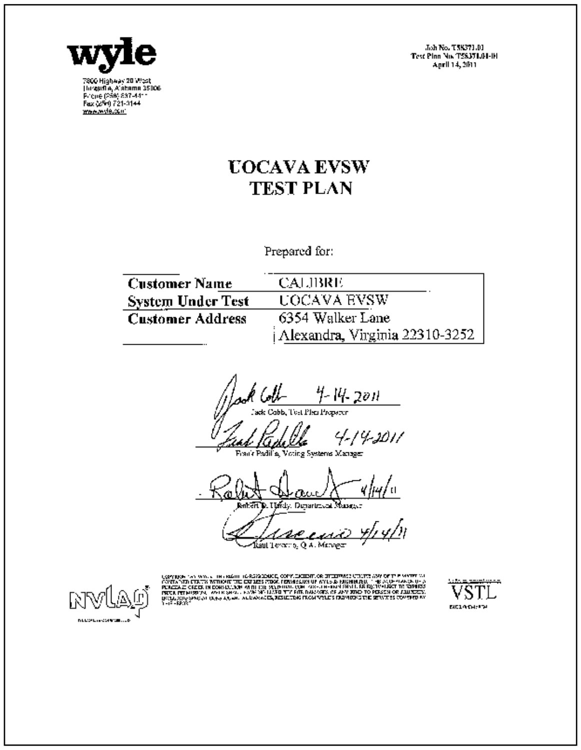
Appendix F – Wyle Laboratories Test Plan and Test Report



wyle

7800 Highway 20 West
Huntsville, Alabama 35806
Phone (256) 837-4411
Fax (256) 721-0144
www.wyle.com

Job No. T58371.01
Test Plan No. T58371.01-01
April 14, 2011

UOCAVA EVSW
TEST PLAN

Prepared for:

Customer Name	CALIBRE
System Under Test	UOCAVA EVSW
Customer Address	6354 Walker Lane Alexandra, Virginia 22310-3252

Jack Cobb 4-14-2011
Jack Cobb, Test Plan Preparer

Frank Padilla 4-14-2011
Frank Padilla, Voting Systems Manager

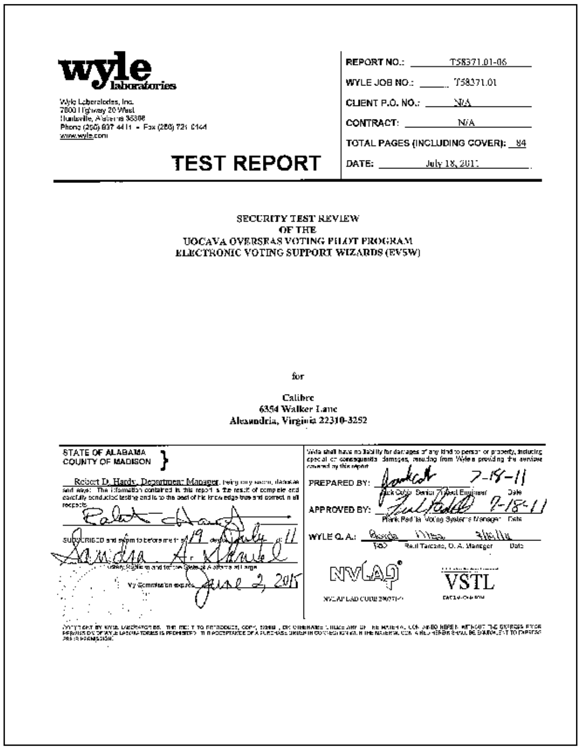
Robert Hardy 4/14/11
Robert D. Hardy, Department Manager

4/14/11
Raul Terceno, Q.A. Manager

NVLAP

COPYRIGHT BY WYLE. THE RIGHT TO REPRODUCE, COPY, EXHIBIT, OR OTHERWISE UTILIZE ANY OF THE MATERIAL CONTAINED HEREIN WITHOUT THE EXPRESS PRIOR PERMISSION OF WYLE IS PROHIBITED. THE ACCEPTANCE OF A PURCHASE ORDER IN CONNECTION WITH THE MATERIAL CONTAINED HEREIN SHALL BE EQUIVALENT TO EXPRESS PRIOR PERMISSION. WYLE SHALL HAVE NO LIABILITY FOR DAMAGES OF ANY KIND TO PERSON OR PROPERTY, INCLUDING SPECIAL OR CONSEQUENTIAL DAMAGES, RESULTING FROM WYLE'S PROVIDING THE SERVICES COVERED BY THIS REPORT.

VSTL



wyle laboratories

Wyle Laboratories, Inc.
7800 Highway 20 West
Huntsville, Alabama 35806
Phone (256) 837 4411 • Fax (256) 721 0144
www.wyle.com

TEST REPORT

REPORT NO.: T58371.01-06
WYLE JOB NO.: T58371.01
CLIENT P.O. NO.: N/A
CONTRACT: N/A
TOTAL PAGES (INCLUDING COVER): 84
DATE: July 18, 2011

SECURITY TEST REVIEW
OF THE
UOCAVA OVERSEAS VOTING PILOT PROGRAM
ELECTRONIC VOTING SUPPORT WIZARDS (EVSW)

for

Calibre
6354 Walker Lane
Aleaandria, Virginia 22310-3252

STATE OF ALABAMA
COUNTY OF MADISON }

Robert D. Hardy, Department Manager, being duly sworn, deposes and says: The information contained in this report is the result of complete and carefully conducted testing and is to the best of his knowledge true and correct in all respects.

Robert Hardy

SUBSCRIBED and sworn to before me this 19 day of July, 2011

Sandra A. Daniel
Notary Public in and for the State of Alabama at Large

My Commission expires June 2, 2015

Wyle shall have no liability for damages of any kind to person or property, including special or consequential damages, resulting from Wyle's providing the services covered by this report.

PREPARED BY: Jack Cobb 7-18-11
Jack Cobb, Senior Project Engineer Date

APPROVED BY: Frank Padilla 7-18-11
Frank Padilla, Voting Systems Manager Date

WYLE Q.A.: 7/18/11
Raul Terceno, Q.A. Manager Date

NVLAP

NVLAP LAB CODE 200771-0

VSTL

COPYRIGHT BY WYLE LABORATORIES. THE RIGHT TO REPRODUCE, COPY, EXHIBIT, OR OTHERWISE UTILIZE ANY OF THE MATERIAL CONTAINED HEREIN WITHOUT THE EXPRESS PRIOR PERMISSION OF WYLE LABORATORIES IS PROHIBITED. THE ACCEPTANCE OF A PURCHASE ORDER IN CONNECTION WITH THE MATERIAL CONTAINED HEREIN SHALL BE EQUIVALENT TO EXPRESS PRIOR PERMISSION.

wyle

7800 Highway 20 West
Huntsville, Alabama 35806
Phone (256) 837-4411
Fax (256) 721-0144
www.wyle.com

Job No. T58371.01
Test Plan No. T58371.01-01
April 14, 2011

UOCAVA EVSW
TEST PLAN

Prepared for:

Customer Name	CALIBRE
System Under Test	UOCAVA EVSW
Customer Address	6354 Walker Lane Alexandra, Virginia 22310-3252

Jack Cobb 4-14-2011
Jack Cobb, Test Plan Preparer

Frank Padilla 4-14-2011
Frank Padilla, Voting Systems Manager

Robert Hardy 4/14/11
Robert D. Hardy, Department Manager

4/14/11
Raul Terceno, Q.A. Manager

NVLAP®
NVLAP LAB CODE 200771-0

U.S. Election Assistance Commission
VSTL
EAC Lab Code 0704

Revisions

REV	DATE	PAGE OR PARAGRAPH AFFECTED	DESCRIPTION OF CHANGES
---	4-14-11	Entire Document	Original Release

TABLE OF CONTENTS

APPENDICES

1.0 INTRODUCTION

The purpose of this Test Plan is to document the procedures that Wyle will follow to perform testing of the Electronic Voting Support Wizards (EVSW) and the [redacted], to the security requirements set forth in Section 5 "Security" of the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements.

At test conclusion, the results of all testing performed as part of this test program will be submitted to the Federal Voter Assistance Program in the form of a final report.

1.1 References

The documents listed below were used in the development of the Test Plan and will be utilized to perform certification testing.

- Uniform and Overseas Citizens Absentee Voting Act Pilot Program Testing Requirements, August 25, 2010
- NIST 800-63 Electronic Authentication Guideline Standards
- Wyle Laboratories' Quality Assurance Program Manual, Revision 5
- ISO 10012-1, "Quality Assurance Requirements for Measuring Equipment"
- NIST SP800-57
- FIPS 140-2

A listing of the Technical Package Documents (TDP) submitted for this test effort is listed in Section 2.0 Deliverable Materials.

1.2 Terms and Abbreviations

Table 1-1 defines all terms and abbreviations applicable to the development of this Test Plan.

Table 1-1 Terms and Abbreviations

Term	Abbreviation	Definition
Commercial Off the Shelf	COTS	---
[redacted]	[redacted]	---
Election Management System	EMS	---
Equipment Under Test	EUT	---
Electronic Voting Support Wizards	EVSW	---
Federal Voter Assistance Program	FVAP	Government organization that provides U.S. citizens worldwide a broad range of non-partisan information and assistance to facilitate their participation in the democratic process.

1.0 INTRODUCTION (CONTINUED)

1.2 Terms and Abbreviations (continued)

Table 1-1 Terms and Abbreviations (continued)

Term	Abbreviation	Definition
Help America Vote Act	HAVA	Act created by United States Congress in 2002.
National Institute of Standards and Technology	NIST	Government organization created to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhances economic security and improves our quality of life.
Specimen Under Test	SUT	---
Technical Data Package	TDP	Manufacturer documentation related to the voting system required to be submitted as a precondition of certification testing.
Uniformed and Overseas Citizens Absentee Voting Act	UOCAVA	U.S. federal law dealing with elections and voting rights for the U.S. citizens residing overseas.
Voting System Test Laboratory	VSTL	EAC accredited third party test laboratory.
Wyle Operating Procedure	WoP	Wyle Test Method or Test Procedure

1.3 Testing Responsibilities

Wyle, an accredited VSTL, will test the EVSW and [redacted] as specified in this Test Plan. The testing will verify that the submitted systems conform to Section 5 of the UOCAVA Pilot Program Testing Requirements.

All testing will be conducted under the guidance of Wyle, by personnel verified by Wyle to be qualified to perform the testing.

1.3.1 Project Schedule

The following table provides the contractual dates agreement between FVAP and Wyle:

Deliverable	Time	Date
Start Date	---	March 21, 2011
Test Plan, Test Cases and Test Matrix Delivery	20 Days	April 18, 2011
Test Case Execution	30 Days	May 30, 2011
Test Report Submission	10 Days	June 13, 2011

1.0 INTRODUCTION (CONTINUED)

1.4 Target of Evaluation Description

This test campaign will evaluate two different types of systems: Electronic Voting Support Wizards (EVSW) and the [redacted]. The EVSW's are electronic ballot delivery systems. The scope for testing the EVSW's will be limited to the following:

- Verifying the voting system distributes the ballot only to the intended voter;
- The information on the ballot or about the voter cannot be accessed by unauthorized persons;
- The EVSW's meet the applicable requirements from Section 5 "Security" of the UOCAVA Pilot Program Testing Requirements.

Below is an illustration of the scope for these systems.

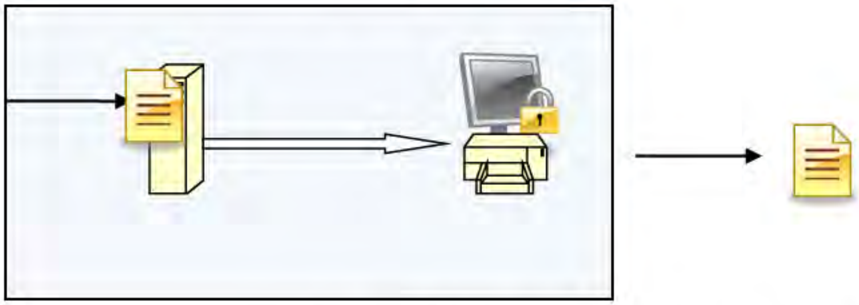


Figure 1-1 EVSW Ballot Delivery Illustration

This test campaign will include the following four EVSW's:

- [redacted]
- [redacted]
- [redacted]
- [redacted]

This test campaign also includes solutions for end-to-end voting remotely. These systems include voter registration, ballot delivery and voted ballot accumulation. The scope for testing these systems will verify supported functionality functions as designed and that the systems meet the applicable requirements from the UOCAVA Pilot Program Testing Requirements Section 5 Security. Below is an illustration from the UOCAVA Pilot Program Testing Requirements illustrating the scope for these systems.

1.0 INTRODUCTION (CONTINUED)

1.4 Target of Evaluation Description (continued)

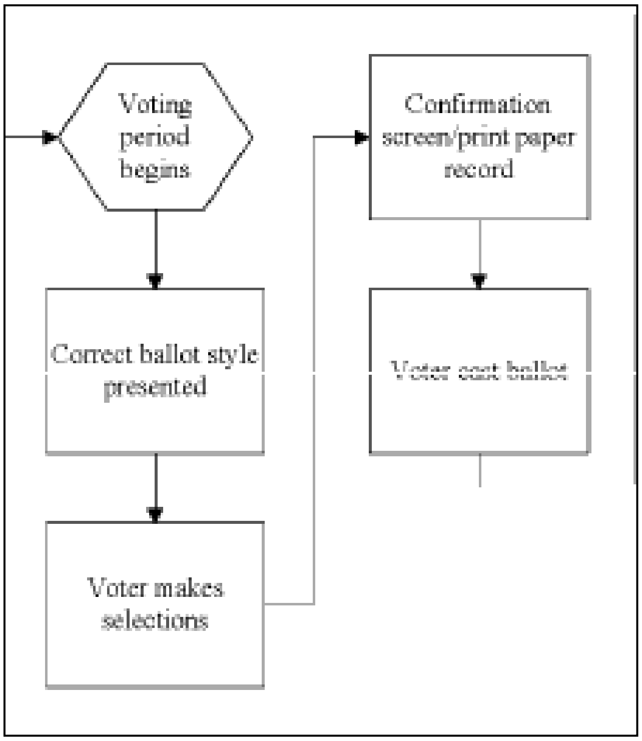

Voting period begins
Correct ballot style presented
Voter makes selections
Confirmation screen/print paper record
Voter cast ballot

Figure 1-1 [redacted] End-to-End System Illustration

This test campaign includes one end-to-end solution:

[redacted]

2.0 MATERIALS REQUIRED FOR TESTING

The materials required for this test campaign include test software and hardware as well as the system hardware and software. Some manufacturers submitted test systems consisting of preloaded software on manufacturer's hardware platforms in Wyle's control. Other manufacturers had live systems that Wyle only had remote access to. This hardware is not being documented in this section.

Table 2-1 Submitted Hardware and Software

Submitted System Under Test (SUT)	Hardware Platform
[redacted] UOCAVA Overseas Voting Server	Apple PowerPC G4 CPU
[redacted]Host Operating System	OS X version 10.5.8
[redacted] Host Software Environment	Ruby on Rails,

2.0 MATERIALS REQUIRED FOR TESTING (CONTINUED)

Table 2-2 Remote Hardware and Software

Remote System Under Test (SUT)	Hardware Platform
[redacted]	Microsoft Windows Azure Hosted Service
[redacted] Server	multi-node ESXi cluster virtual machines with
[redacted] Software	LAMP Platform (Linux, Apache, MySQL and Perl)
[redacted] Encryption Processor	Laptop
[redacted]	Information Requested from Vendor

Table 2-3 Documentation

Document Name	Document Version
[redacted] Elector User Guide	1.0.2
[redacted] User Manual	None
[redacted] FVAP Setup Notes	None
[redacted] FVAP Usage Notes	None
[redacted] Responses to RFI	None
[redacted] Online Help (document)	Dated 7/14/2010
[redacted] Privacy Policy	Dated July, 2010
[redacted] Administration User Doc.	Dated 9/21/2010
[redacted] Level Design and Architecture	1.0
[redacted] Security Overview	1.0
[redacted] System Functionality	None

Table 2-4 Test Equipment and Software

Equipment	Description	Serial Number
Client Terminal (Wyle Lab)	Dell Desktop Optiplex 780	40RYCP1
Client Terminal (Wyle Lab)	Dell Desktop Optiplex 780	40SWCP1
Client Software	Browser, Internet Explorer 8.0	N/A
Client Software	Browser, Safari 5.0.4	N/A

3.0 TEST SPECIFICATIONS

3.1 Requirements

The strategy for evaluating the documented systems described in Section 2 of this document is to divide the UOCAVA Section 5 requirements into three main test areas: functional, cryptographic, and penetration.. Wyle has determined this to be the most efficient and thorough approach. The individual requirements have been mapped to specific test cases in Appendix A "Requirements Matrix" for each system under test.

3.1.1 Functional Tests

The functional test area will focus on inspection, review and execution as the primary test methods. Individual test cases have been design using manufacturer's documentation, architectural documents and security specifications. These test cases are being submitted with this Test Plan as Appendix B. Each test case is defined with a written script. The test consists of executing each step of the script, recording observations and relevant data as each step completes. The date and time of the start and stop of each test will be recorded. At the end of each test, the test conductor will collect all log records and all input and output data.
As the test is conducted any unexpected conditions or incorrect actions will be recorded and any suspected malfunction will be recorded as an exception report and provided to the vendor. The test conductor will continue the test case unless the malfunction invalidates or prevents further testing.

The functional tests are designs to cover the requirements in the following sections of the UOCAVA Pilot Program Testing Requirements:

5.1 Access Control

5.2 Identification and Authentication

5.4 Voting System Integrity Management

5.5 Communication Security

5.6 Logging

5.7 Incident Response

3.1.2 Cryptographic Tests

The cryptographic test area will focus on inspection, review and execution as the primary test methods. All cryptography will be tested for functionality, strength and NIST compliance, no matter which one of the three purposes it serves in the voting system, Confidentiality, Authentication or Random Number Generation (RNG). Those systems that generate cryptographic keys internally will be tested for key management. This includes the generation method, security of the generation method, seed values and RNG health tests. Key establishment and handling will also be tested. Individual test cases have been designed using "Use Case" and verification. These test cases are being submitted with this Test Plan as Appendix C. These tests consist of executing each step while, recording observations and relevant data as each step completes.

3.0 TEST SPECIFICATIONS (CONTINUED)

3.1 Requirements (continued)

3.1.2 Cryptographic Tests (continued)

The cryptographic tests are designs to cover the requirements in the following sections:

5.3 Cryptography

3.1.3 Penetration Tests

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

The exploratory phase of the penetration test will have specific test cases designed and executed. These test cases are based on all information gathered during discovery, any subsequent observations made during the exploratory phase and any Rules Of Engagement (ROE) previously agreed upon by the Wyle and manufacturer.

The penetration tests are designs to cover the requirements in the following sections:

5.8 Physical and Environmental Security

5.9 Penetration Resistance

4.0 TEST DATA

4.1 Data Recording

All equipment utilized for test data recording shall be identified in the test data package. The output test data shall be recorded in an appropriate manner as to allow for data analysis. Additionally, all test results, including functional test data, shall be recorded on the relevant test execution log. Results shall also be recorded real-time in engineering log books.

4.2 Test Data Acceptance Criteria

Wyle shall evaluate all test results against the requirements set forth in Section 5 “Security” of the UOCAVA Pilot Program Testing Requirements. Each SUT shall be evaluated for its performance against the referenced requirements. The acceptable range for system performance and the expected results for each test case shall be derived from the system documentation.

4.0 TEST DATA (CONTINUED)

4.2 Test Data Acceptance Criteria

These parameters shall encompass the test tolerances, the minimum number of combinations or alternatives of input and output conditions that can be exercised to constitute an acceptable test of the parameters involved, and the maximum number of interrupts, halts or other system breaks that may occur due to non-test conditions (excluding events from which recovery occurs automatically or where a relevant status message is displayed).

5.0 TEST PROCEDURE AND CONDITIONS

This section describes Wyle's proposed test procedures and the conditions under which those tests shall be conducted. The following subsections describe test procedures and a statement of the criteria by which readiness and successful completion shall be indicated and measured.

5.1 Test Facilities

All testing shall be conducted at the Wyle, Huntsville, AL facility unless otherwise annotated. All instrumentation, measuring, and test equipment used in the performance of this test campaign shall be listed on the Instrumentation equipment Sheet for each test and shall be calibrated in accordance with Wyle Laboratories' Quality Assurance Program, which complies with the requirements of ANSI/NCSL Z540-1 and ISO 10012-1. Standards used in performing all calibrations are traceable to the National Institute of Standards and Technology (NIST) by report number and date. When no national standards exist, the standards are traceable to international standards or the basis for calibration is otherwise documented.
Unless otherwise specified herein, all remaining tests, including system level functional testing, shall be performed at standard ambient conditions:

• Temperature:	25°C ± 10°C (77°F ± 18°F)
• Relative Humidity:	20 to 90%
• Atmospheric Pressure:	Local Site Pressure

Unless otherwise specified herein, the following tolerances shall be used:

• Time	± 5%
• Temperature	± 3.6°F (2°C)
• Vibration Amplitude	± 10%
• Vibration Frequency	± 2%
• Random Vibration Acceleration	
20 to 500 Hertz	± 1.5 dB
500 to 2000 Hertz	± 3.0 dB
• Random Overall grms	± 1.5 dB

Deviations to the tolerances on Page No. 2 of 11 shall be submitted by the test responsible agency with sufficient engineering information to substantiate the deviation request, but only when best effort technique and system limitations indicate the need for a deviation.

