrete sub requirements. 2) term "default settings" is ambiguous, should require "minimal settings" as per NIST SP 800-92.			
5.6.1.2 Log access	Logs SHALL only be accessible to authorized roles.	Term "authorized roles" is undefined within the requirements. This should be more clearly defined.			
5.6.1.3 Log access	The voting system SHALL restrict log access to append-only for privileged logging processes and read-only for authorized roles.	Term "privileged logging processes" is undefined within the requirements. This should be more clearly defined.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.6.1.4 Logging events	The voting system SHALL log logging failures, log clearing, and log rotation.	This should be split out to discrete 3 sub-requirements.	This requirement does not specify if these logs should contain both voter and administration information.		
5.6.1.5 Log format	The voting system SHALL store log data in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format.		This requirement does not determine if these functions should be part of an administration web based application or at an OS level administration function.		
5.6.1.6 Log separation	The voting system SHALL ensure that each jurisdiction's event logs and each component's logs are separable from each other.	This should be split out to discrete 2 sub-requirements.			
5.6.1.7 Log review	The voting system SHALL include an application or program to view, analyze, and search event logs.	This should be split out to 3 discrete sub-requirements.	This requirement does not determine if these functions should be part of an administration web based application or at an OS level administration function.		

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.6.1.8 Log preservation	All logs SHALL be preserved in a useable manner prior to voting system decommissioning.	Term "prior to voting system decommissioning" is ambiguous. We believe the intent is that the log data remains intact for the life cycle of the given election data for a particular election. This may be defined at the jurisdictional level.			
5.6.1.9 Voter privacy	Logs SHALL NOT contain any data that could violate the privacy of the voter's identity.		This requirement does not outline what information is deemed to violate a voter's identity.		
5.6.1.12 System clock security	Only the system administrator SHALL be permitted to set the system clock.	Would recommend that the "system administrator" role be changed to indicate an appropriately authorized election official.			
5.6.2.1 General	All communications actions SHALL be logged.		This requirement does not define what all communications encompasses.		
5.6.2.2 Log content	The communications log SHALL contain at least the following entries:	1) Enumerate, not using bullets, must be able to explicitly reference. 2) Similar to 5.6.3.1, test method should be Inspection.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.6.3.2 Critical events	All critical events SHALL be recorded in the system event log.	Define a critical event. The requirement as it is now leaves room for interpretation in regards to the scope of the requirement.	This requirement does not define what a critical event might be.		
5.6.3.3 System events	At a minimum the voting system SHALL log the events described in Table 5-2. (The contents of the table appear in this list under the 5.6.3.3 heading)	This section would be better served broken out into subparagraphs. Referencing back to a row or a bullet in a cell many times is problematic. Additionally the requirement only states "voting system" this is a broad scope of equipment and software. Does this apply to the O/S, the voting system application or both? General comment for this table would be to recommend that the term "include but not limited to" be avoided, as this creates ambiguity and a potential for inconsistent interpretation of the requirement.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.6.3.3.a1 Error and exception messages	The source and disposition of system interrupts resulting in entry into exception handling routines.	System interrupts at an operating system / hardware level could be potentially destructive. Source code can be analyzed for an understanding of exception handling routines then a script can be written to invoke a system interruption that would result in an entry into exception handling routines.			
5.6.3.3.a4	Notification of physical violations of security.	The term "physical violations of security" needs to be better defined as to what is included. (i.e. computer room security, motion sensors, chassis alarms, etc.)			
5.6.3.3.a6	All faults and the recovery actions taken.	The term "fault" is ambiguous, needs to be more clearly defined.			
5.6.3.3.a7	Error and exception messages such as ordinary timer system interrupts and normal I/O system interrupts do not need to be logged.	Define "ordinary," and seems to be in conflict with bullet 2.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.6.3.3.b Critical system status messages.	Critical system status messages other than information messages displayed by the device during the course of normal operations. Includes but not limited to: • Diagnostic and status messages upon startup. • The “zero totals” check conducted before opening the voting location.	1) More detail/criteria are needed to define what is considered critical. This may vary from system to system. 2)"Includes but not limited to" creates a large potential for gaps to occur, as well as disagreements by a manufacturer as to what is deemed critical.			