5.0 TEST PROCEDURE AND CONDITIONS (CONTINUED)

5.2 Test Set-Up

All voting machine equipment (hardware and software), shall be received and documented utilizing Wyle Receiving Ticket (WL-218, Nov'85) and proper QA procedures. When voting system hardware is received, Wyle Laboratories Shipping and Receiving personnel shall notify Wyle Laboratories QA personnel. With Wyle Laboratories QA personnel present, each test article shall be unpacked and inspected for obvious signs of degradation and/or damage that may have occurred during transit. Noticeable degradation and/or damage, if present, shall be recorded, photographs shall be taken, and the manufacturer representative shall be notified.
Wyle Laboratories QA personnel shall record the serial numbers and part numbers. Comparison shall be made between those numbers recorded and those listed on the shipper's manifest. Any discrepancies noted shall be brought to the attention of the manufacturer representative for resolution.

TDP items, including all manuals, and all source code modules received shall be inventoried and maintained by the Wyle Laboratories Project Engineer assigned to testing.

For hardware test setup, the system shall be configured as it would be for normal field use. This includes connecting all supporting equipment and peripherals. Wyle personnel shall properly configure and initialize the system, and verify that it is ready to be tested. Wyle shall develop the system performance levels to be measured during operational tests.

5.3 Test Sequence

There is no required test sequence for this test campaign. All systems will be tested for each test area.

5.4 Test Operation Procedures

Wyle Laboratories shall provide the step-by-step procedures for each test case to be conducted. Each step is assigned a test step number and this number, along with critical test data and test procedures information, shall be tabulated onto a Test Control Record for control and the recording of test results.

Any test failures shall be recorded on WH1066, Notice of Anomaly form. These Anomalies shall be reported to the manufacturer.

APPENDIX A
REQUIREMENTS MATRIX

[redacted]

REQUIREMENTS MATRIX

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
Section 5	**Security**		
5.1	**Access Control**		
	This section states requirements for the identification of authorized system users, processes and devices and the authentication or verification of those identities as a prerequisite to granting access to system processes and data. It also includes requirements to limit and control access to critical system components to protect system and data integrity, availability, confidentiality, and accountability. This section applies to all entities attempting to physically enter voting system facilities or to request services or data from the voting system.		
5.1.1	**Separation of Duties**		
5.1.1.1	The voting system SHALL allow the definition of personnel roles with segregated duties and responsibilities on critical processes to prevent a single person from compromising the integrity of the system.	1	Host Server Administration Test Case
5.1.1.2	The voting system SHALL ensure that only authorized roles, groups, or individuals have access to election data.	1	Host Server Administration Test Case
5.1.1.3	The voting system SHALL require at least two persons from a predefined group for validating the election configuration information, accessing the cast vote records, and starting the tabulation process..	N/A	
5.1.2	**Voting System Access**		
	The voting system SHALL provide access control mechanisms designed to permit authorized access and to prevent unauthorized access to the system.	5	Discovery Penetration Test Case
		1	Host Server Administration Test Case
5.1.2.1	The voting system SHALL identify and authenticate each person, to whom access is granted, and the specific functions and data to which each person holds authorized access.	10	Local Ballot Delivery Test Case
		4	Normal Ballot Delivery Test Case
		1	Host Server Administration Test Case
5.1.2.2	The voting system SHALL allow the administrator group or role to configure permissions and functionality for each identity, group or role to include account and group/role creation, modification, and deletion.	1	Host Server Administration Test Case
5.1.2.3	The voting system's default access control permissions SHALL implement the least privileged role or group needed.	1	Host Server Administration Test Case
5.1.2.4	The voting system SHALL prevent a lower-privilege process from modifying a higher-privilege process.	1	Host Server Administration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.1.2.5	The voting system SHALL NOT require its execution as an operating system privileged account and SHALL NOT require the use of an operating system privileged account for its operation.	N/A	
5.1.2.6	The voting system SHALL log the identification of all personnel accessing or attempting to access the voting system to the system event log.	5	Discovery Penetration Test Case
		4	Normal Ballot Delivery Test Case
		1	Host Server Administration Test Case
		10	Local Ballot Delivery Test Case
5.1.2.7	The *(voting system)* SHALL provide tools for monitoring access to the system. These tools SHALL provide specific users real time display of persons accessing the system as well as reports from logs.	5	Discovery Penetration Test Case
		1	Host Server Administration Test Case
5.1.2.8	Vote capture device located at the remote voting location and the central server SHALL have the capability to restrict access to the voting system after a preset number of login failures. a. The lockout threshold SHALL be configurable by appropriate administrators/operators b. The voting system SHALL log the event c. The voting system SHALL immediately send a notification to appropriate administrators/operators of the event. d. The voting system SHALL provide a mechanism for the appropriate administrators/operators to reactivate the account after appropriate confirmation.	5	Discovery Penetration Test Case
		1	Host Server Administration Test Case
5.1.2.9	The voting system SHALL log a notification when any account has been locked out.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.1.2.10	Authenticated sessions on critical processes SHALL have an inactivity time-out control that will require personnel re-authentication when reached. This time-out SHALL be implemented for administration and monitor consoles on all voting system devices.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.1.2.11	Authenticated sessions on critical processes SHALL have a screen-lock functionality that can be manually invoked.	N/A	
5.2	**Identification and Authentication**		
	Authentication mechanisms and their associated strength may vary from one voting system capability and architecture to another but all must meet the minimum requirement to maintain integrity and trust. It is important to consider a range of roles individuals may assume when operating different components in the voting system and each may require different authentication mechanisms. The requirements described in this section vary from role to role. For instance, a kiosk worker will have different identification and authentication characteristics than a voter. Also, for selected critical functions there may be cases where split knowledge or dual authorization is necessary to ensure security. This is especially relevant for critical cryptographic key management functions.		
5.2.1	**Authentication**		
5.2.1.1	Authentication mechanisms supported by the voting system SHALL support authentication strength of at least 1/1,000,000.	11	Host Server Security Test Case
5.2.1.2	The voting system SHALL authenticate users per the minimum authentication methods outlined below. Refer to document for the table layout: http://www.eac.gov/assets/1/AssetManager/UOCAVA_Pilot_Program_Requirments-03.24.10.pdf Table 5-1 Roles : Section 5 | Page 59	11	Host Server Security Test Case
5.2.1.3	The voting system SHALL provide multiple authentication methods to support multi-factor authentication.	4	Normal Ballot Delivery Test Case
		11	Host Server Security Test Case
5.2.1.4	When private or secret authentication data is stored by the voting system, it SHALL be protected to ensure that the confidentiality and integrity of the data are not violated.	11	Host Server Security Test Case
5.2.1.5	The voting system SHALL provide a mechanism to reset a password if it is forgotten, in accordance with the system access/security policy.	1	Host Server Administration Test Case
5.2.1.6	The voting system SHALL allow the administrator group or role to specify password strength for all accounts including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters per NIST 800-63 Electronic Authentication Guideline Standards.	1	Host Server Administration Test Case
5.2.1.7	The voting system SHALL enforce password histories and allow the administrator to configure the history length when passwords are stored by the system.	1	Host Server Administration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.2.1.8	The voting system SHALL ensure that the user name is not used in the password.	1	Host Server Administration Test Case
5.2.1.9	The voting system SHALL provide a means to automatically expire passwords.	1	Host Server Administration Test Case
5.2.1.10	The voting system servers and vote capture devices SHALL identify and authenticate one another using NIST - approved cryptographic authentication methods at the 112 bits of security.	3	Cryptography Test Case
5.2.1.11	Remote voting location site Virtual Private Network (VPN) connections (i.e., vote capture devices) to voting servers SHALL be authenticated using strong mutual cryptographic authentication at the 112 bits of security.	N/A	
5.2.1.12	Message authentication SHALL be used for applications to protect the integrity of the message content using a schema with 112 bits of security.	N/A	
5.2.1.13	IPsec, SSL, or TLS and MAC mechanisms SHALL all be configured to be compliant with FIPS 140-2 using approved algorithm suites and protocols.	3	Cryptography Test Case
5.3	**Cryptography**		
	Cryptography serves several purposes in voting systems. They include: Confidentiality: where necessary the confidentiality of voting records can be provided by encryption; Authentication: data and programs can be authenticated by a digital signature or message authentication codes (MAC), or by comparison of the cryptographic hashes of programs or data with the reliably known hash values of the program or data. If the program or data are altered, then that alteration is detected when the signature or MAC is verified, or the hash on the data or program is compared to the known hash value. Typically the programs loaded on voting systems and the ballot definitions used by voting systems are verified by the systems, while systems apply digital signatures to authenticate the critical audit data that they output. For remote connections cryptographic user authentication mechanism SHALL be based on strong authentication methods; and Random number generation: random numbers are used for several purposes including the creation of cryptographic keys for cryptographic algorithms and methods to provide the services listed above, and as identifiers for voting records that can be used to identify or correlate the records without providing any information that could identify the voter.		
5.3.1	**General Cryptography Requirements**		
5.3.1.1	All cryptographic functionality SHALL be implemented using NIST-approved cryptographic algorithms/schemas, or use published and credible cryptographic algorithms/schemas/protocols.	3	Cryptography Test Case
5.3.1.2	Cryptographic algorithms and schemas SHALL be implemented with a security strength equivalent to at least 112 bits of security to protect sensitive voting information and election records.	3	Cryptography Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.3.1.3	Cryptography used to protect information in-transit over public telecommunication networks SHALL use NIST-approved algorithms and cipher suites. In addition the implementations of these algorithms SHALL be NIST-approved (Cryptographic Algorithm Validation Program).	3	Cryptography Test Case
5.3.2	**Key Management**		
	The following requirements apply to voting systems that generate cryptographic keys internally.		
5.3.2.1	Cryptographic keys generated by the voting system SHALL use a NIST-approved key generation method, or a published and credible key generation method.	3	Cryptography Test Case
5.3.2.2	Compromising the security of the key generation method (e.g., guessing the seed value to initialize the deterministic random number generator (RNG)) SHALL require as least as many operations as determining the value of the generated key.	N/T	
5.3.2.3	If a seed key is entered during the key generation process, entry of the key SHALL meet the key entry requirements in 5.3.3.1. If intermediate key generation values are output from the cryptographic module, the values SHALL be output either in encrypted form or under split knowledge procedures.	3	Cryptography Test Case
5.3.2.4	Cryptographic keys used to protect information in-transit over public telecommunication networks SHALL use NIST-approved key generation methods. If the approved key generation method requires input from a random number generator, then an approved (FIPS 140-2) random number generator SHALL be used.	3	Cryptography Test Case
5.3.2.5	Random number generators used to generate cryptographic keys SHALL implement one or more health tests that provide assurance that the random number generator continues to operate as intended (e.g., the entropy source is not stuck).	3	Cryptography Test Case
5.3.3	**Key Establishment**		
	Key establishment may be performed by automated methods (e.g., use of a public key algorithm), manual methods (use of a manually transported key loading device), or a combination of automated and manual methods.		
5.3.3.1	Secret and private keys established using automated methods SHALL be entered into and output from a voting system in encrypted form. Secret and private keys established using manual methods may be entered into or output from a system in plaintext form.	3	Cryptography Test Case
5.3.4.1	Cryptographic keys stored within the voting system SHALL NOT be stored in plaintext. Keys stored outside the voting system SHALL be protected from disclosure or modification.	3	Cryptography Test Case
5.3.4.2	The voting system SHALL provide methods to zeroize all plaintext secret and private cryptographic keys within the system.	3	Cryptography Test Case
5.3.4.3	The voting system SHALL support the capability to reset cryptographic keys to new values.	3	Cryptography Test Case
5.4	**Voting System Integrity Management**		
	This section addresses the secure deployment and operation of the voting system, including the protection of removable media and protection against malicious software.		

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.4.1	**Protecting the Integrity of the Voting System**		
5.4.1.1	The integrity and authenticity of each individual cast vote SHALL be protected from any tampering or modification during transmission.	N/A	
5.4.1.2	The integrity and authenticity of each individual cast vote SHALL be preserved by means of a digital signature during storage.	N/A	
5.4.1.3	Cast vote data SHALL NOT be permanently stored on the vote capture device.	4	Normal Ballot Delivery Test Case
5.4.1.4	The integrity and authenticity of the electronic ballot box SHALL be protected by means of a digital signature.	N/A	
5.4.1.5	The voting system SHALL use malware detection software to protect against known malware that targets the operating system, services, and applications.	5	Discovery Penetration Test Case
5.4.1.6	The voting system SHALL provide a mechanism for updating malware detection signatures.	5	Discovery Penetration Test Case
5.4.1.7	The voting system SHALL provide the capability for kiosk workers to validate the software used on the vote capture devices as part of the daily initiation of kiosk operations.	N/A	
5.5	**Communications Security**		
	This section provides requirements for communications security. These requirements address ensuring the integrity of transmitted information and protecting the voting system from external communications-based threats.		
5.5.1	**Data Transmission Security**		
5.5.1.1	Voting systems that transmit data over communications links SHALL provide integrity protection for data in transit through the generation of integrity data (digital signatures and/or message authentication codes) for outbound traffic and verification of the integrity data for inbound traffic.	11	Host Server Security Test Case
5.5.1.2	Voting systems SHALL use at a minimum TLS 1.0, SSL 3.1 or equivalent protocols, including all updates to both protocols and implementations as of the date of the submission (e.g., RFC 5746 for TLS 1.0).	3	Cryptography Test Case
5.5.1.3	Voting systems deploying VPNs SHALL configure them to only allow FIPS-compliant cryptographic algorithms and cipher suites.	N/A	
5.5.1.4	Each communicating device SHALL have a unique system identifier.	5	Discovery Penetration Test Case
5.5.1.5	Each device SHALL mutually strongly authenticate using the system identifier before additional network data packets are processed.	6	Remote Terminal Security Test Case
		1	Host Server Administration Test Case
5.5.1.6	Data transmission SHALL preserve the secrecy of voters' ballot selections and SHALL prevent the violation of ballot secrecy and integrity.	5	Discovery Penetration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.5.2	**External Threats**		
	Voting systems SHALL implement protections against external threats to which the system may be susceptible.	5	Discovery Penetration Test Case
		6	Remote Terminal Security Test Case
		1	Host Server Administration Test Case
5.5.2.1	Voting system components SHALL have the ability to enable or disable physical network interfaces.	1	Host Server Administration Test Case
5.5.2.2	The number of active ports and associated network services and protocols SHALL be restricted to the minimum required for the voting system to function.	11	Host Server Security Test Case
5.5.2.3	The voting system SHALL block all network connections that are not over a mutually authenticated channel.	11	Host Server Security Test Case
5.6	**Logging**		
5.6.1	**Log Management**		
5.6.1.1	The voting system SHALL implement default settings for secure log management activities, including log generation, transmission, storage, analysis, and disposal.	1	Host Server Administration Test Case
5.6.1.2	Logs SHALL only be accessible to authorized roles.	1	Host Server Administration Test Case
5.6.1.3	The voting system SHALL restrict log access to append-only for privileged logging processes and read-only for authorized roles.	1	Host Server Administration Test Case
5.6.1.4	The voting system SHALL log logging failures, log clearing, and log rotation.	1	Host Server Administration Test Case
5.6.1.5	The voting system SHALL store log data in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format.	1	Host Server Administration Test Case
5.6.1.6	The voting system SHALL ensure that each jurisdiction's event logs and each component's logs are separable from each other.	N/A	
5.6.1.7	The voting system SHALL include an application or program to view, analyze, and search event logs.	1	Host Server Administration Test Case
5.6.1.8	All logs SHALL be preserved in a useable manner prior to voting system decommissioning.	1	Host Server Administration Test Case
5.6.1.9	Logs SHALL NOT contain any data that could violate the privacy of the voter's identity.	4	Normal Ballot Delivery Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.6.1.10	Timekeeping mechanisms SHALL generate time and date values, including hours, minutes, and seconds.	1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
		10	Local Ballot Delivery Test Case
5.6.1.11	The precision of the timekeeping mechanism SHALL be able to distinguish and properly order all log events.	10	Local Ballot Delivery Test Case
		4	Normal Ballot Delivery Test Case
5.6.1.12	Only the system administrator SHALL be permitted to set the system clock.	1	Host Server Administration Test Case
5.6.2	**Communication Logging**		
5.6.2.1	All communications actions SHALL be logged.	5	Discovery Penetration Test Case
		4	Normal Ballot Delivery Test Case
		1	Host Server Administration Test Case
		3	Cryptography Test Case
5.6.2.2	The communications log SHALL contain at least the following entries: Times when the communications are activated and deactivated; Services accessed; Identification of the device which data was transmitted to or received from; Identification of authorized entity; and Successful and unsuccessful attempts to access communications or services.	4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case
5.6.3	**System Event Logging**		
	This section describes requirements for the voting system to perform event logging for system maintenance troubleshooting, recording the history of system activity, and detecting unauthorized or malicious activity. The operating system, and/or applications software may perform the actual event logging. There may be multiple logs in use for any system component.		

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.6.3.1	The voting system SHALL log the following data for each event: a. System ID; b. Unique event ID and/or type; c. Timestamp; d. Success or failure of event, if applicable; e. User ID triggering the event, if applicable; and f. Jurisdiction, if applicable.	4	Normal Ballot Delivery Test Case
		1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
		7	Recovery form hardware error Test Case
5.6.3.2	All critical events SHALL be recorded in the system event log.	7	Recovery form hardware error Test Case
		4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case
5.6.3.3	At a minimum the voting system SHALL log the events described in the table below. NOTE: See "Table 5-2 System Events" in document - page 71	1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
		3	Cryptography Test Case
		7	Recovery form hardware error Test Case
		5	Discovery Penetration Test Case
5.7	**Incident Response**		
5.7.1	**Incident Response Support**		
5.7.1.1	Manufacturers SHALL document what types of system operations or security events (e.g., failure of critical component, detection of malicious code, unauthorized access to restricted data) are classified as critical.	N/A	
5.7.1.2	An alarm that notifies appropriate personnel SHALL be generated on the vote capture device, system server, or tabulation device, depending upon which device has the error, if a critical event is detected.	N/A	
5.8	**Physical and Environmental Security**		
5.8.1	**Physical Access**		
5.8.1.1	Any unauthorized physical access SHALL leave physical evidence that an unauthorized event has taken place.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.8.2.1	The voting system SHALL disable physical ports and access points that are not essential to voting operations, testing, and auditing.	11	Host Server Security Test Case
5.8.3.1	If a physical connection between the vote capture device and a component is broken, the affected vote capture device port SHALL be automatically disabled.	N/A	
5.8.3.2	The voting system SHALL produce a visual alarm if a connected component is physically disconnected.	N/A	
5.8.3.3	An event log entry that identifies the name of the affected device SHALL be generated if a vote capture device component is disconnected.	7	Recovery form hardware error Test Case
5.8.3.4	Disabled ports SHALL only be re-enabled by authorized administrators.	1	Host Server Administration Test Case
5.8.3.5	Vote capture devices SHALL be designed with the capability to restrict physical access to voting device ports that accommodate removable media with the exception of ports used to activate a voting session.	N/A	
5.8.3.6	Vote capture devices SHALL be designed to give a physical indication of tampering or unauthorized access to ports and all other access points, if used as described in the manufacturer's documentation.	N/A	
5.8.3.7	Vote capture devices SHALL be designed such that physical ports can be manually disabled by an authorized administrator.	N/A	
5.8.4	**Door Cover and Panel Security**		
5.8.4.1	Access points such as covers and panels SHALL be secured by locks or tamper evident or tamper resistant countermeasures and SHALL be implemented so that kiosk workers can monitor access to vote capture device components through these points.	N/A	
5.8.5	**Secure Paper Record Receptacle**		
	If the voting system provides paper record containers then they SHALL be designed such that any unauthorized physical access results in physical evidence that an unauthorized event has taken place.	N/A	
5.8.6	**Secure Physical Lock and Key**		
5.8.6.1	Voting equipment SHALL be designed with countermeasures that provide physical indication that unauthorized attempts have been made to access locks installed for security purposes.	N/A	
5.8.6.2	Manufacturers SHALL provide locking systems for securing vote capture devices that can make use of keys that are unique to each owner.	N/A	
5.8.7	**Media Protection**		
	These requirements apply to all media, both paper and digital, that contain personal privacy related data or other protected or sensitive types of information.		

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.8.7.1	The voting system SHALL meet the following requirements: a. All paper records (including rejected ones) printed at the kiosk locations SHALL be deposited in a secure container; b. Vote capture device hardware, software and sensitive information (e.g., electoral roll) SHALL be physically protected to prevent unauthorized modification or disclosure; and c. Vote capture device hardware components, peripherals and removable media SHALL be identified and registered by means of a unique serial number or other identifier.	N/A	
5.9	**Penetration Resistance**		
5.9.1	**Resistance to Penetration Attempt**		
5.9.1.1	The voting system SHALL be resistant to attempts to penetrate the system by any remote unauthorized entity.	5	Discovery Penetration Test Case
5.9.1.2	The voting system SHALL be configured to minimize ports, responses and information disclosure about the system while still providing appropriate functionality.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.9.1.3	The voting system SHALL provide no access, information or services to unauthorized entities.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.9.1.4	All interfaces SHALL be penetration resistant including TCP/IP, wireless, and modems from any point in the system.	11	Host Server Security Test Case
5.9.1.5	The configuration and setup to attain penetration resistance SHALL be clearly and completely documented.	N/A	
5.9.2.1	The scope of penetration testing SHALL include all the voting system components. The scope of penetration testing includes but is not limited to the following: System server; Vote capture devices; Tabulation device; All items setup and configured per Technical Data Package (TDP) recommendations; Local wired and wireless networks; and 03/09/2011 Internet connections.	5	Discovery Penetration Test Case
5.9.2.2	Penetration testing SHALL be conducted on a voting system set up in a controlled lab environment. Setup and configuration SHALL be conducted in accordance with the TDP, and SHALL replicate the real world environment in which the voting system will be used.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.9.2.3	The penetration testing team SHALL conduct white box testing using manufacturer supplied documentation and voting system architecture information. Documentation includes the TDP and user documentation. The testing team SHALL have access to any relevant information regarding the voting system configuration. This includes, but is not limited to, network layout and Internet Protocol addresses for system devices and components. The testing team SHALL be provided any source code included in the TDP.	N/A	
5.9.2.04	Penetration testing seeks out vulnerabilities in the voting system that might be used to change the outcome of an election, interfere with voter ability to cast ballots, ballot counting, or compromise ballot secrecy. The penetration testing team SHALL prioritize testing efforts based on the following: a. Threat scenarios for the voting system under investigation; b. Remote attacks SHALL be prioritized over in-person attacks; c. Attacks with a large impact SHALL be prioritized over attacks with a more narrow impact; and d. Attacks that can change the outcome of an election SHALL be prioritized over attacks that compromise ballot secrecy or cause non-selective denial of service.	5	Discovery Penetration Test Case

[redacted]

REQUIREMENTS MATRIX

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
Section 5	**Security**		
5.1	**Access Control**		
	This section states requirements for the identification of authorized system users, processes and devices and the authentication or verification of those identities as a prerequisite to granting access to system processes and data. It also includes requirements to limit and control access to critical system components to protect system and data integrity, availability, confidentiality, and accountability. This section applies to all entities attempting to physically enter voting system facilities or to request services or data from the voting system.		
5.1.1	**Separation of Duties**		
5.1.1.1	The voting system SHALL allow the definition of personnel roles with segregated duties and responsibilities on critical processes to prevent a single person from compromising the integrity of the system.	1	Host Server Administration Test Case
5.1.1.2	The voting system SHALL ensure that only authorized roles, groups, or individuals have access to election data.	1	Host Server Administration Test Case
5.1.1.3	The voting system SHALL require at least two persons from a predefined group for validating the election configuration information, accessing the cast vote records, and starting the tabulation process..	N/A	
5.1.2	**Voting System Access**		
	The voting system SHALL provide access control mechanisms designed to permit authorized access and to prevent unauthorized access to the system.		
5.1.2.1	The voting system SHALL identify and authenticate each person to whom access is granted, and the specific functions and data to which each person holds authorized access.	1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
5.1.2.2	The voting system SHALL allow the administrator group or role to configure permissions and functionality for each identity, group or role to include account and group/role creation, modification, and deletion.	1	Host Server Administration Test Case
5.1.2.3	The voting system's default access control permissions SHALL implement the least privileged role or group needed.	1	Host Server Administration Test Case
5.1.2.4	The voting system SHALL prevent a lower-privilege process from modifying a higher-privilege process.	1	Host Server Administration Test Case
5.1.2.5	The voting system SHALL NOT require its execution as an operating system privileged account and SHALL NOT require the use of an operating system privileged account for its operation.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.1.2.6	The voting system SHALL log the identification of all personnel accessing or attempting to access the voting system to the system event log.	7	Recovery form hardware error Test Case
		1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case
5.1.2.7	The *(voting system)* SHALL provide tools for monitoring access to the system. These tools SHALL provide specific users real time display of persons accessing the system as well as reports from logs.	1	Host Server Administration Test Case
5.1.2.8	Vote capture device located at the remote voting location and the central server SHALL have the capability to restrict access to the voting system after a preset number of login failures. a. The lockout threshold SHALL be configurable by appropriate administrators/operators b. The voting system SHALL log the event c. The voting system SHALL immediately send a notification to appropriate administrators/operators of the event. d. The voting system SHALL provide a mechanism for the appropriate administrators/operators to reactivate the account after appropriate confirmation.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.1.2.9	The voting system SHALL log a notification when any account has been locked out.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.1.2.10	Authenticated sessions on critical processes SHALL have an inactivity time-out control that will require personnel re-authentication when reached. This time-out SHALL be implemented for administration and monitor consoles on all voting system devices.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.1.2.11	Authenticated sessions on critical processes SHALL have a screen-lock functionality that can be manually invoked.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.2	**Identification and Authentication**		
	Authentication mechanisms and their associated strength may vary from one voting system capability and architecture to another but all must meet the minimum requirement to maintain integrity and trust. It is important to consider a range of roles individuals may assume when operating different components in the voting system and each may require different authentication mechanisms. The requirements described in this section vary from role to role. For instance, a kiosk worker will have different identification and authentication characteristics than a voter. Also, for selected critical functions there may be cases where split knowledge or dual authorization is necessary to ensure security. This is especially relevant for critical cryptographic key management functions.		
5.2.1	**Authentication**		
5.2.1.1	Authentication mechanisms supported by the voting system SHALL support authentication strength of at least 1/1,000,000.	11	Host Server Security Test Case
5.2.1.2	The voting system SHALL authenticate users per the minimum authentication methods outlined below. Refer to document for the table layout: http://www.eac.gov/assets/1/AssetManager/UOCAVA_Pilot_Program_Requirments-03.24.10.pdf Table 5-1 Roles : Section 5 | Page 59	11	Host Server Security Test Case
5.2.1.3	The voting system SHALL provide multiple authentication methods to support multi-factor authentication.	1	Host Server Administration Test Case
5.2.1.4	When private or secret authentication data is stored by the voting system, it SHALL be protected to ensure that the confidentiality and integrity of the data are not violated.	11	Host Server Security Test Case
5.2.1.5	The voting system SHALL provide a mechanism to reset a password if it is forgotten, in accordance with the system access/security policy.	1	Host Server Administration Test Case
5.2.1.6	The voting system SHALL allow the administrator group or role to specify password strength for all accounts including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters per NIST 800-63 Electronic Authentication Guideline Standards.	1	Host Server Administration Test Case
5.2.1.7	The voting system SHALL enforce password histories and allow the administrator to configure the history length when passwords are stored by the system.	1	Host Server Administration Test Case
5.2.1.8	The voting system SHALL ensure that the user name is not used in the password.	1	Host Server Administration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.2.1.9	The voting system SHALL provide a means to automatically expire passwords.	1	Host Server Administration Test Case
5.2.1.10	The voting system servers and vote capture devices SHALL identify and authenticate one another using NIST - approved cryptographic authentication methods at the 112 bits of security.	3	Cryptography Test Case
5.2.1.11	Remote voting location site Virtual Private Network (VPN) connections (i.e., vote capture devices) to voting servers SHALL be authenticated using strong mutual cryptographic authentication at the 112 bits of security.	N/A	
5.2.1.12	Message authentication SHALL be used for applications to protect the integrity of the message content using a schema with 112 bits of security.	11	Host Server Security Test Case
5.2.1.13	IPsec, SSL, or TLS and MAC mechanisms SHALL all be configured to be compliant with FIPS 140-2 using approved algorithm suites and protocols.	3	Cryptography Test Case
5.3	**Cryptography**		
	Cryptography serves several purposes in voting systems. They include: Confidentiality: where necessary the confidentiality of voting records can be provided by encryption; Authentication: data and programs can be authenticated by a digital signature or message authentication codes (MAC), or by comparison of the cryptographic hashes of programs or data with the reliably known hash values of the program or data. If the program or data are altered, then that alteration is detected when the signature or MAC is verified, or the hash on the data or program is compared to the known hash value. Typically the programs loaded on voting systems and the ballot definitions used by voting systems are verified by the systems, while systems apply digital signatures to authenticate the critical audit data that they output. For remote connections cryptographic user authentication mechanism SHALL be based on strong authentication methods; and Random number generation: random numbers are used for several purposes including the creation of cryptographic keys for cryptographic algorithms and methods to provide the services listed above, and as identifiers for voting records that can be used to identify or correlate the records without providing any information that could identify the voter.		
5.3.1	**General Cryptography Requirements**		
5.3.1.1	All cryptographic functionality SHALL be implemented using NIST-approved cryptographic algorithms/schemas, or use published and credible cryptographic algorithms/schemas/protocols.	3	Cryptography Test Case
5.3.1.2	Cryptographic algorithms and schemas SHALL be implemented with a security strength equivalent to at least 112 bits of security to protect sensitive voting information and election records.	3	Cryptography Test Case
5.3.1.3	Cryptography used to protect information in-transit over public telecommunication networks SHALL use NIST-approved algorithms and cipher suites. In addition the implementations of these algorithms SHALL be NIST-approved (Cryptographic Algorithm Validation Program).	3	Cryptography Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.3.2	**Key Management**		
	The following requirements apply to voting systems that generate cryptographic keys internally.		
5.3.2.1	Cryptographic keys generated by the voting system SHALL use a NIST-approved key generation method, or a published and credible key generation method.	3	Cryptography Test Case
5.3.2.2	Compromising the security of the key generation method (e.g., guessing the seed value to initialize the deterministic random number generator (RNG)) SHALL require as least as many operations as determining the value of the generated key.	N/T	
5.3.2.3	If a seed key is entered during the key generation process, entry of the key SHALL meet the key entry requirements in 5.3.3.1. If intermediate key generation values are output from the cryptographic module, the values SHALL be output either in encrypted form or under split knowledge procedures.	3	Cryptography Test Case
5.3.2.4	Cryptographic keys used to protect information in-transit over public telecommunication networks SHALL use NIST-approved key generation methods. If the approved key generation method requires input from a random number generator, then an approved (FIPS 140-2) random number generator SHALL be used.	3	Cryptography Test Case
5.3.2.5	Random number generators used to generate cryptographic keys SHALL implement one or more health tests that provide assurance that the random number generator continues to operate as intended (e.g., the entropy source is not stuck).	3	Cryptography Test Case
5.3.3	**Key Establishment**		
	Key establishment may be performed by automated methods (e.g., use of a public key algorithm), manual methods (use of a manually transported key loading device), or a combination of automated and manual methods.		
5.3.3.1	Secret and private keys established using automated methods SHALL be entered into and output from a voting system in encrypted form. Secret and private keys established using manual methods may be entered into or output from a system in plaintext form.	3	Cryptography Test Case
5.3.4.1	Cryptographic keys stored within the voting system SHALL NOT be stored in plaintext. Keys stored outside the voting system SHALL be protected from disclosure or modification.	3	Cryptography Test Case
5.3.4.2	The voting system SHALL provide methods to zeroize all plaintext secret and private cryptographic keys within the system.	3	Cryptography Test Case
5.3.4.3	The voting system SHALL support the capability to reset cryptographic keys to new values.	3	Cryptography Test Case
5.4	**Voting System Integrity Management**		
	This section addresses the secure deployment and operation of the voting system, including the protection of removable media and protection against malicious software.		
5.4.1	**Protecting the Integrity of the Voting System**		
5.4.1.1	The integrity and authenticity of each individual cast vote SHALL be protected from any tampering or modification during transmission.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.4.1.2	The integrity and authenticity of each individual cast vote SHALL be preserved by means of a digital signature during storage.	N/A	
5.4.1.3	Cast vote data SHALL NOT be permanently stored on the vote capture device.	4	Normal Ballot Delivery Test Case
5.4.1.4	The integrity and authenticity of the electronic ballot box SHALL be protected by means of a digital signature.	N/A	
5.4.1.5	The voting system SHALL use malware detection software to protect against known malware that targets the operating system, services, and applications.	5	Discovery Penetration Test Case
5.4.1.6	The voting system SHALL provide a mechanism for updating malware detection signatures.	5	Discovery Penetration Test Case
5.4.1.7	The voting system SHALL provide the capability for kiosk workers to validate the software used on the vote capture devices as part of the daily initiation of kiosk operations.	N/A	
5.5	**Communications Security**		
	This section provides requirements for communications security. These requirements address ensuring the integrity of transmitted information and protecting the voting system from external communications-based threats.		
5.5.1	**Data Transmission Security**		
5.5.1.1	Voting systems that transmit data over communications links SHALL provide integrity protection for data in transit through the generation of integrity data (digital signatures and/or message authentication codes) for outbound traffic and verification of the integrity data for inbound traffic.	11	Host Server Security Test Case
5.5.1.2	Voting systems SHALL use at a minimum TLS 1.0, SSL 3.1 or equivalent protocols, including all updates to both protocols and implementations as of the date of the submission (e.g., RFC 5746 for TLS 1.0).	11	Host Server Security Test Case
5.5.1.3	Voting systems deploying VPNs SHALL configure them to only allow FIPS-compliant cryptographic algorithms and cipher suites.	N/A	
5.5.1.4	Each communicating device SHALL have a unique system identifier.	11	Host Server Security Test Case
5.5.1.5	Each device SHALL mutually strongly authenticate using the system identifier before additional network data packets are processed.	11	Host Server Security Test Case
5.5.1.6	Data transmission SHALL preserve the secrecy of voters' ballot selections and SHALL prevent the violation of ballot secrecy and integrity.	5	Discovery Penetration Test Case
5.5.2	**External Threats**		
	Voting systems SHALL implement protections against external threats to which the system may be susceptible.	5	Discovery Penetration Test Case
5.5.2.1	Voting system components SHALL have the ability to enable or disable physical network interfaces.	1	Host Server Administration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.5.2.2	The number of active ports and associated network services and protocols SHALL be restricted to the minimum required for the voting system to function.	11	Host Server Security Test Case
5.5.2.3	The voting system SHALL block all network connections that are not over a mutually authenticated channel.	11	Host Server Security Test Case
5.6	**Logging**		
5.6.1	**Log Management**		
5.6.1.1	The voting system SHALL implement default settings for secure log management activities, including log generation, transmission, storage, analysis, and disposal.	1	Host Server Administration Test Case
5.6.1.2	Logs SHALL only be accessible to authorized roles.	1	Host Server Administration Test Case
5.6.1.3	The voting system SHALL restrict log access to append-only for privileged logging processes and read-only for authorized roles.	1	Host Server Administration Test Case
5.6.1.4	The voting system SHALL log logging failures, log clearing, and log rotation.	1	Host Server Administration Test Case
5.6.1.5	The voting system SHALL store log data in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format.	1	Host Server Administration Test Case
5.6.1.6	The voting system SHALL ensure that each jurisdiction's event logs and each component's logs are separable from each other.	N/A	
5.6.1.7	The voting system SHALL include an application or program to view, analyze, and search event logs.	1	Host Server Administration Test Case
5.6.1.8	All logs SHALL be preserved in a useable manner prior to voting system decommissioning.	1	Host Server Administration Test Case
5.6.1.9	Logs SHALL NOT contain any data that could violate the privacy of the voter's identity.	4	Normal Ballot Delivery Test Case
5.6.1.10	Timekeeping mechanisms SHALL generate time and date values, including hours, minutes, and seconds.	4	Normal Ballot Delivery Test Case
		1	Host Server Administration Test Case
5.6.1.11	The precision of the timekeeping mechanism SHALL be able to distinguish and properly order all log events.	4	Normal Ballot Delivery Test Case
5.6.1.12	Only the system administrator SHALL be permitted to set the system clock.	N/A	
5.6.2	**Communication Logging**		

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.6.2.1	All communications actions SHALL be logged.	4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case
5.6.2.2	The communications log SHALL contain at least the following entries: Times when the communications are activated and deactivated; Services accessed; Identification of the device which data was transmitted to or received from; Identification of authorized entity; and Successful and unsuccessful attempts to access communications or services.	4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case
5.6.3	**System Event Logging**		
	This section describes requirements for the voting system to perform event logging for system maintenance troubleshooting, recording the history of system activity, and detecting unauthorized or malicious activity. The operating system, and/or applications software may perform the actual event logging. There may be multiple logs in use for any system component.		
5.6.3.1	The voting system SHALL log the following data for each event: a. System ID; b. Unique event ID and/or type; c. Timestamp; d. Success or failure of event, if applicable; e. User ID triggering the event, if applicable; and f. Jurisdiction, if applicable.	1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
		7	Recovery form hardware error Test Case
		5	Discovery Penetration Test Case
5.6.3.2	All critical events SHALL be recorded in the system event log.	5	Discovery Penetration Test Case
		4	Normal Ballot Delivery Test Case
		7	Recovery form hardware error Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.6.3.3	At a minimum the voting system SHALL log the events described in the table below. NOTE: See "Table 5-2 System Events" in document - page 71	1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case
		7	Recovery form hardware error Test Case
5.7	**Incident Response**		
5.7.1	**Incident Response Support**		
5.7.1.1	Manufacturers SHALL document what types of system operations or security events (e.g., failure of critical component, detection of malicious code, unauthorized access to restricted data) are classified as critical.	N/A	
5.7.1.2	An alarm that notifies appropriate personnel SHALL be generated on the vote capture device, system server, or tabulation device, depending upon which device has the error, if a critical event is detected.	N/A	
5.8	**Physical and Environmental Security**		
5.8.1	**Physical Access**		
5.8.1.1	Any unauthorized physical access SHALL leave physical evidence that an unauthorized event has taken place.	N/A	
5.8.2.1	The voting system SHALL disable physical ports and access points that are not essential to voting operations, testing, and auditing.	11	Host Server Security Test Case
5.8.3.1	If a physical connection between the vote capture device and a component is broken, the affected vote capture device port SHALL be automatically disabled.	N/A	
5.8.3.2	The voting system SHALL produce a visual alarm if a connected component is physically disconnected.	N/A	
5.8.3.3	An event log entry that identifies the name of the affected device SHALL be generated if a vote capture device component is disconnected.	7	Recovery form hardware error Test Case
5.8.3.4	Disabled ports SHALL only be re-enabled by authorized administrators.	1	Host Server Administration Test Case
5.8.3.5	Vote capture devices SHALL be designed with the capability to restrict physical access to voting device ports that accommodate removable media with the exception of ports used to activate a voting session.	N/A	
5.8.3.6	Vote capture devices SHALL be designed to give a physical indication of tampering or unauthorized access to ports and all other access points, if used as described in the manufacturer's documentation.	N/A	
5.8.3.7	Vote capture devices SHALL be designed such that physical ports can be manually disabled by an authorized administrator.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.8.4	**Door Cover and Panel Security**		
5.8.4.1	Access points such as covers and panels SHALL be secured by locks or tamper evident or tamper resistant countermeasures and SHALL be implemented so that kiosk workers can monitor access to vote capture device components through these points.	N/A	
5.8.5	**Secure Paper Record Receptacle**		
	If the voting system provides paper record containers then they SHALL be designed such that any unauthorized physical access results in physical evidence that an unauthorized event has taken place.	N/A	
5.8.6	**Secure Physical Lock and Key**		
5.8.6.1	Voting equipment SHALL be designed with countermeasures that provide physical indication that unauthorized attempts have been made to access locks installed for security purposes.	N/A	
5.8.6.2	Manufacturers SHALL provide locking systems for securing vote capture devices that can make use of keys that are unique to each owner.	N/A	
5.8.7	**Media Protection**		
	These requirements apply to all media, both paper and digital, that contain personal privacy related data or other protected or sensitive types of information.		
5.8.7.1	The voting system SHALL meet the following requirements: a. All paper records (including rejected ones) printed at the kiosk locations SHALL be deposited in a secure container; b. Vote capture device hardware, software and sensitive information (e.g., electoral roll) SHALL be physically protected to prevent unauthorized modification or disclosure; and c. Vote capture device hardware components, peripherals and removable media SHALL be identified and registered by means of a unique serial number or other identifier.	N/A	
5.9	**Penetration Resistance**		
5.9.1	**Resistance to Penetration Attempts**		
5.9.1.1	The voting system SHALL be resistant to attempts to penetrate the system by any remote unauthorized entity.	5	Discovery Penetration Test Case
		11	Host Server Security Test Case
5.9.1.2	The voting system SHALL be configured to minimize ports, responses and information disclosure about the system while still providing appropriate functionality.	5	Discovery Penetration Test Case
		11	Host Server Security Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.9.1.3	The voting system SHALL provide no access, information or services to unauthorized entities.	5	Discovery Penetration Test Case
		1	Host Server Administration Test Case
5.9.1.4	All interfaces SHALL be penetration resistant including TCP/IP, wireless, and modems from any point in the system.	11	Host Server Security Test Case
5.9.1.5	The configuration and setup to attain penetration resistance SHALL be clearly and completely documented.	N/A	
5.9.2.1	The scope of penetration testing SHALL include all the voting system components. The scope of penetration testing includes but is not limited to the following: System server; Vote capture devices; Tabulation device; All items setup and configured per Technical Data Package (TDP) recommendations; Local wired and wireless networks; and 03/09/2011 Internet connections.	5	Discovery Penetration Test Case
5.9.2.2	Penetration testing SHALL be conducted on a voting system set up in a controlled lab environment. Setup and configuration SHALL be conducted in accordance with the TDP, and SHALL replicate the real world environment in which the voting system will be used.	N/A	
5.9.2.3	The penetration testing team SHALL conduct white box testing using manufacturer supplied documentation and voting system architecture information. Documentation includes the TDP and user documentation. The testing team SHALL have access to any relevant information regarding the voting system configuration. This includes, but is not limited to, network layout and Internet Protocol addresses for system devices and components. The testing team SHALL be provided any source code included in the TDP.	N/A	
5.9.2.04	Penetration testing seeks out vulnerabilities in the voting system that might be used to change the outcome of an election, interfere with voter ability to cast ballots, ballot counting, or compromise ballot secrecy. The penetration testing team SHALL prioritize testing efforts based on the following: a. Threat scenarios for the voting system under investigation; b. Remote attacks SHALL be prioritized over in-person attacks; c. Attacks with a large impact SHALL be prioritized over attacks with a more narrow impact; and d. Attacks that can change the outcome of an election SHALL be prioritized over attacks that compromise ballot secrecy or cause non-selective denial of service.	5	Discovery Penetration Test Case