5.6.3.3.c Noncritical status messages	Non-critical status messages that are generated by the data quality monitor or by software and hardware condition monitors.	1) Need better criteria for determining what is noncritical versus what are critical status messages. 2) Need clarification as to what is meant by "data quality monitor." This term seems to be very subjective and open to interpretation. Likely to cause significant disagreement as to what is.			
5.6.3.3.e Shutdown and restarts	Both normal and abnormal shutdowns and restarts.	Recommend adding "Power up" to this line item.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.6.3.3.f Changes to system configuration settings	Changes to system configuration settings - Configuration settings include but are not limited to registry keys, kernel settings, logging settings, and other system configuration settings.	Recommend additional specificity , rather than alluding to "other system configuration settings"			
5.6.3.3.g Integrity checks for executables, configuration files, data and logs	Integrity checks that may indicate possible tampering with files and data.	Should explicitly call out "logs" in description.			
5.6.3.3.h The addition and deletion of files	Files added or deleted from the system.	Recommend additional detail as to file types. Would not recommend having to track temporary files that are automatically handled within the system.			
5.6.3.3.m3	All access attempts to application and underlying system resources.	Recommend removal of "…and underlying system resources", as this is beyond the scope of the voting system applications logging scope.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.6.3.3.o Installation, upgrading, patching, or modification of software or firmware	Logging for installation, upgrading, patching, or modification of software or firmware include logging what was installed, upgraded, or modified as well as a cryptographic hash or other secure identifier of the old and new versions of the data.	1) This line item needs to be explicitly broken out into individual requirements. The potential scope is very large. In an initial certification, upgrading/ patching/ modification may not be available. 2) "Cryptographic hash" needs to be defined. Recommend using "hash code" instead.			
5.6.3.3.p1 Changes to configuration settings	Includes but not limited to: Changes to critical function settings. At a minimum critical function settings include location of ballot definition file, contents of the ballot definition file, vote reporting, location of logs, and system configuration settings.	This requirement should be split out to more explicitly address either voting system applications or the underlying operating system.			
5.6.3.3.p2	Changes to settings including but are not limited to enabling and disabling services.	This requirement should be split out to more explicitly address either voting system applications or the underlying operating system.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.6.3.3.p3	Starting and stopping processes.	This requirement should be split out to more explicitly address either voting system applications or the underlying operating system.			
5.6.3.3.s Changes to cryptographic keys	At a minimum critical cryptographic setting include key addition, key removal, and rekeying.	Recommend adding "key zeroization."			
5.6.3.3.t1 Voting events	Voting events include: Opening and closing the voting period.	Recommend including successful delivery of appropriate ballot style to the voter.			
5.7.1.1 Critical events	Manufacturers SHALL document what types of system operations or security events (e.g., failure of critical component, detection of malicious code, unauthorized access to restricted data) are classified as critical.	1) Recommend that NIST/FVAP list minimum criteria of what should be classified as critical, in order to create a consistency for this requirement. 2) Recommend removal of "e.g." and giving specific criteria that must be met, as in 1) above.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.8 Physical and Environmental Security		Recommend that additional specificity is added to explicitly call out whether each requirement is for the voting system (election creation machines and accumulation/tallying central servers included), or just the vote capture device.			
5.8.2.1 Non-essential ports	The voting system SHALL disable physical ports and access points that are not essential to voting operations, testing, and auditing.	Recommend that "testing" be removed. In a production environment, do not want "test" ports/access points enabled.			
5.8.3.1 Physical port shutdown requirement	If a physical connection between the vote capture device and a component is broken, the affected vote capture device port SHALL be automatically disabled.	Recommend changing Test Method to Functional.			
5.8.3.2 Physical component alarm requirement	The voting system SHALL produce a visual alarm if a connected component is physically disconnected.	Recommend changing Test Method to Functional.			
5.8.3.4 Physical port enablement requirement	Disabled ports SHALL only be re-enabled by authorized administrators.	Recommend changing Test Method to Functional.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.8.3.5 Physical port restriction requirement	Vote capture devices SHALL be designed with the capability to restrict physical access to voting device ports that accommodate removable media with the exception of ports used to activate a voting session.	If implementing with custom designed vote capture device this requirement is applicable. If implementing with COTS products, this would not be applicable.			