[redacted]

REQUIREMENTS MATRIX

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
Section 5	**Security**		
5.1	**Access Control**		
	This section states requirements for the identification of authorized system users, processes and devices and the authentication or verification of those identities as a prerequisite to granting access to system processes and data. It also includes requirements to limit and control access to critical system components to protect system and data integrity, availability, confidentiality, and accountability. This section applies to all entities attempting to physically enter voting system facilities or to request services or data from the voting system.		
5.1.1	**Separation of Duties**		
5.1.1.1	The voting system SHALL allow the definition of personnel roles with segregated duties and responsibilities on critical processes to prevent a single person from compromising the integrity of the system.	1	Host Server Administration Test Case
5.1.1.2	The voting system SHALL ensure that only authorized roles, groups, or individuals have access to election data.	5	Discovery Penetration Test Case
5.1.1.3	The voting system SHALL require at least two persons from a predefined group for validating the election configuration information, accessing the cast vote records, and starting the tabulation process..	N/A	
5.1.2	**Voting System Access**		
	The voting system SHALL provide access control mechanisms designed to permit authorized access and to prevent unauthorized access to the system.		
5.1.2.1	The voting system SHALL identify and authenticate each person to whom access is granted, and the specific functions and data to which each person holds authorized access.	4	Normal Ballot Delivery Test Case
		1	Host Server Administration Test Case
		12	Voter Registration Request Test Case
5.1.2.2	The voting system SHALL allow the administrator group or role to configure permissions and functionality for each identity, group or role to include account and group/role creation, modification, and deletion.	1	Host Server Administration Test Case
5.1.2.3	The voting system's default access control permissions SHALL implement the least privileged role or group needed.	1	Host Server Administration Test Case
5.1.2.4	The voting system SHALL prevent a lower-privilege process from modifying a higher-privilege process.	1	Host Server Administration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.1.2.5	The voting system SHALL NOT require its execution as an operating system privileged account and SHALL NOT require the use of an operating system privileged account for its operation.	N/A	
5.1.2.6	The voting system SHALL log the identification of all personnel accessing or attempting to access the voting system to the system event log.	4	Normal Ballot Delivery Test Case
		1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
		12	Voter Registration Request Test Case
5.1.2.7	The *(voting system)* SHALL provide tools for monitoring access to the system. These tools SHALL provide specific users real time display of persons accessing the system as well as reports from logs.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.1.2.8	Vote capture device located at the remote voting location and the central server SHALL have the capability to restrict access to the voting system after a preset number of login failures. a. The lockout threshold SHALL be configurable by appropriate administrators/operators b. The voting system SHALL log the event c. The voting system SHALL immediately send a notification to appropriate administrators/operators of the event. d. The voting system SHALL provide a mechanism for the appropriate administrators/operators to reactivate the account after appropriate confirmation.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.1.2.9	The voting system SHALL log a notification when any account has been locked out.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.1.2.10	Authenticated sessions on critical processes SHALL have an inactivity time-out control that will require personnel re-authentication when reached. This time-out SHALL be implemented for administration and monitor consoles on all voting system devices.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.1.2.11	Authenticated sessions on critical processes SHALL have a screen-lock functionality that can be manually invoked.	N/A	
5.2	**Identification and Authentication**		
	Authentication mechanisms and their associated strength may vary from one voting system capability and architecture to another but all must meet the minimum requirement to maintain integrity and trust. It is important to consider a range of roles individuals may assume when operating different components in the voting system and each may require different authentication mechanisms. The requirements described in this section vary from role to role. For instance, a kiosk worker will have different identification and authentication characteristics than a voter. Also, for selected critical functions there may be cases where split knowledge or dual authorization is necessary to ensure security. This is especially relevant for critical cryptographic key management functions.		
5.2.1	**Authentication**		
5.2.1.1	Authentication mechanisms supported by the voting system SHALL support authentication strength of at least 1/1,000,000.	11	Host Server Security Test Case
5.2.1.2	The voting system SHALL authenticate users per the minimum authentication methods outlined below. Refer to document for the table layout: http://www.eac.gov/assets/1/AssetManager/UOCAVA_Pilot_Program_Requirments-03.24.10.pdf Table 5-1 Roles : Section 5 | Page 59	11	Host Server Security Test Case
5.2.1.3	The voting system SHALL provide multiple authentication methods to support multi-factor authentication.	1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
		12	Voter Registration Request Test Case
5.2.1.4	When private or secret authentication data is stored by the voting system, it SHALL be protected to ensure that the confidentiality and integrity of the data are not violated.	11	Host Server Security Test Case
5.2.1.5	The voting system SHALL provide a mechanism to reset a password if it is forgotten, in accordance with the system access/security policy.	1	Host Server Administration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.2.1.6	The voting system SHALL allow the administrator group or role to specify password strength for all accounts including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters per NIST 800-63 Electronic Authentication Guideline Standards.	1	Host Server Administration Test Case
5.2.1.7	The voting system SHALL enforce password histories and allow the administrator to configure the history length when passwords are stored by the system.	1	Host Server Administration Test Case
5.2.1.8	The voting system SHALL ensure that the user name is not used in the password.	1	Host Server Administration Test Case
5.2.1.9	The voting system SHALL provide a means to automatically expire passwords.	1	Host Server Administration Test Case
5.2.1.10	The voting system servers and vote capture devices SHALL identify and authenticate one another using NIST - approved cryptographic authentication methods at the 112 bits of security.	3	Cryptography Test Case
5.2.1.11	Remote voting location site Virtual Private Network (VPN) connections (i.e., vote capture devices) to voting servers SHALL be authenticated using strong mutual cryptographic authentication at the 112 bits of security.	N/A	
5.2.1.12	Message authentication SHALL be used for applications to protect the integrity of the message content using a schema with 112 bits of security.	11	Host Server Security Test Case
5.2.1.13	IPsec, SSL, or TLS and MAC mechanisms SHALL all be configured to be compliant with FIPS 140-2 using approved algorithm suites and protocols.	3	Cryptography Test Case
5.3	**Cryptography**		
	Cryptography serves several purposes in voting systems. They include: Confidentiality: where necessary the confidentiality of voting records can be provided by encryption; Authentication: data and programs can be authenticated by a digital signature or message authentication codes (MAC), or by comparison of the cryptographic hashes of programs or data with the reliably known hash values of the program or data. If the program or data are altered, then that alteration is detected when the signature or MAC is verified, or the hash on the data or program is compared to the known hash value. Typically the programs loaded on voting systems and the ballot definitions used by voting systems are verified by the systems, while systems apply digital signatures to authenticate the critical audit data that they output. For remote connections cryptographic user authentication mechanism SHALL be based on strong authentication methods; and		

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.3	**Cryptography (continued)**		
	Random number generation: random numbers are used for several purposes including the creation of cryptographic keys for cryptographic algorithms and methods to provide the services listed above, and as identifiers for voting records that can be used to identify or correlate the records without providing any information that could identify the voter.		
5.3.1	**General Cryptography Requirements**		
5.3.1.1	All cryptographic functionality SHALL be implemented using NIST-approved cryptographic algorithms/schemas, or use published and credible cryptographic algorithms/schemas/protocols.	3	Cryptography Test Case
5.3.1.2	Cryptographic algorithms and schemas SHALL be implemented with a security strength equivalent to at least 112 bits of security to protect sensitive voting information and election records.	3	Cryptography Test Case
5.3.1.3	Cryptography used to protect information in-transit over public telecommunication networks SHALL use NIST-approved algorithms and cipher suites. In addition the implementations of these algorithms SHALL be NIST-approved (Cryptographic Algorithm Validation Program).	3	Cryptography Test Case
5.3.2	**Key Management**		
	The following requirements apply to voting systems that generate cryptographic keys internally.		
5.3.2.1	Cryptographic keys generated by the voting system SHALL use a NIST-approved key generation method, or a published and credible key generation method.	3	Cryptography Test Case
5.3.2.2	Compromising the security of the key generation method (e.g., guessing the seed value to initialize the deterministic random number generator (RNG)) SHALL require as least as many operations as determining the value of the generated key.	N/T	
5.3.2.3	If a seed key is entered during the key generation process, entry of the key SHALL meet the key entry requirements in 5.3.3.1. If intermediate key generation values are output from the cryptographic module, the values SHALL be output either in encrypted form or under split knowledge procedures.	3	Cryptography Test Case
5.3.2.4	Cryptographic keys used to protect information in-transit over public telecommunication networks SHALL use NIST-approved key generation methods. If the approved key generation method requires input from a random number generator, then an approved (FIPS 140-2) random number generator SHALL be used.	3	Cryptography Test Case
5.3.2.5	Random number generators used to generate cryptographic keys SHALL implement one or more health tests that provide assurance that the random number generator continues to operate as intended (e.g., the entropy source is not stuck).	3	Cryptography Test Case
5.3.3	**Key Establishment**		
	Key establishment may be performed by automated methods (e.g., use of a public key algorithm), manual methods (use of a manually transported key loading device), or a combination of automated and manual methods.		

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.3.3.1	Secret and private keys established using automated methods SHALL be entered into and output from a voting system in encrypted form. Secret and private keys established using manual methods may be entered into or output from a system in plaintext form.	3	Cryptography Test Case
5.3.4.1	Cryptographic keys stored within the voting system SHALL NOT be stored in plaintext. Keys stored outside the voting system SHALL be protected from disclosure or modification.	3	Cryptography Test Case
5.3.4.2	The voting system SHALL provide methods to zeroize all plaintext secret and private cryptographic keys within the system.	3	Cryptography Test Case
5.3.4.3	The voting system SHALL support the capability to reset cryptographic keys to new values.	3	Cryptography Test Case
5.4	**Voting System Integrity Management**		
	This section addresses the secure deployment and operation of the voting system, including the protection of removable media and protection against malicious software.		
5.4.1	**Protecting the Integrity of the Voting System**		
5.4.1.1	The integrity and authenticity of each individual cast vote SHALL be protected from any tampering or modification during transmission.	N/A	
5.4.1.2	The integrity and authenticity of each individual cast vote SHALL be preserved by means of a digital signature during storage.	N/A	
5.4.1.3	Cast vote data SHALL NOT be permanently stored on the vote capture device.	4	Normal Ballot Delivery Test Case
5.4.1.4	The integrity and authenticity of the electronic ballot box SHALL be protected by means of a digital signature.	N/A	
5.4.1.5	The voting system SHALL use malware detection software to protect against known malware that targets the operating system, services, and applications.	5	Discovery Penetration Test Case
5.4.1.6	The voting system SHALL provide a mechanism for updating malware detection signatures.	5	Discovery Penetration Test Case
5.4.1.7	The voting system SHALL provide the capability for kiosk workers to validate the software used on the vote capture devices as part of the daily initiation of kiosk operations.	N/A	
5.5	**Communications Security**		
	This section provides requirements for communications security. These requirements address ensuring the integrity of transmitted information and protecting the voting system from external communications-based threats.		

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.5.1	**Data Transmission Security**		
5.5.1.1	Voting systems that transmit data over communications links SHALL provide integrity protection for data in transit through the generation of integrity data (digital signatures and/or message authentication codes) for outbound traffic and verification of the integrity data for inbound traffic.	3	Cryptography Test Case
5.5.1.2	Voting systems SHALL use at a minimum TLS 1.0, SSL 3.1 or equivalent protocols, including all updates to both protocols and implementations as of the date of the submission (e.g., RFC 5746 for TLS 1.0).	11	Host Server Security Test Case
5.5.1.3	Voting systems deploying VPNs SHALL configure them to only allow FIPS-compliant cryptographic algorithms and cipher suites.	N/A	
5.5.1.4	Each communicating device SHALL have a unique system identifier.	11	Host Server Security Test Case
5.5.1.5	Each device SHALL mutually strongly authenticate using the system identifier before additional network data packets are processed.	11	Host Server Security Test Case
5.5.1.6	Data transmission SHALL preserve the secrecy of voters' ballot selections and SHALL prevent the violation of ballot secrecy and integrity.	5	Discovery Penetration Test Case
5.5.2	**External Threats**		
	Voting systems SHALL implement protections against external threats to which the system may be susceptible.	5	Discovery Penetration Test Case
5.5.2.1	Voting system components SHALL have the ability to enable or disable physical network interfaces.	1	Host Server Administration Test Case
5.5.2.2	The number of active ports and associated network services and protocols SHALL be restricted to the minimum required for the voting system to function.	11	Host Server Security Test Case
5.5.2.3	The voting system SHALL block all network connections that are not over a mutually authenticated channel.	11	Host Server Security Test Case
5.6	**Logging**		
5.6.1	**Log Management**		
5.6.1.1	The voting system SHALL implement default settings for secure log management activities, including log generation, transmission, storage, analysis, and disposal.	1	Host Server Administration Test Case
5.6.1.2	Logs SHALL only be accessible to authorized roles.	1	Host Server Administration Test Case
5.6.1.3	The voting system SHALL restrict log access to append-only for privileged logging processes and read-only for authorized roles.	1	Host Server Administration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.6.1.4	The voting system SHALL log logging failures, log clearing, and log rotation.	1	Host Server Administration Test Case
5.6.1.5	The voting system SHALL store log data in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format.	1	Host Server Administration Test Case
5.6.1.6	The voting system SHALL ensure that each jurisdiction's event logs and each component's logs are separable from each other.	N/A	
5.6.1.7	The voting system SHALL include an application or program to view, analyze, and search event logs.	1	Host Server Administration Test Case
5.6.1.8	All logs SHALL be preserved in a useable manner prior to voting system decommissioning.	1	Host Server Administration Test Case
5.6.1.9	Logs SHALL NOT contain any data that could violate the privacy of the voter's identity.	4	Normal Ballot Delivery Test Case
5.6.1.10	Timekeeping mechanisms SHALL generate time and date values, including hours, minutes, and seconds.	4	Normal Ballot Delivery Test Case
		1	Host Server Administration Test Case
5.6.1.11	The precision of the timekeeping mechanism SHALL be able to distinguish and properly order all log events.	4	Normal Ballot Delivery Test Case
5.6.1.12	Only the system administrator SHALL be permitted to set the system clock.	NA	
5.6.2	**Communication Logging**		
5.6.2.1	All communications actions SHALL be logged.	3	Cryptography Test Case
		5	Discovery Penetration Test Case
		4	Normal Ballot Delivery Test Case
		1	Host Server Administration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.6.2.2	The communications log SHALL contain at least the following entries: Times when the communications are activated and deactivated; Services accessed; Identification of the device which data was transmitted to or received from; Identification of authorized entity; and Successful and unsuccessful attempts to access communications or services.	5	Discovery Penetration Test Case
		4	Normal Ballot Delivery Test Case
5.6.3	**System Event Logging**		
	This section describes requirements for the voting system to perform event logging for system maintenance troubleshooting, recording the history of system activity, and detecting unauthorized or malicious activity. The operating system, and/or applications software may perform the actual event logging. There may be multiple logs in use for any system component.		
5.6.3.1	The voting system SHALL log the following data for each event: a. System ID; b. Unique event ID and/or type; c. Timestamp; d. Success or failure of event, if applicable; e. User ID triggering the event, if applicable; and f. Jurisdiction, if applicable.	7	Recovery From Hardware Error Test Case
		4	Normal Ballot Delivery Test Case
		1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.6.3.2	All critical events SHALL be recorded in the system event log.	5	Discovery Penetration Test Case
		4	Normal Ballot Delivery Test Case
		7	Recovery From Hardware Error Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.6.3.3	At a minimum the voting system SHALL log the events described in the table below. NOTE: See "Table 5-2 System Events" in document - page 71	4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case
		3	Cryptography Test Case
		1	Host Server Administration Test Case
		7	Recovery From Hardware Error Test Case
5.7	**Incident Response**		
5.7.1	**Incident Response Support**		
5.7.1.1	Manufacturers SHALL document what types of system operations or security events (e.g., failure of critical component, detection of malicious code, unauthorized access to restricted data) are classified as critical.	N/A	
5.7.1.2	An alarm that notifies appropriate personnel SHALL be generated on the vote capture device, system server, or tabulation device, depending upon which device has the error, if a critical event is detected.	N/A	
5.8	**Physical and Environmental Security**		
5.8.1	**Physical Access**		
5.8.1.1	Any unauthorized physical access SHALL leave physical evidence that an unauthorized event has taken place.	N/A	
5.8.2.1	The voting system SHALL disable physical ports and access points that are not essential to voting operations, testing, and auditing.	11	Host Server Security Test Case
5.8.3.1	If a physical connection between the vote capture device and a component is broken, the affected vote capture device port SHALL be automatically disabled.	N/A	
5.8.3.2	The voting system SHALL produce a visual alarm if a connected component is physically disconnected.	N/A	
5.8.3.3	An event log entry that identifies the name of the affected device SHALL be generated if a vote capture device component is disconnected.	7	Recovery From Hardware Error Test Case
5.8.3.4	Disabled ports SHALL only be re-enabled by authorized administrators.	1	Host Server Administration Test Case
5.8.3.5	Vote capture devices SHALL be designed with the capability to restrict physical access to voting device ports that accommodate removable media with the exception of ports used to activate a voting session.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.8.3.6	Vote capture devices SHALL be designed to give a physical indication of tampering or unauthorized access to ports and all other access points, if used as described in the manufacturer's documentation.	N/A	
5.8.3.7	Vote capture devices SHALL be designed such that physical ports can be manually disabled by an authorized administrator.	N/A	
5.8.4	**Door Cover and Panel Security**		
5.8.4.1	Access points such as covers and panels SHALL be secured by locks or tamper evident or tamper resistant countermeasures and SHALL be implemented so that kiosk workers can monitor access to vote capture device components through these points.	N/A	
5.8.5	**Secure Paper Record Receptacle**		
	If the voting system provides paper record containers then they SHALL be designed such that any unauthorized physical access results in physical evidence that an unauthorized event has taken place.	N/A	
5.8.6	**Secure Physical Lock and Key**		
5.8.6.1	Voting equipment SHALL be designed with countermeasures that provide physical indication that unauthorized attempts have been made to access locks installed for security purposes.	N/A	
5.8.6.2	Manufacturers SHALL provide locking systems for securing vote capture devices that can make use of keys that are unique to each owner.	N/A	
5.8.7	**Media Protection**		
	These requirements apply to all media, both paper and digital, that contain personal privacy related data or other protected or sensitive types of information.		
5.8.7.1	The voting system SHALL meet the following requirements: a. All paper records (including rejected ones) printed at the kiosk locations SHALL be deposited in a secure container; b. Vote capture device hardware, software and sensitive information (e.g., electoral roll) SHALL be physically protected to prevent unauthorized modification or disclosure; and c. Vote capture device hardware components, peripherals and removable media SHALL be identified and registered by means of a unique serial number or other identifier.	N/A	
5.9	**Penetration Resistance**		
5.9.1	**Resistance to Penetration Attempts**		
5.9.1.1	The voting system SHALL be resistant to attempts to penetrate the system by any remote unauthorized entity.	5	Discovery Penetration Test Case
		11	Host Server Security Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.9.1.2	The voting system SHALL be configured to minimize ports, responses and information disclosure about the system while still providing appropriate functionality.	5	Discovery Penetration Test Case
		11	Host Server Security Test Case
5.9.1.3	The voting system SHALL provide no access, information or services to unauthorized entities.	5	Discovery Penetration Test Case
		1	Host Server Administration Test Case
5.9.1.4	All interfaces SHALL be penetration resistant including TCP/IP, wireless, and modems from any point in the system.	11	Host Server Security Test Case
5.9.1.5	The configuration and setup to attain penetration resistance SHALL be clearly and completely documented.	N/A	
5.9.2.1	The scope of penetration testing SHALL include all the voting system components. The scope of penetration testing includes but is not limited to the following: System server; Vote capture devices; Tabulation device; All items setup and configured per Technical Data Package (TDP) recommendations; Local wired and wireless networks; and 03/09/2011 Internet connections.	5	Discovery Penetration Test Case
5.9.2.2	Penetration testing SHALL be conducted on a voting system set up in a controlled lab environment. Setup and configuration SHALL be conducted in accordance with the TDP, and SHALL replicate the real world environment in which the voting system will be used.	N/A	
5.9.2.3	The penetration testing team SHALL conduct white box testing using manufacturer supplied documentation and voting system architecture information. Documentation includes the TDP and user documentation. The testing team SHALL have access to any relevant information regarding the voting system configuration. This includes, but is not limited to, network layout and Internet Protocol addresses for system devices and components. The testing team SHALL be provided any source code included in the TDP.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.9.2.04	Penetration testing seeks out vulnerabilities in the voting system that might be used to change the outcome of an election, interfere with voter ability to cast ballots, ballot counting, or compromise ballot secrecy. The penetration testing team SHALL prioritize testing efforts based on the following: a. Threat scenarios for the voting system under investigation; b. Remote attacks SHALL be prioritized over in-person attacks; c. Attacks with a large impact SHALL be prioritized over attacks with a more narrow impact; and d. Attacks that can change the outcome of an election SHALL be prioritized over attacks that compromise ballot secrecy or cause non-selective denial of service.	5	Discovery Penetration Test Case

[redacted]

REQUIREMENTS MATRIX

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted]Functional Requirements Matrix	Test Case No.	Test Case Description
Section 5	**Security**		
5.1	**Access Control**		
	This section states requirements for the identification of authorized system users, processes and devices and the authentication or verification of those identities as a prerequisite to granting access to system processes and data. It also includes requirements to limit and control access to critical system components to protect system and data integrity, availability, confidentiality, and accountability. This section applies to all entities attempting to physically enter voting system facilities or to request services or data from the voting system.		
5.1.1	**Separation of Duties**		
5.1.1.1	The voting system SHALL allow the definition of personnel roles with segregated duties and responsibilities on critical processes to prevent a single person from compromising the integrity of the system.	1	Host Server Administration Test Case
5.1.1.2	The voting system SHALL ensure that only authorized roles, groups, or individuals have access to election data.	1	Host Server Administration Test Case
5.1.1.3	The voting system SHALL require at least two persons from a predefined group for validating the election configuration information, accessing the cast vote records, and starting the tabulation process..	N/A	
5.1.2	**Voting System Access**		
	The voting system SHALL provide access control mechanisms designed to permit authorized access and to prevent unauthorized access to the system.	5	Discovery Penetration Test Case
		1	Host Server Administration Test Case
5.1.2.1	The voting system SHALL identify and authenticate each person to whom access is granted, and the specific functions and data to which each person holds authorized access.	1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
5.1.2.2	The voting system SHALL allow the administrator group or role to configure permissions and functionality for each identity, group or role to include account and group/role creation, modification, and deletion.	1	Host Server Administration Test Case
5.1.2.3	The voting system's default access control permissions SHALL implement the least privileged role or group needed.	1	Host Server Administration Test Case
5.1.2.4	The voting system SHALL prevent a lower-privilege process from modifying a higher-privilege process.	1	Host Server Administration Test Case
5.1.2.5	The voting system SHALL NOT require its execution as an operating system privileged account and SHALL NOT require the use of an operating system privileged account for its operation.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.1.2.6	The voting system SHALL log the identification of all personnel accessing or attempting to access the voting system to the system event log.	1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case
5.1.2.7	The *(voting system)* SHALL provide tools for monitoring access to the system. These tools SHALL provide specific users real time display of persons accessing the system as well as reports from logs.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.1.2.8	Vote capture device located at the remote voting location and the central server SHALL have the capability to restrict access to the voting system after a preset number of login failures. a. The lockout threshold SHALL be configurable by appropriate administrators/operators b. The voting system SHALL log the event c. The voting system SHALL immediately send a notification to appropriate administrators/operators of the event. d. The voting system SHALL provide a mechanism for the appropriate administrators/operators to reactivate the account after appropriate confirmation.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.1.2.9	The voting system SHALL log a notification when any account has been locked out.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.1.2.10	Authenticated sessions on critical processes SHALL have an inactivity time-out control that will require personnel re-authentication when reached. This time-out SHALL be implemented for administration and monitor consoles on all voting system devices.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.1.2.11	Authenticated sessions on critical processes SHALL have a screen-lock functionality that can be manually invoked.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.2	**Identification and Authentication**		
	Authentication mechanisms and their associated strength may vary from one voting system capability and architecture to another but all must meet the minimum requirement to maintain integrity and trust. It is important to consider a range of roles individuals may assume when operating different components in the voting system and each may require different authentication mechanisms. The requirements described in this section vary from role to role. For instance, a kiosk worker will have different identification and authentication characteristics than a voter. Also, for selected critical functions there may be cases where split knowledge or dual authorization is necessary to ensure security. This is especially relevant for critical cryptographic key management functions.		
5.2.1	**Authentication**		
5.2.1.1	Authentication mechanisms supported by the voting system SHALL support authentication strength of at least 1/1,000,000.	11	Host Server Security Test Case
5.2.1.2	The voting system SHALL authenticate users per the minimum authentication methods outlined below. Refer to document for the table layout: http://www.eac.gov/assets/1/AssetManager/UOCAVA_Pilot_Program_Requirments-03.24.10.pdf Table 5-1 Roles : Section 5 | Page 59	11	Host Server Security Test Case
5.2.1.3	The voting system SHALL provide multiple authentication methods to support multi-factor authentication.	4	Normal Ballot Delivery Test Case
		11	Host Server Security Test Case
5.2.1.4	When private or secret authentication data is stored by the voting system, it SHALL be protected to ensure that the confidentiality and integrity of the data are not violated.	11	Host Server Security Test Case
5.2.1.5	The voting system SHALL provide a mechanism to reset a password if it is forgotten, in accordance with the system access/security policy.	1	Host Server Administration Test Case
5.2.1.6	The voting system SHALL allow the administrator group or role to specify password strength for all accounts including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters per NIST 800-63 Electronic Authentication Guideline Standards.	1	Host Server Administration Test Case
5.2.1.7	The voting system SHALL enforce password histories and allow the administrator to configure the history length when passwords are stored by the system.	1	Host Server Administration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.2.1.8	The voting system SHALL ensure that the user name is not used in the password.	1	Host Server Administration Test Case
5.2.1.9	The voting system SHALL provide a means to automatically expire passwords.	1	Host Server Administration Test Case
5.2.1.10	The voting system servers and vote capture devices SHALL identify and authenticate one another using NIST - approved cryptographic authentication methods at the 112 bits of security.	3	Cryptography Test Case
5.2.1.11	Remote voting location site Virtual Private Network (VPN) connections (i.e., vote capture devices) to voting servers SHALL be authenticated using strong mutual cryptographic authentication at the 112 bits of security.	N/A	
5.2.1.12	Message authentication SHALL be used for applications to protect the integrity of the message content using a schema with 112 bits of security.	11	Host Server Security Test Case
5.2.1.13	IPsec, SSL, or TLS and MAC mechanisms SHALL all be configured to be compliant with FIPS 140-2 using approved algorithm suites and protocols.	3	Cryptography Test Case
5.3	**Cryptography**		
	Cryptography serves several purposes in voting systems. They include: Confidentiality: where necessary the confidentiality of voting records can be provided by encryption; Authentication: data and programs can be authenticated by a digital signature or message authentication codes (MAC), or by comparison of the cryptographic hashes of programs or data with the reliably known hash values of the program or data. If the program or data are altered, then that alteration is detected when the signature or MAC is verified, or the hash on the data or program is compared to the known hash value. Typically the programs loaded on voting systems and the ballot definitions used by voting systems are verified by the systems, while systems apply digital signatures to authenticate the critical audit data that they output. For remote connections cryptographic user authentication mechanism SHALL be based on strong authentication methods; and Random number generation: random numbers are used for several purposes including the creation of cryptographic keys for cryptographic algorithms and methods to provide the services listed above, and as identifiers for voting records that can be used to identify or correlate the records without providing any information that could identify the voter.		
5.3.1	**General Cryptography Requirements**		
5.3.1.1	All cryptographic functionality SHALL be implemented using NIST-approved cryptographic algorithms/schemas, or use published and credible cryptographic algorithms/schemas/protocols.	3	Cryptography Test Case
5.3.1.2	Cryptographic algorithms and schemas SHALL be implemented with a security strength equivalent to at least 112 bits of security to protect sensitive voting information and election records.	3	Cryptography Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.3.1.3	Cryptography used to protect information in-transit over public telecommunication networks SHALL use NIST-approved algorithms and cipher suites. In addition the implementations of these algorithms SHALL be NIST-approved (Cryptographic Algorithm Validation Program).	3	Cryptography Test Case
5.3.2	**Key Management**		
	The following requirements apply to voting systems that generate cryptographic keys internally.		
5.3.2.1	Cryptographic keys generated by the voting system SHALL use a NIST-approved key generation method, or a published and credible key generation method.	3	Cryptography Test Case
5.3.2.2	Compromising the security of the key generation method (e.g., guessing the seed value to initialize the deterministic random number generator (RNG)) SHALL require as least as many operations as determining the value of the generated key.	N/T	
5.3.2.3	If a seed key is entered during the key generation process, entry of the key SHALL meet the key entry requirements in 5.3.3.1. If intermediate key generation values are output from the cryptographic module, the values SHALL be output either in encrypted form or under split knowledge procedures.	3	Cryptography Test Case
5.3.2.4	Cryptographic keys used to protect information in-transit over public telecommunication networks SHALL use NIST-approved key generation methods. If the approved key generation method requires input from a random number generator, then an approved (FIPS 140-2) random number generator SHALL be used.	3	Cryptography Test Case
5.3.2.5	Random number generators used to generate cryptographic keys SHALL implement one or more health tests that provide assurance that the random number generator continues to operate as intended (e.g., the entropy source is not stuck).	3	Cryptography Test Case
5.3.3	**Key Establishment**		
	Key establishment may be performed by automated methods (e.g., use of a public key algorithm), manual methods (use of a manually transported key loading device), or a combination of automated and manual methods.		
5.3.3.1	Secret and private keys established using automated methods SHALL be entered into and output from a voting system in encrypted form. Secret and private keys established using manual methods may be entered into or output from a system in plaintext form.	3	Cryptography Test Case
5.3.4.1	Cryptographic keys stored within the voting system SHALL NOT be stored in plaintext. Keys stored outside the voting system SHALL be protected from disclosure or modification.	3	Cryptography Test Case
5.3.4.2	The voting system SHALL provide methods to zeroize all plaintext secret and private cryptographic keys within the system.	3	Cryptography Test Case
5.3.4.3	The voting system SHALL support the capability to reset cryptographic keys to new values.	3	Cryptography Test Case
5.4	**Voting System Integrity Management**		
	This section addresses the secure deployment and operation of the voting system, including the protection of removable media and protection against malicious software.		

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.4.1	**Protecting the Integrity of the Voting System**		
5.4.1.1	The integrity and authenticity of each individual cast vote SHALL be protected from any tampering or modification during transmission.	N/A	
5.4.1.2	The integrity and authenticity of each individual cast vote SHALL be preserved by means of a digital signature during storage.	N/A	
5.4.1.3	Cast vote data SHALL NOT be permanently stored on the vote capture device.	4	Normal Ballot Delivery Test Case
5.4.1.4	The integrity and authenticity of the electronic ballot box SHALL be protected by means of a digital signature.	N/A	
5.4.1.5	The voting system SHALL use malware detection software to protect against known malware that targets the operating system, services, and applications.	5	Discovery Penetration Test Case
5.4.1.6	The voting system SHALL provide a mechanism for updating malware detection signatures.	5	Discovery Penetration Test Case
5.4.1.7	The voting system SHALL provide the capability for kiosk workers to validate the software used on the vote capture devices as part of the daily initiation of kiosk operations.	N/A	
5.5	**Communications Security**		
	This section provides requirements for communications security. These requirements address ensuring the integrity of transmitted information and protecting the voting system from external communications-based threats.		
5.5.1	**Data Transmission Security**		
5.5.1.1	Voting systems that transmit data over communications links SHALL provide integrity protection for data in transit through the generation of integrity data (digital signatures and/or message authentication codes) for outbound traffic and verification of the integrity data for inbound traffic.	11	Host Server Security Test Case
5.5.1.2	Voting systems SHALL use at a minimum TLS 1.0, SSL 3.1 or equivalent protocols, including all updates to both protocols and implementations as of the date of the submission (e.g., RFC 5746 for TLS 1.0).	3	Cryptography Test Case
5.5.1.3	Voting systems deploying VPNs SHALL configure them to only allow FIPS-compliant cryptographic algorithms and cipher suites.	N/A	
5.5.1.4	Each communicating device SHALL have a unique system identifier.	11	Host Server Security Test Case
5.5.1.5	Each device SHALL mutually strongly authenticate using the system identifier before additional network data packets are processed.	11	Host Server Security Test Case
5.5.1.6	Data transmission SHALL preserve the secrecy of voters' ballot selections and SHALL prevent the violation of ballot secrecy and integrity.	5	Discovery Penetration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.5.2	**External Threats**		
	Voting systems SHALL implement protections against external threats to which the system may be susceptible.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.5.2.1	Voting system components SHALL have the ability to enable or disable physical network interfaces.	1	Host Server Administration Test Case
5.5.2.2	The number of active ports and associated network services and protocols SHALL be restricted to the minimum required for the voting system to function.	11	Host Server Security Test Case
5.5.2.3	The voting system SHALL block all network connections that are not over a mutually authenticated channel.	11	Host Server Security Test Case
5.6	**Logging**		
5.6.1	**Log Management**		
5.6.1.1	The voting system SHALL implement default settings for secure log management activities, including log generation, transmission, storage, analysis, and disposal.	1	Host Server Administration Test Case
5.6.1.2	Logs SHALL only be accessible to authorized roles.	1	Host Server Administration Test Case
5.6.1.3	The voting system SHALL restrict log access to append-only for privileged logging processes and read-only for authorized roles.	1	Host Server Administration Test Case
5.6.1.4	The voting system SHALL log logging failures, log clearing, and log rotation.	1	Host Server Administration Test Case
5.6.1.5	The voting system SHALL store log data in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format.	1	Host Server Administration Test Case
5.6.1.6	The voting system SHALL ensure that each jurisdiction's event logs and each component's logs are separable from each other.	N/A	
5.6.1.7	The voting system SHALL include an application or program to view, analyze, and search event logs.	1	Host Server Administration Test Case
5.6.1.8	All logs SHALL be preserved in a useable manner prior to voting system decommissioning.	1	Host Server Administration Test Case
5.6.1.9	Logs SHALL NOT contain any data that could violate the privacy of the voter's identity.	4	Normal Ballot Delivery Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.6.1.10	Timekeeping mechanisms SHALL generate time and date values, including hours, minutes, and seconds.	4	Normal Ballot Delivery Test Case
		1	Host Server Administration Test Case
		10	Local Ballot Delivery Test Case
5.6.1.11	The precision of the timekeeping mechanism SHALL be able to distinguish and properly order all log events.	4	Normal Ballot Delivery Test Case
5.6.1.12	Only the system administrator SHALL be permitted to set the system clock.	N/A	
5.6.2	**Communication Logging**		
5.6.2.1	All communications actions SHALL be logged.	4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case
		1	Host Server Administration Test Case
5.6.2.2	The communications log SHALL contain at least the following entries: Times when the communications are activated and deactivated; Services accessed; Identification of the device which data was transmitted to or received from; Identification of authorized entity; and Successful and unsuccessful attempts to access communications or services.	4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case
5.6.3	**System Event Logging**		
	This section describes requirements for the voting system to perform event logging for system maintenance troubleshooting, recording the history of system activity, and detecting unauthorized or malicious activity. The operating system, and/or applications software may perform the actual event logging. There may be multiple logs in use for any system component.		

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.6.3.1	The voting system SHALL log the following data for each event: a. System ID; b. Unique event ID and/or type; c. Timestamp; d. Success or failure of event, if applicable; e. User ID triggering the event, if applicable; and f. Jurisdiction, if applicable.	1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
		7	Recovery form hardware error Test Case
		5	Discovery Penetration Test Case
5.6.3.2	All critical events SHALL be recorded in the system event log.	5	Discovery Penetration Test Case
		4	Normal Ballot Delivery Test Case
		7	Recovery form hardware error Test Case
5.6.3.3	At a minimum the voting system SHALL log the events described in the table below. NOTE: See "Table 5-2 System Events" in document - page 71	1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case
		7	Recovery form hardware error Test Case
5.7	**Incident Response**		
5.7.1	**Incident Response Support**		
5.7.1.1	Manufacturers SHALL document what types of system operations or security events (e.g., failure of critical component, detection of malicious code, unauthorized access to restricted data) are classified as critical.	N/A	
5.7.1.2	An alarm that notifies appropriate personnel SHALL be generated on the vote capture device, system server, or tabulation device, depending upon which device has the error, if a critical event is detected.	N/A	
5.8	**Physical and Environmental Security**		
5.8.1	**Physical Access**		
5.8.1.1	Any unauthorized physical access SHALL leave physical evidence that an unauthorized event has taken place.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.8.2.1	The voting system SHALL disable physical ports and access points that are not essential to voting operations, testing, and auditing.	11	Host Server Security Test Case
5.8.3.1	If a physical connection between the vote capture device and a component is broken, the affected vote capture device port SHALL be automatically disabled.	N/A	
5.8.3.2	The voting system SHALL produce a visual alarm if a connected component is physically disconnected.	N/A	
5.8.3.3	An event log entry that identifies the name of the affected device SHALL be generated if a vote capture device component is disconnected.	7	Recovery form hardware error Test Case
5.8.3.4	Disabled ports SHALL only be re-enabled by authorized administrators.	1	Host Server Administration Test Case
5.8.3.5	Vote capture devices SHALL be designed with the capability to restrict physical access to voting device ports that accommodate removable media with the exception of ports used to activate a voting session.	N/A	
5.8.3.6	Vote capture devices SHALL be designed to give a physical indication of tampering or unauthorized access to ports and all other access points, if used as described in the manufacturer's documentation.	N/A	
5.8.3.7	Vote capture devices SHALL be designed such that physical ports can be manually disabled by an authorized administrator.	N/A	
5.8.4	**Door Cover and Panel Security**		
5.8.4.1	Access points such as covers and panels SHALL be secured by locks or tamper evident or tamper resistant countermeasures and SHALL be implemented so that kiosk workers can monitor access to vote capture device components through these points.	N/A	
5.8.5	**Secure Paper Record Receptacle**		
	If the voting system provides paper record containers then they SHALL be designed such that any unauthorized physical access results in physical evidence that an unauthorized event has taken place.	N/A	
5.8.6	**Secure Physical Lock and Key**		
5.8.6.1	Voting equipment SHALL be designed with countermeasures that provide physical indication that unauthorized attempts have been made to access locks installed for security purposes.	N/A	
5.8.6.2	Manufacturers SHALL provide locking systems for securing vote capture devices that can make use of keys that are unique to each owner.	N/A	
5.8.7	**Media Protection**		
	These requirements apply to all media, both paper and digital, that contain personal privacy related data or other protected or sensitive types of information.		