5.8.3.6 Physical port tamper evidence requirement	Vote capture devices SHALL be designed to give a physical indication of tampering or unauthorized access to ports and all other access points, if used as described in the manufacturer's documentation.	If implementing with custom designed vote capture device this requirement is applicable. If implementing with COTS products, this would not be applicable.			
5.8.3.7 Physical port disability capability requirement	Vote capture devices SHALL be designed such that physical ports can be manually disabled by an authorized administrator.	If implementing with custom designed vote capture device this requirement is applicable. If implementing with COTS products, this would not be applicable.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.8.4.1 Access point Security requirement	Access points such as covers and panels SHALL be secured by locks or tamper evident or tamper resistant countermeasures and SHALL be implemented so that kiosk workers can monitor access to vote capture device components through these points.	Enumerate the activities.			
5.8.6.1	Voting equipment SHALL be designed with countermeasures that provide physical indication that unauthorized attempts have been made to access locks installed for security purposes.	If implementing with custom designed vote capture device this requirement is applicable. If implementing with COTS products, this would not be applicable.			
5.8.7 Media Protection	These requirements apply to all media, both paper and digital, that contain personal privacy related data or other protected or sensitive types of information.	Recommend changing "person privacy related data" to "personally identifiable information (PII)", which is a common industry term.			
5.9 Penetration Resistance		Recommend referencing NIST SP dealing with hardening.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.9.1.1 Resistant to attempts	The voting system SHALL be resistant to attempts to penetrate the system by any remote unauthorized entity.	Recommend defining resistant levels more definitively, and enumerating by device types within a voting system.			
5.9.1.2 System information disclosure	The voting system SHALL be configured to minimize ports, responses and information disclosure about the system while still providing appropriate functionality.	1) Recommend defining "appropriate functionality" by device types within a voting system. 2) Recommend referencing NIST SP dealing with hardening.			
5.9.1.3 System access	The voting system SHALL provide no access, information or services to unauthorized entities.	Enumerate the activities.			
5.9.1.4 Interfaces	All interfaces SHALL be penetration resistant including TCP/IP, wireless, and modems from any point in the system.	Recommend closing all ports and shutting down all services not needed to perform voting activities.			
5.9.2 Penetration Resistance Test and Evaluation		This section is oriented to the VSTL. As such it should not be in the requirements document that manufacturers are held to, but in a "Program Manual" that outlines the scope of a test plan to be created for the system to be tested			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.9.2.1 Scope	The scope of penetration testing SHALL include all the voting system components. The scope of penetration testing includes but is not limited to the following:	Define Test Method "Penetration" versus "Functional."			
5.9.2.2 Test environment	Penetration testing SHALL be conducted on a voting system set up in a controlled lab environment. Setup and configuration SHALL be conducted in accordance with the TDP, and SHALL replicate the real world environment in which the voting system will be used.	1) This requirement appears to be oriented to the VSTL not the manufacturer. 2) This may not be feasible for all systems. Have encountered systems that are cloud base, for example.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.9.2.3 White box testing	The penetration testing team SHALL conduct white box testing using manufacturer supplied documentation and voting system architecture information. Documentation includes the TDP and user documentation. The testing team SHALL have access to any relevant information regarding the voting system configuration. This includes, but is not limited to, network layout and Internet Protocol addresses for system devices and components. The testing team SHALL be provided any source code included in the TDP.	1) This requirement appears to be oriented to the VSTL, not the manufacturer. 2) The original text is not a definition of white box testing. 3) With added text, the source code review that would be required would be prohibitive from a cost/benefit viewpoint.			

Section	Requirement	VSTL Comments		Penetration Testing Comments	Operation Vote Comments
		SLI	Wyle		
5.9.2.4 Focus and priorities	Penetration testing seeks out vulnerabilities in the voting system that might be used to change the outcome of an election, interfere with voter ability to cast ballots, ballot counting, or compromise ballot secrecy. The penetration testing team SHALL prioritize testing efforts based on the following:	1) This requirement appears to be oriented to the VSTL, not the manufacturer.			
9.5.1.9 Open market procurement of COTS software	The software installation procedures SHALL specify that COTS software SHALL be obtained from the open market.			Recommend adoption of DoD guidance for erasable media.	