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.8.7.1	The voting system SHALL meet the following requirements: a. All paper records (including rejected ones) printed at the kiosk locations SHALL be deposited in a secure container; b. Vote capture device hardware, software and sensitive information (e.g., electoral roll) SHALL be physically protected to prevent unauthorized modification or disclosure; and c. Vote capture device hardware components, peripherals and removable media SHALL be identified and registered by means of a unique serial number or other identifier.	N/A	
5.9	**Penetration Resistance**		
5.9.1	**Resistance to Penetration Attempts**		
5.9.1.1	The voting system SHALL be resistant to attempts to penetrate the system by any remote unauthorized entity.	5	Discovery Penetration Test Case
		11	Host Server Security Test Case
5.9.1.2	The voting system SHALL be configured to minimize ports, responses and information disclosure about the system while still providing appropriate functionality.	5	Discovery Penetration Test Case
		11	Host Server Security Test Case
5.9.1.3	The voting system SHALL provide no access, information or services to unauthorized entities.	5	Discovery Penetration Test Case
		1	Host Server Administration Test Case
5.9.1.4	All interfaces SHALL be penetration resistant including TCP/IP, wireless, and modems from any point in the system.	11	Host Server Security Test Case
5.9.1.5	The configuration and setup to attain penetration resistance SHALL be clearly and completely documented.	N/A	
5.9.2.1	The scope of penetration testing SHALL include all the voting system components. The scope of penetration testing includes but is not limited to the following: System server; Vote capture devices; Tabulation device; All items setup and configured per Technical Data Package (TDP) recommendations; Local wired and wireless networks; and03/09/2011 Internet connections.	5	Discovery Penetration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.9.2.2	Penetration testing SHALL be conducted on a voting system set up in a controlled lab environment. Setup and configuration SHALL be conducted in accordance with the TDP, and SHALL replicate the real world environment in which the voting system will be used.	N/A	
5.9.2.3	The penetration testing team SHALL conduct white box testing using manufacturer supplied documentation and voting system architecture information. Documentation includes the TDP and user documentation. The testing team SHALL have access to any relevant information regarding the voting system configuration. This includes, but is not limited to, network layout and Internet Protocol addresses for system devices and components. The testing team SHALL be provided any source code included in the TDP.	N/A	
5.9.2.04	Penetration testing seeks out vulnerabilities in the voting system that might be used to change the outcome of an election, interfere with voter ability to cast ballots, ballot counting, or compromise ballot secrecy. The penetration testing team SHALL prioritize testing efforts based on the following: a. Threat scenarios for the voting system under investigation; b. Remote attacks SHALL be prioritized over in-person attacks; c. Attacks with a large impact SHALL be prioritized over attacks with a more narrow impact; and d. Attacks that can change the outcome of an election SHALL be prioritized over attacks that compromise ballot secrecy or cause non-selective denial of service.	5	Discovery Penetration Test Case

[redacted]

REQUIREMENTS MATRIX

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
Section 5	**Security**		
5.1	**Access Control**		
	This section states requirements for the identification of authorized system users, processes and devices and the authentication or verification of those identities as a prerequisite to granting access to system processes and data. It also includes requirements to limit and control access to critical system components to protect system and data integrity, availability, confidentiality, and accountability. This section applies to all entities attempting to physically enter voting system facilities or to request services or data from the voting system.		
5.1.1	**Separation of Duties**		
5.1.1.1	The voting system SHALL allow the definition of personnel roles with segregated duties and responsibilities on critical processes to prevent a single person from compromising the integrity of the system.	1	Host Server Administration Test Case
5.1.1.2	The voting system SHALL ensure that only authorized roles, groups, or individuals have access to election data.	1	Host Server Administration Test Case
5.1.1.3	The voting system SHALL require at least two persons from a predefined group for validating the election configuration information, accessing the cast vote records, and starting the tabulation process..	N/A	
5.1.2	**Voting System Access**		
	The voting system SHALL provide access control mechanisms designed to permit authorized access and to prevent unauthorized access to the system.	5	Discovery Penetration Test Case
		1	Host Server Administration Test Case
5.1.2.1	The voting system SHALL identify and authenticate each person to whom access is granted, and the specific functions and data to which each person holds authorized access.	1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
5.1.2.2	The voting system SHALL allow the administrator group or role to configure permissions and functionality for each identity, group or role to include account and group/role creation, modification, and deletion.	1	Host Server Administration Test Case
5.1.2.3	The voting system's default access control permissions SHALL implement the least privileged role or group needed.	1	Host Server Administration Test Case
5.1.2.4	The voting system SHALL prevent a lower-privilege process from modifying a higher-privilege process.	1	Host Server Administration Test Case
5.1.2.5	The voting system SHALL NOT require its execution as an operating system privileged account and SHALL NOT require the use of an operating system privileged account for its operation.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.1.2.6	The voting system SHALL log the identification of all personnel accessing or attempting to access the voting system to the system event lo g.	7	Recovery form hardware error Test Case
		1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case
5.1.2.7	The *(voting system)* SHALL provide tools for monitoring access to the system. These tools SHALL provide specific users real time display of persons accessing the system as well as reports from logs.	1	Host Server Administration Test Case
5.1.2.8	Vote capture device located at the remote voting location and the central server SHALL have the capability to restrict access to the voting system after a preset number of login failures. a. The lockout threshold SHALL be configurable by appropriate administrators/operators b. The voting system SHALL log the event c. The voting system SHALL immediately send a notification to appropriate administrators/operators of the event. d. The voting system SHALL provide a mechanism for the appropriate administrators/operators to reactivate the account after appropriate confirmation.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.1.2.9	The voting system SHALL log a notification when any account has been locked out.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.1.2.10	Authenticated sessions on critical processes SHALL have an inactivity time-out control that will require personnel re-authentication when reached. This time-out SHALL be implemented for administration and monitor consoles on all voting system devices.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.1.2.11	Authenticated sessions on critical processes SHALL have a screen-lock functionality that can be manually invoked.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.2	**Identification and Authentication**		
	Authentication mechanisms and their associated strength may vary from one voting system capability and architecture to another but all must meet the minimum requirement to maintain integrity and trust. It is important to consider a range of roles individuals may assume when operating different components in the voting system and each may require different authentication mechanisms. The requirements described in this section vary from role to role. For instance, a kiosk worker will have different identification and authentication characteristics than a voter. Also, for selected critical functions there may be cases where split knowledge or dual authorization is necessary to ensure security. This is especially relevant for critical cryptographic key management functions.		
5.2.1	**Authentication**		
5.2.1.1	Authentication mechanisms supported by the voting system SHALL support authentication strength of at least 1/1,000,000.	11	Host Server Security Test Case
5.2.1.2	The voting system SHALL authenticate users per the minimum authentication methods outlined below. Refer to document for the table layout: http://www.eac.gov/assets/1/AssetManager/UOCAVA_Pilot_Program_Requirments-03.24.10.pdf Table 5-1 Roles : Section 5 | Page 59	11	Host Server Security Test Case
5.2.1.3	The voting system SHALL provide multiple authentication methods to support multi-factor authentication.	1	Host Server Administration Test Case
5.2.1.4	When private or secret authentication data is stored by the voting system, it SHALL be protected to ensure that the confidentiality and integrity of the data are not violated.	11	Host Server Security Test Case
5.2.1.5	The voting system SHALL provide a mechanism to reset a password if it is forgotten, in accordance with the system access/security policy.	1	Host Server Administration Test Case
5.2.1.6	The voting system SHALL allow the administrator group or role to specify password strength for all accounts including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters per NIST 800-63 Electronic Authentication Guideline Standards.	1	Host Server Administration Test Case
5.2.1.7	The voting system SHALL enforce password histories and allow the administrator to configure the history length when passwords are stored by the system.	1	Host Server Administration Test Case
5.2.1.8	The voting system SHALL ensure that the user name is not used in the password.	1	Host Server Administration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.2.1.9	The voting system SHALL provide a means to automatically expire passwords.	1	Host Server Administration Test Case
5.2.1.10	The voting system servers and vote capture devices SHALL identify and authenticate one another using NIST - approved cryptographic authentication methods at the 112 bits of security.	3	Cryptography Test Case
5.2.1.11	Remote voting location site Virtual Private Network (VPN) connections (i.e., vote capture devices) to voting servers SHALL be authenticated using strong mutual cryptographic authentication at the 112 bits of security.	N/A	
5.2.1.12	Message authentication SHALL be used for applications to protect the integrity of the message content using a schema with 112 bits of security.	11	Host Server Security Test Case
5.2.1.13	IPsec, SSL, or TLS and MAC mechanisms SHALL all be configured to be compliant with FIPS 140-2 using approved algorithm suites and protocols.	3	Cryptography Test Case
5.3	**Cryptography**		
	Cryptography serves several purposes in voting systems. They include: Confidentiality: where necessary the confidentiality of voting records can be provided by encryption; Authentication: data and programs can be authenticated by a digital signature or message authentication codes (MAC), or by comparison of the cryptographic hashes of programs or data with the reliably known hash values of the program or data. If the program or data are altered, then that alteration is detected when the signature or MAC is verified, or the hash on the data or program is compared to the known hash value. Typically the programs loaded on voting systems and the ballot definitions used by voting systems are verified by the systems, while systems apply digital signatures to authenticate the critical audit data that they output. For remote connections cryptographic user authentication mechanism SHALL be based on strong authentication methods; and Random number generation: random numbers are used for several purposes including the creation of cryptographic keys for cryptographic algorithms and methods to provide the services listed above, and as identifiers for voting records that can be used to identify or correlate the records without providing any information that could identify the voter.		
5.3.1	**General Cryptography Requirements**		
5.3.1.1	All cryptographic functionality SHALL be implemented using NIST-approved cryptographic algorithms/schemas, or use published and credible cryptographic algorithms/schemas/protocols.	3	Cryptography Test Case
5.3.1.2	Cryptographic algorithms and schemas SHALL be implemented with a security strength equivalent to at least 112 bits of security to protect sensitive voting information and election records.	3	Cryptography Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.3.1.3	Cryptography used to protect information in-transit over public telecommunication networks SHALL use NIST-approved algorithms and cipher suites. In addition the implementations of these algorithms SHALL be NIST-approved (Cryptographic Algorithm Validation Program).	3	Cryptography Test Case
5.3.2	**Key Management**		
	The following requirements apply to voting systems that generate cryptographic keys internally.		
5.3.2.1	Cryptographic keys generated by the voting system SHALL use a NIST-approved key generation method, or a published and credible key generation method.	3	Cryptography Test Case
5.3.2.2	Compromising the security of the key generation method (e.g., guessing the seed value to initialize the deterministic random number generator (RNG)) SHALL require as least as many operations as determining the value of the generated key.	N/T	
5.3.2.3	If a seed key is entered during the key generation process, entry of the key SHALL meet the key entry requirements in 5.3.3.1. If intermediate key generation values are output from the cryptographic module, the values SHALL be output either in encrypted form or under split knowledge procedures.	3	Cryptography Test Case
5.3.2.4	Cryptographic keys used to protect information in-transit over public telecommunication networks SHALL use NIST-approved key generation methods. If the approved key generation method requires input from a random number generator, then an approved (FIPS 140-2) random number generator SHALL be used.	3	Cryptography Test Case
5.3.2.5	Random number generators used to generate cryptographic keys SHALL implement one or more health tests that provide assurance that the random number generator continues to operate as intended (e.g., the entropy source is not stuck).	3	Cryptography Test Case
5.3.3	**Key Establishment**		
	Key establishment may be performed by automated methods (e.g., use of a public key algorithm), manual methods (use of a manually transported key loading device), or a combination of automated and manual methods.		
5.3.3.1	Secret and private keys established using automated methods SHALL be entered into and output from a voting system in encrypted form. Secret and private keys established using manual methods may be entered into or output from a system in plaintext form.	3	Cryptography Test Case
5.3.4.1	Cryptographic keys stored within the voting system SHALL NOT be stored in plaintext. Keys stored outside the voting system SHALL be protected from disclosure or modification.	3	Cryptography Test Case
5.3.4.2	The voting system SHALL provide methods to zeroize all plaintext secret and private cryptographic keys within the system.	3	Cryptography Test Case
5.3.4.3	The voting system SHALL support the capability to reset cryptographic keys to new values.	3	Cryptography Test Case
5.4	**Voting System Integrity Management**		
	This section addresses the secure deployment and operation of the voting system, including the protection of removable media and protection against malicious software.		

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.4.1	**Protecting the Integrity of the Voting System**		
5.4.1.1	The integrity and authenticity of each individual cast vote SHALL be protected from any tampering or modification during transmission.	N/A	
5.4.1.2	The integrity and authenticity of each individual cast vote SHALL be preserved by means of a digital signature during storage.	N/A	
5.4.1.3	Cast vote data SHALL NOT be permanently stored on the vote capture device.	4	Normal Ballot Delivery Test Case
5.4.1.4	The integrity and authenticity of the electronic ballot box SHALL be protected by means of a digital signature.	N/A	
5.4.1.5	The voting system SHALL use malware detection software to protect against known malware that targets the operating system, services, and applications.	5	Discovery Penetration Test Case
5.4.1.6	The voting system SHALL provide a mechanism for updating malware detection signatures.	5	Discovery Penetration Test Case
5.4.1.7	The voting system SHALL provide the capability for kiosk workers to validate the software used on the vote capture devices as part of the daily initiation of kiosk operations.	N/A	
5.5	**Communications Security**		
	This section provides requirements for communications security. These requirements address ensuring the integrity of transmitted information and protecting the voting system from external communications-based threats.		
5.5.1	**Data Transmission Security**		
5.5.1.1	Voting systems that transmit data over communications links SHALL provide integrity protection for data in transit through the generation of integrity data (digital signatures and/or message authentication codes) for outbound traffic and verification of the integrity data for inbound traffic.	11	Host Server Security Test Case
5.5.1.2	Voting systems SHALL use at a minimum TLS 1.0, SSL 3.1 or equivalent protocols, including all updates to both protocols and implementations as of the date of the submission (e.g., RFC 5746 for TLS 1.0).	11	Host Server Security Test Case
5.5.1.3	Voting systems deploying VPNs SHALL configure them to only allow FIPS-compliant cryptographic algorithms and cipher suites.	N/A	
5.5.1.4	Each communicating device SHALL have a unique system identifier.	11	Host Server Security Test Case
5.5.1.5	Each device SHALL mutually strongly authenticate using the system identifier before additional network data packets are processed.	11	Host Server Security Test Case
5.5.1.6	Data transmission SHALL preserve the secrecy of voters' ballot selections and SHALL prevent the violation of ballot secrecy and integrity.	5	Discovery Penetration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.5.2	**External Threats**		
	Voting systems SHALL implement protections against external threats to which the system may be susceptible.	1	Host Server Administration Test Case
		6	Remote Terminal Security Test Case
		5	Discovery Penetration Test Case
5.5.2.1	Voting system components SHALL have the ability to enable or disable physical network interfaces.	1	Host Server Administration Test Case
5.5.2.2	The number of active ports and associated network services and protocols SHALL be restricted to the minimum required for the voting system to function.	11	Host Server Security Test Case
5.5.2.3	The voting system SHALL block all network connections that are not over a mutually authenticated channel.	11	Host Server Security Test Case
5.6	**Logging**		
5.6.1	**Log Management**		
5.6.1.1	The voting system SHALL implement default settings for secure log management activities, including log generation, transmission, storage, analysis, and disposal.	1	Host Server Administration Test Case
5.6.1.2	Logs SHALL only be accessible to authorized roles.	1	Host Server Administration Test Case
5.6.1.3	The voting system SHALL restrict log access to append-only for privileged logging processes and read-only for authorized roles.	1	Host Server Administration Test Case
5.6.1.4	The voting system SHALL log logging failures, log clearing, and log rotation.	1	Host Server Administration Test Case
5.6.1.5	The voting system SHALL store log data in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format.	1	Host Server Administration Test Case
5.6.1.6	The voting system SHALL ensure that each jurisdiction's event logs and each component's logs are separable from each other.	N/A	
5.6.1.7	The voting system SHALL include an application or program to view, analyze, and search event logs.	1	Host Server Administration Test Case
5.6.1.8	All logs SHALL be preserved in a useable manner prior to voting system decommissioning.	1	Host Server Administration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.6.1.9	Logs SHALL NOT contain any data that could violate the privacy of the voter's identity.	4	Normal Ballot Delivery Test Case
		13	Registration Processing Test Case
5.6.1.10	Timekeeping mechanisms SHALL generate time and date values, including hours, minutes, and seconds.	4	Normal Ballot Delivery Test Case
		1	Host Server Administration Test Case
		13	Registration Processing Test Case
5.6.1.11	The precision of the timekeeping mechanism SHALL be able to distinguish and properly order all log events.	4	Normal Ballot Delivery Test Case
		13	Registration Processing Test Case
5.6.1.12	Only the system administrator SHALL be permitted to set the system clock.	N/A	
5.6.2	**Communication Logging**		
5.6.2.1	All communications actions SHALL be logged.	4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case
		13	Registration Processing Test Case
5.6.2.2	The communications log SHALL contain at least the following entries: Times when the communications are activated and deactivated; Services accessed; Identification of the device which data was transmitted to or received from; Identification of authorized entity; and Successful and unsuccessful attempts to access communications or services.	4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.6.3	**System Event Logging**		
	This section describes requirements for the voting system to perform event logging for system maintenance troubleshooting, recording the history of system activity, and detecting unauthorized or malicious activity. The operating system, and/or applications software may perform the actual event logging. There may be multiple logs in use for any system component.		
5.6.3.1	The voting system SHALL log the following data for each event: a. System ID; b. Unique event ID and/or type; c. Timestamp; d. Success or failure of event, if applicable; e. User ID triggering the event, if applicable; and f. Jurisdiction, if applicable.	1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
		7	Recovery form hardware error Test Case
		5	Discovery Penetration Test Case
5.6.3.2	All critical events SHALL be recorded in the system event log.	5	Discovery Penetration Test Case
		4	Normal Ballot Delivery Test Case
		7	Recovery form hardware error Test Case
		13	Registration Processing Test Case
5.6.3.3	At a minimum the voting system SHALL log the events described in the table below. NOTE: See "Table 5-2 System Events" in document - page 71	1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case
		7	Recovery form hardware error Test Case
5.7	**Incident Response**		
5.7.1	**Incident Response Support**		
5.7.1.1	Manufacturers SHALL document what types of system operations or security events (e.g., failure of critical component, detection of malicious code, unauthorized access to restricted data) are classified as critical.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.7.1.2	An alarm that notifies appropriate personnel SHALL be generated on the vote capture device, system server, or tabulation device, depending upon which device has the error, if a critical event is detected.	N/A	
5.8	**Physical and Environmental Security**		
5.8.1	**Physical Access**		
5.8.1.1	Any unauthorized physical access SHALL leave physical evidence that an unauthorized event has taken place.	N/A	
5.8.2.1	The voting system SHALL disable physical ports and access points that are not essential to voting operations, testing, and auditing.	11	Host Server Security Test Case
5.8.3.1	If a physical connection between the vote capture device and a component is broken, the affected vote capture device port SHALL be automatically disabled.	N/A	
5.8.3.2	The voting system SHALL produce a visual alarm if a connected component is physically disconnected.	N/A	
5.8.3.3	An event log entry that identifies the name of the affected device SHALL be generated if a vote capture device component is disconnected.	7	Recovery form hardware error Test Case
5.8.3.4	Disabled ports SHALL only be re-enabled by authorized administrators.	1	Host Server Administration Test Case
5.8.3.5	Vote capture devices SHALL be designed with the capability to restrict physical access to voting device ports that accommodate removable media with the exception of ports used to activate a voting session.	N/A	
5.8.3.6	Vote capture devices SHALL be designed to give a physical indication of tampering or unauthorized access to ports and all other access points, if used as described in the manufacturer's documentation.	N/A	
5.8.3.7	Vote capture devices SHALL be designed such that physical ports can be manually disabled by an authorized administrator.	N/A	
5.8.4	**Door Cover and Panel Security**		
5.8.4.1	Access points such as covers and panels SHALL be secured by locks or tamper evident or tamper resistant countermeasures and SHALL be implemented so that kiosk workers can monitor access to vote capture device components through these points.	N/A	
5.8.5	**Secure Paper Record Receptacle**		
	If the voting system provides paper record containers then they SHALL be designed such that any unauthorized physical access results in physical evidence that an unauthorized event has taken place.	N/A	
5.8.6	**Secure Physical Lock and Key**		
5.8.6.1	Voting equipment SHALL be designed with countermeasures that provide physical indication that unauthorized attempts have been made to access locks installed for security purposes.	N/A	
5.8.6.2	Manufacturers SHALL provide locking systems for securing vote capture devices that can make use of keys that are unique to each owner.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.8.7	**Media Protection**		
	These requirements apply to all media, both paper and digital, that contain personal privacy related data or other protected or sensitive types of information.		
5.8.7.1	The voting system SHALL meet the following requirements: a. All paper records (including rejected ones) printed at the kiosk locations SHALL be deposited in a secure container; b. Vote capture device hardware, software and sensitive information (e.g., electoral roll) SHALL be physically protected to prevent unauthorized modification or disclosure; and c. Vote capture device hardware components, peripherals and removable media SHALL be identified and registered by means of a unique serial number or other identifier.	N/A	
5.9	**Penetration Resistance**		
5.9.1	**Resistance to Penetration Attempts**		
5.9.1.1	The voting system SHALL be resistant to attempts to penetrate the system by any remote unauthorized entity.	5	Discovery Penetration Test Case
		11	Host Server Security Test Case
5.9.1.2	The voting system SHALL be configured to minimize ports, responses and information disclosure about the system while still providing appropriate functionality.	5	Discovery Penetration Test Case
		11	Host Server Security Test Case
5.9.1.3	The voting system SHALL provide no access, information or services to unauthorized entities.	5	Discovery Penetration Test Case
		1	Host Server Administration Test Case
5.9.1.4	All interfaces SHALL be penetration resistant including TCP/IP, wireless, and modems from any point in the system.	11	Host Server Security Test Case
5.9.1.5	The configuration and setup to attain penetration resistance SHALL be clearly and completely documented.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.9.2.1	The scope of penetration testing SHALL include all the voting system components. The scope of penetration testing includes but is not limited to the following: System server; Vote capture devices; Tabulation device; All items setup and configured per Technical Data Package (TDP) recommendations; Local wired and wireless networks; and03/09/2011 Internet connections.	5	Discovery Penetration Test Case
5.9.2.2	Penetration testing SHALL be conducted on a voting system set up in a controlled lab environment. Setup and configuration SHALL be conducted in accordance with the TDP, and SHALL replicate the real world environment in which the voting system will be used.	N/A	
5.9.2.3	The penetration testing team SHALL conduct white box testing using manufacturer supplied documentation and voting system architecture information. Documentation includes the TDP and user documentation. The testing team SHALL have access to any relevant information regarding the voting system configuration. This includes, but is not limited to, network layout and Internet Protocol addresses for system devices and components. The testing team SHALL be provided any source code included in the TDP.	N/A	
5.9.2.04	Penetration testing seeks out vulnerabilities in the voting system that might be used to change the outcome of an election, interfere with voter ability to cast ballots, ballot counting, or compromise ballot secrecy. The penetration testing team SHALL prioritize testing efforts based on the following: a. Threat scenarios for the voting system under investigation; b. Remote attacks SHALL be prioritized over in-person attacks; c. Attacks with a large impact SHALL be prioritized over attacks with a more narrow impact; and d. Attacks that can change the outcome of an election SHALL be prioritized over attacks that compromise ballot secrecy or cause non-selective denial of service.	5	Discovery Penetration Test Case

APPENDIX B
FUNCTIONAL TEST CASES
(Submitted under separate cover)

APPENDIX C
CRYPTOGRAPHIC TEST CASES
(Submitted under separate cover)

APPENDIX D
DISCOVERY PHASE PENTRATION
TEST CASES

(Submitted under separate cover)

wyle laboratories

Wyle Laboratories, Inc.
7800 Highway 20 West
Huntsville, Alabama 35806
Phone (256) 837-4411 • Fax (256) 721-0144
www.wyle.com

TEST REPORT

REPORT NO.: T58371.01-06

WYLE JOB NO.: T58371.01

CLIENT P.O. NO.: N/A

CONTRACT: N/A

TOTAL PAGES (INCLUDING COVER): 84

DATE: July 18, 2011

SECURITY TEST REVIEW OF THE UOCAVA OVERSEAS VOTING PILOT PROGRAM ELECTRONIC VOTING SUPPORT WIZARDS (EVSW)

for

Calibre
6354 Walker Lane
Alexandria, Virginia 22310-3252

STATE OF ALABAMA
COUNTY OF MADISON }

Robert D. Hardy, Department Manager, being duly sworn, deposes and says: The information contained in this report is the result of complete and carefully conducted testing and is to the best of his knowledge true and correct in all respects.

Robert Hardy

SUBSCRIBED and sworn to before me this 19 day of July 2011

Sandra A. Daniel

Notary Public in and for the State of Alabama at Large

My Commission expires June 2, 2015

Wyle shall have no liability for damages of any kind to person or property, including special or consequential damages, resulting from Wyle's providing the services covered by this report.

PREPARED BY: 7-18-11
Jack Cobb, Senior Project Engineer Date

APPROVED BY: 7-18-11
Frank Padilla, Voting Systems Manager Date

WYLE Q. A.: Rionda Moss 7/19/11
FOR Raul Terceno, Q. A. Manager Date

NVLAP®
NVLAP LAB CODE 200771-0

U.S. Election Assistance Commission
VSTL
EAC Lab Code 0704

TABLE OF CONTENTS

Page No.

ATTACHMENT

1.0 INTRODUCTION

1.1 Objective

This report documents the procedures followed and the results obtained during testing performed by Wyle on five independent (different Manufacturer's) Electronic Voting Support Wizard (EVSW) systems. The primary purpose of this testing was to demonstrate that the submitted systems conformed to Section 5 "Security" of the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements.

1.2 Scope

The scope of testing for this test campaign was limited to Section 5 "Security" of the UOCAVA Pilot Program Testing Requirements. These requirements were written for a remote electronic Kiosk. The EVSW systems submitted for the test campaign were each designed and deployed prior to the development of these standards. During this test campaign, all applicable requirements were attempted to be tested by Wyle for each EVSW system.

This test campaign included testing in the following areas:

<u>Functional Tests</u>

The functional test area focused on inspection, review and execution as the primary test methods. The functional tests were designed to cover the requirements in the following sections of the UOCAVA Pilot Program Testing Requirements:

5.1 Access Control

5.2 Identification and Authentication

5.4 Voting System Integrity Management

5.5 Communication Security

5.6 Logging

5.7 Incident Response

<u>Cryptographic Tests</u>

The cryptographic test area focused on inspection, review and execution as the primary test methods. The cryptographic tests were designed to cover the requirements in the following section:

5.3 Cryptography

<u>Penetration Tests</u>

The penetration test area was broken into two phases: discovery and exploratory. The penetration tests were designed to cover the requirements in the following sections:

5.8 Physical and Environmental Security

5.9 Penetration Resistance

1.0 INTRODUCTION (CONTINUED)

1.3 Customer

Calibre
6354 Walker Lane
Alexandria, Virginia 22310-3252

1.4 References

The documents listed were utilized to perform testing.

- Wyle Laboratories Quotation No. 545/052353-R1/DB, dated December 22, 2010
- National Voluntary Laboratory Accreditation Program NIST Handbook 150, 2006 Edition, "NVLAP Procedures and General Requirements (NIST Handbook 150)", dated February 2006
- National Voluntary Laboratory Accreditation Program NIST Handbook 150-22, 2008 Edition, "Voting System Testing (NIST Handbook 150-22)", dated May 2008
- Wyle Laboratories' Quality Assurance Program Manual, Revision 3
- ANSI/NCSL Z540-1, "Calibration Laboratories and Measuring and Test Equipment, General Requirements"
- ISO 10012-1, "Quality Assurance Requirements for Measuring Equipment"
- Election Assistance Commission, "Uniform and Overseas Citizens Absentee Voting Act Pilot Program Testing Requirements", August 25, 2010
- NIST 800-63 Electronic Authentication Guideline Standards
- NIST SP800-57 Computer Security
- FIPS 140-2 Security Requirements for Cryptographic Modules
- Manufacturer's submitted documentation – may have included any of the following types of documentation: overview, design or architecture, functional, user manual, hardware, setup, registration, or help.

1.5 Summary

The EVSW systems were subjected to the tests required per the scope of this test campaign. Testing was performed at Wyle Laboratories, Huntsville, Alabama Test Facility from March 2 through June 24, 2011. All hard copy data generated by the performance of these tests was retained by Wyle as raw data.

Details of the systems tested and the tests performed are provided in redacted format in the following sections.

2.0 TEST EQUIPMENT DESCRIPTION

2.1 System Overview

The systems submitted for this test campaign ranged from web based online ballot delivery systems to web based online internet voting systems. Each system was accessible from any internet capable computing device via a vendor chosen host web server.

A generic / redacted description of the EVSW systems submitted for testing follows.

System A: [redacted] The administration website allows for management and general administrative tasks. The voter website allows for identity verification, voting, and reviewing of ballots.

System B: [redacted] Voter data, candidates, contests, and election information is uploaded through an administrative website that provides:

- Tiered access based on user location, permission, and role;
- Interfaces to upload mass voter and election data;
- The capability to associate ballots with styles and precincts; and
- Usage metrics, ballot tracking and alerts.

Voters are able to access the uploaded information via a separate voter website.

System C: [redacted]. The back-end (administrative) website allows for request and elector management and general administrative tasks. The front-end (elector) website allows for registration and voting options.

System D: [redacted]. Voter data, candidates, contests, and election information is uploaded through an administrative website that provides:

- Tiered access based on user location, permission, and role;
- Interfaces to upload mass voter and election data;
- The capability to associate ballots with styles and precincts; and
- Usage metrics, ballot tracking and alerts.

Voters are able to access the uploaded information via a separate voter website.

System E: [redacted]. Voter data, candidates, contests, and election information is uploaded through an administrative website that provides:

- Tiered access based on user location, permission, and role;
- Interfaces to upload mass voter and election data;
- The capability to associate ballots with styles and precincts; and
- Usage metrics, ballot tracking and alerts.

Voters are able to access the uploaded information via a separate voter website.

2.0 TEST EQUIPMENT DESCRIPTION (CONTINUED)

2.2 Software

Each EVSW system was tested with software as submitted by the manufacturer.

2.3 Hardware

The manufacturer's applications were each web-based and therefore did not have locally available hardware.

2.4 Test Tools/Materials

This subsection enumerates any and all test materials needed to perform functional testing. The equipment was used to implement the test cases on each EVSW system evaluated.

Table 2-3 Test Materials

Test Material	Quantity
Dell OptiPlex 780	1
Windows 7	1
IE (Internet Explorer) 8	1

3.0 TEST PROCEDURES AND RESULTS

The methodology utilized to perform testing differed from that from a typical test campaign in three primary ways: control and possession of the system hardware, technical documentation and source code. During the course of a typical certification test campaign, manufacturers' provide the hardware and a Technical Data Package (TDP) for each system being tested. For this test campaign, Wyle was not provided a full TDP for the systems tested. The absence of technical documentation limited the requirements that could be evaluated due to a lack of information for defining test cases. Additionally, in typical certification efforts, a source code review will be performed on all proprietary software. Source code reviews were not required during this effort; therefore, the execution of the penetration testing was limited and "white-box" level testing could not be performed.

Each EVSW system was subjected to all tests as required for the scope of the test campaign. For testing purposes, test cases were developed using the manufacturer's documentation, architectural documents, and security specifications, as well as "Use Case" and verification methods. These test cases were then mapped to the applicable requirements of Section 5 "Security" of the UOCAVA Pilot Program Testing Requirements. This test campaign included the following core test cases: Functional, Penetration and Cryptography. The UOCAVA Functional Requirements Matrix, contained in Appendix A of this report, presents the requirements tested, test cases utilized to test each applicable requirement, and designates all non-applicable requirements (marked "N/A").

3.1 Functional Tests

Functional tests were performed by Wyle qualified personnel (henceforth referred to as Wyle) to validate compliance to the applicable UOCAVA requirements. The following test methods were used during functional tests: inspection, review, and execution. Wyle executed some combination of the following set of test cases that were specifically designed for each EVSW system.

3.0 TEST PROCEDURES AND RESULTS (CONTINUED)

3.1 Functional Tests (continued)

Below is a brief description of each of the test cases utilized:

- TC01HostAdmin (Host Server Administration) – A test to verify the roles of the system administrator and the ability to maintain user roles, passwords, logs and other voting system administrative functions.

- TC04BallotDelivery (Normal Ballot Delivery) – A test to verify accurately ballot delivery, implementation of authentication prior to allowing voter access to the ballot, and logging of events.

- TC10BallotDelivery (Local Ballot Delivery) – A test to verify accurate ballot delivery, implementation of authentication prior to allowing voter access to the ballot, and logging of events.

- TC12VoterRegReq (Voter Registration Request) – A test to verify a voter can securely register to vote on-line. The test includes authentication of voter credentials.

- TC13RegProcess (Registration Processing) – A test to verify the ability of an election administrator to view voter requests and accept or reject the request based on successful comparison of the voter's credentials.

- TC14NormalVoting (Normal Voting) – A test to verify accurate ballot delivery, implementation of authentication prior to allowing voter access to the ballot, and logging of events.

The functional test cases executed for each system under test are listed in the table below.

Table 3-1 Functional Test Cases

System	Test Cases
A	TC01HostAdmin (Host Server Administration) TC10BallotDelivery (Local Ballot Delivery)
B	TC01HostAdmin (Host Server Administration) TC04BallotDelivery (Normal Ballot Delivery)
C	TC01HostAdmin (Host Server Administration) TC12VoterRegReq (Voter Registration Request) TC13RegProcess (Registration Processing) TC14NormalVoting (Normal Voting)
D	TC01HostAdmin (Host Server Administration) TC04BallotDelivery (Normal Ballot Delivery)
E	TC01HostAdmin (Host Server Administration) TC12VoterRegReq (Voter Registration Request) TC13RegProcess (Registration Processing) TC04BallotDelivery (Normal Ballot Delivery)

3.0 TEST PROCEDURES AND RESULTS (CONTINUED)

3.1 Functional Tests (continued)

The findings from the performance of each test case are detailed in the following paragraphs.

Summary Findings

For Systems A, B, D, and E, the following paragraph applies:

TC01HostAdmin

During the Host Admin test case Wyle logged in with the administrative account provided by the vendor. An attempt was made to dump logs and manipulate any stored data. Data from the logs was analyzed to determine compliance with the UOCAVA requirements. Wyle then attempted to modify the user data and login credentials. Validation was performed to validate that all requirements for voter security were met per the UOCAVA requirements. Wyle then attempted to create administration accounts and validate security of administration accounts. Admin accounts were used to validate roles and responsibilities of each administrator. Attempts were made to access administration functionality without use of the administration login.

System A specifics for TC01HostAdmin:

During the performance of the test case, the following issues were noted:

- Admin page functionality was very limited.
- Admin account management is system based
- There is nothing implemented to limit incorrect login attempts.
- System does not have a lock out function.
- System does not have a time out control.
- Passwords would need to be reset by a system administrator.
- Log files must be generated by the admin on local system. They will then be in the format selected by the admin.
- Many requirements could not be tested do to the architecture requiring physical access to the server.

System B specifics for TC01HostAdmin:

During the performance of the test case, it was noted that the following core functions were untestable:

- User functionality was very limited.
- Logs were not tested. Only a voter’s log was available.
- No reporting was available.
- Admin account management was not functional.

3.0 TEST PROCEDURES AND RESULTS (CONTINUED)

3.1 Functional Tests (continued)

System D specifics for TC01HostAdmin:

During the performance of the test case, the following issues were noted:

- There is only one login for each election.
- Incorrect login attempts are not limited.
- The administrator of the election can send a new password for that user. At which point, the author can then customize his/her own password if they so choose. For the <redacted>, the password is set by the system administrator and the user cannot reset it.
- An administrator does not configure the password strength configuration.
- There is nothing in place to limit the use of historically used passwords.
- There is not a restriction on user password matching the user name.
- There is not a password expiration option.
- The log remains continuous and cannot be cleared.

System E specifics for TC01HostAdmin:

During the performance of the test case, the following issues were noted:

- Nothing is implemented to limit incorrect login attempts.
- System does not have a lock out function.
- Administrator cannot set the password strength configuration
- There is not anything in place to limit the use of historically used passwords.
- There is not a restriction on user password matching the user name.
- Passwords do not expire.
- Logs are retained and do not get cleared.
- Member login log is not exportable

For System C, the following paragraph applies for TC01HostAdmin:

During performance of testing, Wyle was able to verify the system contained segregation of duties and those duties were maintainable. The system does require passwords and provides an event log, but not all requirements were met for these functions.

3.0 TEST PROCEDURES AND RESULTS (CONTINUED)

3.1 Functional Tests (continued)

System C specifics for TC01HostAdmin:

During the performance of the test case, the following issues were noted:

- Upon creation of a new user and default role is the administrator role.
- No ability for the user to reset their password. This function is handled by requesting a password change.
- No limit on incorrect login attempts.
- No password expiration.
- The current system logging is not as detailed per the requirements.

TC01HostAdmin – Synopsis of Summary Findings – All Tested Systems:

Per the UOCAVA requirements tested by test case TC01HostAdmin, Wyle deduced from the above summary findings that the primary areas of deficiency of the systems tested can be categorized into one of the following areas.

- Login functions.
- Password functions.
- Log generation functions.

TC04BallotDelivery

For Systems A, B, D, and E, the following paragraph applies:

During the Ballot Delivery test case Wyle logged in with the voter accounts provided by the vendor. Attempts were made to access multiple ballots using a single voter. Analysis was done to determine the level of security of data as a result of the ballot delivery process. Wyle attempted to gain access to a ballot by an unauthorized voter. Wyle attempted to gain access to administration information utilizing voter credentials.

System A specifics for TC04BallotDelivery:

During the performance of the test case, it the following issues were noted:

- There is nothing implemented to limit incorrect login attempts.
- System does not have a lock out function.
- System does not have a time out control.
- Passwords would need to be reset by a system administrator.

3.0 TEST PROCEDURES AND RESULTS (CONTINUED)

3.1 Functional Tests (continued)

System B specifics for TC04BallotDelivery:

During the performance of the test case, it was noted that the following core functions were untestable:

- Blank Ballot delivery

System D specifics for TC04BallotDelivery:

During the performance of the test case, the following issues were noted:

- There is not a restriction on user password matching the user name.
- There is not a password expiration option.
- It was noted that the pages are being cached and would give a hacker the ability to return to pages that should be secure.

System E specifics for TC04BallotDelivery:

- No issues noted.

TC04HostAdmin – Synopsis of Summary Findings – All Tested Systems:

Per the UOCAVA requirements tested by test case TC04HostAdmin, Wyle deduced from the above summary findings that the primary areas of deficiency of the systems tested can be categorized into one of the following areas.

- Login functions.
- Password functions.

TC12 Registration Request Test Case

System C specifics for TC12 Registration Request Test Case:

During performance of testing, Wyle was able to verify a voter could successfully and securely submit information and request an online registration. The test also verified authentication of a registered voter with credential from the system. There were no discrepancies to report.

System E specifics for TC12 Registration Request Test Case:

During performance of the test case, Wyle logged in with the voter credentials provided by the vendor. Analysis was done to determine the level of security of data as a result of the registration request process. Wyle attempted to gain access to a ballot by registering unauthorized voter. Wyle attempted to gain access to administration information utilizing voter credentials.

3.0 TEST PROCEDURES AND RESULTS (CONTINUED)

3.1 Functional Tests (continued)

During the performance of the test case, the following issues were noted:

- It was noticed that after the registration is completed, a user can use the back button and still see the registration information.

TC12 Registration Request Test Case – Synopsis of Summary Findings – Tested Systems:

For the two systems supporting these areas of the UOCAVA requirements, the one area of deficiency has to do with limiting web page caching and session storage of user input information that might be miss-used to compromise privacy or security.

TC13 Registration Processing Test Case

System C specifics for TC13 Registration Processing Test Case:

During performance of testing, Wyle was able to verify a user logged in with administrative duties could approve and reject requests submitted by on online voter. Wyle was also able to authenticate voter credential against an approved UOCAVA registered voter list.

- There were no discrepancies to report.

System E specifics for TC13 Registration Processing Test Case:

During performance of the test case, Wyle logged in with the administrative accounts provided by the vendor. Analysis was done to determine the level of security of data as a result of the registration request process. Validation was made that admins do validation of voter credentials.

- There were no discrepancies to report.

TC13HostAdmin – Synopsis of Summary Findings – Tested Systems:

For the two systems supporting these areas of the UOCAVA requirements, there were no discrepancies to report.

TC14 Normal Voting

During performance of testing, Wyle was able to submit an accurate online ballot. Wyle also verified that a voter must be a registered and approved to gain access to a ballot. Voters are also only able to vote one time. The system does log some events for the voting process, but the log function does not meet all requirements.

A summary of discrepancies are listed below:

- No ability for the user to reset their password. This function is handled by requesting a password change.
- No limit on incorrect login attempts.

3.0 TEST PROCEDURES AND RESULTS (CONTINUED)

3.1 Functional Tests (continued)

- No password expiration.
- The current system logging is not as detailed per the requirements.

TC14 Normal Voting – Synopsis of Summary Findings – Tested Systems:

Per the UOCAVA requirements tested by test case TC14 Normal Voting, Wyle deduced from the above summary findings that the primary areas of deficiency of the system tested can be categorized into one of the following areas.

- Login functions.
- Password functions.
- Log generation functions.

3.2 Cryptographic Tests

Cryptographic Tests were performed to validate compliance to the applicable UOCAVA requirements.

Three test methods were used during performance of the cryptographic tests: inspection, review, and execution. Wyle executed some combination of the following set of test cases that were specifically designed for each EVSW system. Below is a brief description of each of the test cases utilized:

- TC03CryptoTestSheet (Manufacturer) – A test to verify the functionality, strength and NIST compliance of the system, no matter which one of the three purposes it serves in the voting system (Confidentiality, Authentication or Random Number Generation (RNG)).

Summary Findings

The following summary applied to all systems tested in this campaign:

During performance of testing, Wyle was able to verify portions of the cryptographic requirements. Key management and key establishment could not be tested due to lack of documentation in this area as well as physical access to the system necessary to complete these two areas of cryptographic testing. Wyle only had access to the client side functionality; therefore, no administrator credentialed cryptographic testing could be performed. The test cases and results obtained are presented in Appendix B of this document.

3.0 TEST PROCEDURES AND RESULTS (CONTINUED)

3.3 Penetration Tests

Penetration tests were performed to determine the security of each EVSW system and to validate compliance to the applicable UOCAVA requirements.

The penetration test area was broken into two phases: discovery and exploratory. The discovery phase consisted of performing scans while the system was running with leveraged and unleveraged credentials. These scans provided information about the ports, protocols, and hardware configurations as well as simulated certain portions of an attack on vulnerable areas of the system. The information gathered was provided to a certified security professional, who analyzed the results and determined the best method and types of attacks to be performed during the exploratory phase of testing. Specific test cases were then designed and executed during the exploratory phase of the penetration tests. These test cases were based on all information gathered during discovery, any subsequent observations made during the exploratory phase and any Rules Of Engagement (ROE) previously agreed upon by Wyle and the manufacturer.

Below is a brief description of each of the test cases utilized:

- TC05DiscoveryPenetration (Manufacturer) – A test to seek out vulnerabilities in the voting system and to verify the system's resistance to any remote unauthorized entity.

Summary Findings

NOTE: Information redacted. In general, all vulnerabilities discovered and their level (high, medium, low) were reported to each manufacturer. However, any discovered vulnerabilities could not be exploited in the time constraint set for the exploratory phase of the penetration test. Details of this test case can be found in Appendix B of this document. NOTE: Appendix B information redacted in this report.

TC05DiscoveryPenetration

During performance of testing, Wyle sought to discover vulnerabilities that fall into risk levels of "High", "Medium", or "Low".

System A specifics for **TC05DiscoveryPenetration**:

A summary of risk levels are listed below:

- Low risk area – 11 found.

System B specifics for **TC05DiscoveryPenetration**:

A summary of risk levels are listed below:

- SQL attempts exposed some information that could be useful to an attacker.

3.0 TEST PROCEDURES AND RESULTS (CONTINUED)

3.3 Penetration Tests

System C specifics for **TC05DiscoveryPenetration**:

A summary of risk levels are listed below:

- Low risk area – 22 found.

System D specifics for **TC05DiscoveryPenetration**:

A summary of risk levels are listed below:

- Low risk area – 42 found.
- Medium risk area – 8 found.

System E specifics for **TC05DiscoveryPenetration**:

- No risk areas were located in the time constraint set for penetration testing.

TC05DiscoveryPenetration – Synopsis of Summary Findings – Tested Systems:

Penetration testing discovered primarily “low” risk areas of vulnerability in the systems tested in this test campaign. Regardless of the risk level/areas located, none of these could be exploited in the time constraint set for the exploratory phase of the penetration testing.

3.4 Test Summary

For the specific test cases executed, and the results for each system, refer to Attachment B “Test Cases”. Overall assessment of the test results for each system tested and the specific requirement by system “Pass/Fail” are presented in Attachment C “Statistical Analysis of the UOCAVA EVSW’s”. As for the ability of the EVSW’s tested to meet the requirements, the results observed during testing is provided below:

Table 3-1 Test Result Summary

Average Summary	Pass	Fail	Not Tested	N/A
	24%	22%	24%	30%

ATTACHMENT A

REQUIREMENT MATRIX

Overall, during the execution of this test campaign, Wyle did not encounter any major problems working with the requirements. However, Wyle feels that some of the requirements can be clearer and better defined to make them more testable. The following table contains comments and recommendations per requirement. As for the Non-Applicable requirements, Wyle did not attempt to test them; therefore, recommendations are not provided. Additionally, the Not Tested requirements were attempted to be applied but could not be tested under this test campaign due to the current configuration of the systems tested. The major areas that Wyle is unable to comment on are the Communication Security, Penetration Resistance, and Cryptography sections.

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix	Test Case Description	Wyle Comment
Section 5	**Security**		
5.1	**Access Control**		
	This section states requirements for the identification of authorized system users, processes and devices and the authentication or verification of those identities as a prerequisite to granting access to system processes and data. It also includes requirements to limit and control access to critical system components to protect system and data integrity, availability, confidentiality, and accountability. This section applies to all entities attempting to physically enter voting system facilities or to request services or data from the voting system.		
5.1.1	**Separation of Duties**		
5.1.1.1	The voting system SHALL allow the definition of personnel roles with segregated duties and responsibilities on critical processes to prevent a single person from compromising the integrity of the system.	Administration Test Case	Specific roles should be defined to facilitate true segregation of duties.
5.1.1.2	The voting system SHALL ensure that only authorized roles, groups, or individuals have access to election data.	Administration Test Case	
5.1.1.3	The voting system SHALL require at least two persons from a predefined group for validating the election configuration information, accessing the cast vote records, and starting the tabulation process.	N/A	Current web based system do not do tabulation so this requirement was not applicable to our testing. The majority of election configuration is done independent of the Web application and is therefore not a critical function of our testing.
5.1.2	**Voting System Access**		
	The voting system SHALL provide access control mechanisms designed to permit authorized access and to prevent unauthorized access to the system.	Penetration Test Case Administration Test Case	This requirement does not define at what minimum level this security should be implemented.
5.1.2.1	The voting system SHALL identify and authenticate each person, to whom access is granted, and the specific functions and data to which each person holds authorized access.	Administration Test Case Ballot Delivery Test Case	This requirement does not define at what minimum level this security should be implemented.
5.1.2.2	The voting system SHALL allow the administrator group or role to configure permissions and functionality for each identity, group or role to include account and group/role creation, modification, and deletion.	Administration Test Case	This requirement does not state whether this should be a system OS level or at a web based administration application level.
5.1.2.3	The voting system's default access control permissions SHALL implement the least privileged role or group needed.	Administration Test Case	

UOCAVA Req. No.	**Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix**	**Test Case Description**	**Wyle Comment**
5.1.2.4	The voting system SHALL prevent a lower-privilege process from modifying a higher-privilege process.	Administration Test Case	
5.1.2.5	The voting system SHALL NOT require its execution as an operating system privileged account and SHALL NOT require the use of an operating system privileged account for its operation.	N/A	Wyle's testing was based on utilization of a web based application. Therefore this did not apply directly. But, it was noted that in some systems tested the OS administration privileges were required to configure election information.
5.1.2.6	The voting system SHALL log the identification of all personnel accessing or attempting to access the voting system to the system event log.	Administration Test Case Ballot Delivery Test Case Penetration Test Case	This requirement does not define what information should be logged. Some systems only log Administration functions while others only log Voter information.
5.1.2.7	The *(voting system)* SHALL provide tools for monitoring access to the system. These tools SHALL provide specific users real time display of persons accessing the system as well as reports from logs.	Administration Test Case	This requirement does not define what information should be logged. This requirement also does not state if the tool is to be accessible via the Web based administration application or at an OS Level.
5.1.2.8	Vote capture device located at the remote voting location and the central server SHALL have the capability to restrict access to the voting system after a preset number of login failures. a. The lockout threshold SHALL be configurable by appropriate administrators/operators b. The voting system SHALL log the event c. The voting system SHALL immediately send a notification to appropriate administrators/operators of the event. d. The voting system SHALL provide a mechanism for the appropriate administrators/operators to reactivate the account after appropriate confirmation.	Administration Test Case Penetration Test Case	This requirement does not define if this needs to be at a Web application level or at OS level. Reactivation of an account should not require utilization of anything but the Web based application.
5.1.2.9	The voting system SHALL log a notification when any account has been locked out.	Administration Test Case Penetration Test Case	This requirement does not define what information should be logged.

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix	Test Case Description	Wyle Comment
5.1.2.10	Authenticated sessions on critical processes SHALL have an inactivity time-out control that will require personnel re-authentication when reached. This time-out SHALL be implemented for administration and monitor consoles on all voting system devices.	Administration Test Case Penetration Test Case	This requirement does not define how this function should be configured.
5.1.2.11	Authenticated sessions on critical processes SHALL have a screen-lock functionality that can be manually invoked.	N/A	This requirement was deemed N/A due to the web based application being accessible from a privately controlled PC and not a public Voting site.
5.2	**Identification and Authentication**		
	Authentication mechanisms and their associated strength may vary from one voting system capability and architecture to another but all must meet the minimum requirement to maintain integrity and trust. It is important to consider a range of roles individuals may assume when operating different components in the voting system and each may require different authentication mechanisms. The requirements described in this section vary from role to role. For instance, a kiosk worker will have different identification and authentication characteristics than a voter. Also, for selected critical functions there may be cases where split knowledge or dual authorization is necessary to ensure security. This is especially relevant for critical cryptographic key management functions.		
5.2.1	**Authentication**		
5.2.1.1	Authentication mechanisms supported by the voting system SHALL support authentication strength of at least 1/1,000,000.	Administration Test Case	
5.2.1.2	The voting system SHALL authenticate users per the minimum authentication methods outlined below. Refer to document for the table layout: http://www.eac.gov/assets/1/AssetManager/UOCAVA_Pilot_Program_Requirments-03.24.10.pdf Table 5-1 Roles : Section 5 | Page 59	Administration Test Case	Since these systems do not tabulate and are not located in a polling location, the groups for Election Judge and Kiosk Worker do not really apply. (See Table 5-1 Roles : Section 5 | Page 59.)
5.2.1.3	The voting system SHALL provide multiple authentication methods to support multi-factor authentication.	Administration Test Case	This requirement does not define what minimum level is required.

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix	Test Case Description	Wyle Comment
5.2.1.4	When private or secret authentication data is stored by the voting system, it SHALL be protected to ensure that the confidentiality and integrity of the data are not violated.	Administration Test Case	
5.2.1.5	The voting system SHALL provide a mechanism to reset a password if it is forgotten, in accordance with the system access/security policy.	Administration Test Case	This requirement does not define if this function is to be Web Based.
5.2.1.6	The voting system SHALL allow the administrator group or role to specify password strength for all accounts including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters per NIST 800-63 Electronic Authentication Guideline Standards.	Administration Test Case	This requirement does not define if this configuration is to be Web Based or OS configurable.
5.2.1.7	The voting system SHALL enforce password histories and allow the administrator to configure the history length when passwords are stored by the system.	Administration Test Case	This requirement does not define if this configuration is to be Web Based or OS configurable.
5.2.1.8	The voting system SHALL ensure that the user name is not used in the password.	Administration Test Case	
5.2.1.9	The voting system SHALL provide a means to automatically expire passwords.	Administration Test Case	
5.2.1.10	The voting system servers and vote capture devices SHALL identify and authenticate one another using NIST - approved cryptographic authentication methods at the 112 bits of security.	Cryptography Test Case	This requirement does not define which NIST standard or level to use.
5.2.1.11	Remote voting location site Virtual Private Network (VPN) connections (i.e., vote capture devices) to voting servers SHALL be authenticated using strong mutual cryptographic authentication at the 112 bits of security.	N/A	Wyle deems this requirement N/A due to the Web Based architecture. VPN systems will only be utilized at a system server level.
5.2.1.12	Message authentication SHALL be used for applications to protect the integrity of the message content using a schema with 112 bits of security.	Cryptography Test Case	
5.2.1.13	IPsec, SSL, or TLS and MAC mechanisms SHALL all be configured to be compliant with FIPS 140-2 using approved algorithm suites and protocols.	Cryptography Test Case	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix	Test Case Description	Wyle Comment
5.3	**Cryptography**		
	Cryptography serves several purposes in voting systems. They include: Confidentiality: where necessary the confidentiality of voting records can be provided by encryption; Authentication: data and programs can be authenticated by a digital signature or message authentication codes (MAC), or by comparison of the cryptographic hashes of programs or data with the reliably known hash values of the program or data. If the program or data are altered, then that alteration is detected when the signature or MAC is verified, or the hash on the data or program is compared to the known hash value. Typically the programs loaded on voting systems and the ballot definitions used by voting systems are verified by the systems, while systems apply digital signatures to authenticate the critical audit data that they output. For remote connections cryptographic user authentication mechanism SHALL be based on strong authentication methods; and Random number generation: random numbers are used for several purposes including the creation of cryptographic keys for cryptographic algorithms and methods to provide the services listed above, and as identifiers for voting records that can be used to identify or correlate the records without providing any information that could identify the voter.		
5.3.1	**General Cryptography Requirements**		
5.3.1.1	All cryptographic functionality SHALL be implemented using NIST-approved cryptographic algorithms/schemas, or use published and credible cryptographic algorithms/schemas/protocols.	Cryptography Test Case	This requirement does not define what minimum NIST level is required.
5.3.1.2	Cryptographic algorithms and schemas SHALL be implemented with a security strength equivalent to at least 112 bits of security to protect sensitive voting information and election records.	Cryptography Test Case	
5.3.1.3	Cryptography used to protect information in-transit over public telecommunication networks SHALL use NIST-approved algorithms and cipher suites. In addition the implementations of these algorithms SHALL be NIST-approved (Cryptographic Algorithm Validation Program).	Cryptography Test Case	This requirement does not define which NIST standard or level to use.

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix	Test Case Description	Wyle Comment
5.3.2	**Key Management**		
	The following requirements apply to voting systems that generate cryptographic keys internally.		
5.3.2.1	Cryptographic keys generated by the voting system SHALL use a NIST-approved key generation method, or a published and credible key generation method.	Cryptography Test Case	This requirement does not define which NIST standard or level to use.
5.3.2.2	Compromising the security of the key generation method (e.g., guessing the seed value to initialize the deterministic random number generator (RNG)) SHALL require as least as many operations as determining the value of the generated key.	Cryptography Test Case	
5.3.2.3	If a seed key is entered during the key generation process, entry of the key SHALL meet the key entry requirements in 5.3.3.1. If intermediate key generation values are output from the cryptographic module, the values SHALL be output either in encrypted form or under split knowledge procedures.	Cryptography Test Case	
5.3.2.4	Cryptographic keys used to protect information in-transit over public telecommunication networks SHALL use NIST-approved key generation methods. If the approved key generation method requires input from a random number generator, then an approved (FIPS 140-2) random number generator SHALL be used.	Cryptography Test Case	This requirement does not define which NIST standard or level to use.
5.3.2.5	Random number generators used to generate cryptographic keys SHALL implement one or more health tests that provide assurance that the random number generator continues to operate as intended (e.g., the entropy source is not stuck).	Cryptography Test Case	
5.3.3	**Key Establishment**		
	Key establishment may be performed by automated methods (e.g., use of a public key algorithm), manual methods (use of a manually transported key loading device), or a combination of automated and manual methods.		
5.3.3.1	Secret and private keys established using automated methods SHALL be entered into and output from a voting system in encrypted form. Secret and private keys established using manual methods may be entered into or output from a system in plaintext form.	Cryptography Test Case	
5.3.4.1	Cryptographic keys stored within the voting system SHALL NOT be stored in plaintext. Keys stored outside the voting system SHALL be protected from disclosure or modification.	Cryptography Test Case	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix	Test Case Description	Wyle Comment
5.3.4.2	The voting system SHALL provide methods to zeroize all plaintext secret and private cryptographic keys within the system.	Cryptography Test Case	
5.3.4.3	The voting system SHALL support the capability to reset cryptographic keys to new values.	Cryptography Test Case	
5.4	**Voting System Integrity Management**		
	This section addresses the secure deployment and operation of the voting system, including the protection of removable media and protection against malicious software.		
5.4.1	**Protecting the Integrity of the Voting System**		
5.4.1.1	The integrity and authenticity of each individual cast vote SHALL be protected from any tampering or modification during transmission.	Ballot Delivery Test Case	
5.4.1.2	The integrity and authenticity of each individual cast vote SHALL be preserved by means of a digital signature during storage.	Ballot Delivery Test Case	
5.4.1.3	Cast vote data SHALL NOT be permanently stored on the vote capture device.	Ballot Delivery Test Case	
5.4.1.4	The integrity and authenticity of the electronic ballot box SHALL be protected by means of a digital signature.	Ballot Delivery Test Case	
5.4.1.5	The voting system SHALL use malware detection software to protect against known malware that targets the operating system, services, and applications.	Penetration Test Case	
5.4.1.6	The voting system SHALL provide a mechanism for updating malware detection signatures.	Penetration Test Case	
5.4.1.7	The voting system SHALL provide the capability for kiosk workers to validate the software used on the vote capture devices as part of the daily initiation of kiosk operations.	N/A	Wyle deems this requirement N/A due to the Web Based architecture.
5.5	**Communications Security**		
	This section provides requirements for communications security. These requirements address ensuring the integrity of transmitted information and protecting the voting system from external communications-based threats.		
5.5.1	**Data Transmission Security**		
5.5.1.1	Voting systems that transmit data over communications links SHALL provide integrity protection for data in transit through the generation of integrity data (digital signatures and/or message authentication codes) for outbound traffic and verification of the integrity data for inbound traffic.	Host Server Security Test Case	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix	Test Case Description	Wyle Comment
5.5.1.2	Voting systems SHALL use at a minimum TLS 1.0, SSL 3.1 or equivalent protocols, including all updates to both protocols and implementations as of the date of the submission (e.g., RFC 5746 for TLS 1.0).	Host Server Security Test Case	
5.5.1.3	Voting systems deploying VPNs SHALL configure them to only allow FIPS-compliant cryptographic algorithms and cipher suites.	N/A	Wyle deems this requirement N/A due to the Web Based architecture. VPN systems will only be utilized at a system server level.
5.5.1.4	Each communicating device SHALL have a unique system identifier.	Host Server Security Test Case	
5.5.1.5	Each device SHALL mutually strongly authenticate using the system identifier before additional network data packets are processed.	Host Server Security Test Case	
5.5.1.6	Data transmission SHALL preserve the secrecy of voters' ballot selections and SHALL prevent the violation of ballot secrecy and integrity.	Penetration Test Case	
5.5.2	**External Threats**		
	Voting systems SHALL implement protections against external threats to which the system may be susceptible.	Penetration Test Case	
5.5.2.1	Voting system components SHALL have the ability to enable or disable physical network interfaces.	Administration Test Case	
5.5.2.2	The number of active ports and associated network services and protocols SHALL be restricted to the minimum required for the voting system to function.	Penetration Test Case	
5.5.2.3	The voting system SHALL block all network connections that are not over a mutually authenticated channel.	Penetration Test Case	
5.6	**Logging**		
5.6.1	**Log Management**		
5.6.1.1	The voting system SHALL implement default settings for secure log management activities, including log generation, transmission, storage, analysis, and disposal.	Administration Test Case	
5.6.1.2	Logs SHALL only be accessible to authorized roles.	Administration Test Case	
5.6.1.3	The voting system SHALL restrict log access to append-only for privileged logging processes and read-only for authorized roles.	Administration Test Case	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix	Test Case Description	Wyle Comment
5.6.1.4	The voting system SHALL log logging failures, log clearing, and log rotation.	Administration Test Case	This requirement does not specify if these logs should contain both voter and administration information.
5.6.1.5	The voting system SHALL store log data in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format.	Administration Test Case	This requirement does not determine if these functions should be part of an administration web based application or at an OS level administration function.
5.6.1.6	The voting system SHALL ensure that each jurisdiction's event logs and each component's logs are separable from each other.	Administration Test Case	
5.6.1.7	The voting system SHALL include an application or program to view, analyze, and search event logs.	Administration Test Case	This requirement does not determine if these functions should be part of an administration web based application or at an OS level administration function.
5.6.1.8	All logs SHALL be preserved in a useable manner prior to voting system decommissioning.	Administration Test Case	
5.6.1.9	Logs SHALL NOT contain any data that could violate the privacy of the voter's identity.	Ballot Delivery Test Case	This requirement does not outline what information is deemed to violate a voter's identity. These systems utilize several voter specific credentials that are required for proper identification of voters.
		Registration Processing Test Case	
5.6.1.10	Timekeeping mechanisms SHALL generate time and date values, including hours, minutes, and seconds.	Ballot Delivery Test Case	
		Administration Test Case	
		Registration Processing Test Case	
5.6.1.11	The precision of the timekeeping mechanism SHALL be able to distinguish and properly order all log events.	Ballot Delivery Test Case	This requirement must meet 5.6.1.10
		Registration Processing Test Case	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix	Test Case Description	Wyle Comment
5.6.1.12	Only the system administrator SHALL be permitted to set the system clock.	N/A	Wyle determined that this requirement is N/A due to this function being a system administration function.
5.6.2	**Communication Logging**		
5.6.2.1	All communications actions SHALL be logged.	Penetration Test Case	This requirement does not define what all communications encompasses.
5.6.2.2	The communications log SHALL contain at least the following entries: Times when the communications are activated and deactivated; Services accessed; Identification of the device which data was transmitted to or received from; Identification of authorized entity; and Successful and unsuccessful attempts to access communications or services.	Ballot Delivery Test Case Penetration Test Case	
5.6.3	**System Event Logging**		
	This section describes requirements for the voting system to perform event logging for system maintenance troubleshooting, recording the history of system activity, and detecting unauthorized or malicious activity. The operating system, and/or applications software may perform the actual event logging. There may be multiple logs in use for any system component.		
5.6.3.1	The voting system SHALL log the following data for each event: a. System ID; b. Unique event ID and/or type; c. Timestamp; d. Success or failure of event, if applicable; e. User ID triggering the event, if applicable; and f. Jurisdiction, if applicable.	Administration Test Case Ballot Delivery Test Case Recovery form hardware error Test Case Penetration Test Case	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix	Test Case Description	Wyle Comment
5.6.3.2	All critical events SHALL be recorded in the system event log.	Penetration Test Case Ballot Delivery Test Case Recovery form hardware error Test Case Registration Processing Test Case	This requirement does not define what a critical event might be.
5.6.3.3	At a minimum the voting system SHALL log the events described in the table below. NOTE: See "Table 5-2 System Events" in document - page 71	Administration Test Case Ballot Delivery Test Case Penetration Test Case Recovery form hardware error Test Case	Wyle was unable to completely validate this requirement due to limited access to physical hardware. The majority of the events defined are from a server OS level and not a web based application level.
5.7	**Incident Response**		
5.7.1	**Incident Response Support**		
5.7.1.1	Manufacturers SHALL document what types of system operations or security events (e.g., failure of critical component, detection of malicious code, unauthorized access to restricted data) are classified as critical.	N/A	Wyle determined that this requirement is not applicable to a web based application. But it is a requirement for a web server and therefore could not be tested at this time.
5.7.1.2	An alarm that notifies appropriate personnel SHALL be generated on the vote capture device, system server, or tabulation device, depending upon which device has the error, if a critical event is detected.	N/A	Wyle determined that this requirement is not applicable to a web based application. A system server notification should be sent to administrators when issues arise with the web server.
5.8	**Physical and Environmental Security**		
5.8.1	**Physical Access**		

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix	Test Case Description	Wyle Comment
5.8.1.1	Any unauthorized physical access SHALL leave physical evidence that an unauthorized event has taken place.	N/A	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.
5.8.2.1	The voting system SHALL disable physical ports and access points that are not essential to voting operations, testing, and auditing.	Host Server Security Test Case	
5.8.3.1	If a physical connection between the vote capture device and a component is broken, the affected vote capture device port SHALL be automatically disabled.	N/A	Wyle determined that this requirement is not applicable to a web based application. A physical connection will only be made during a single instance of vote casting.
5.8.3.2	The voting system SHALL produce a visual alarm if a connected component is physically disconnected.	N/A	Wyle determined that this requirement is not applicable to a web based application.
5.8.3.3	An event log entry that identifies the name of the affected device SHALL be generated if a vote capture device component is disconnected.	N/A	Wyle determined that this requirement is not applicable to a web based application.
5.8.3.4	Disabled ports SHALL only be re-enabled by authorized administrators.	Administration Test Case	
5.8.3.5	Vote capture devices SHALL be designed with the capability to restrict physical access to voting device ports that accommodate removable media with the exception of ports used to activate a voting session.	N/A	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.
5.8.3.6	Vote capture devices SHALL be designed to give a physical indication of tampering or unauthorized access to ports and all other access points, if used as described in the manufacturer's documentation.	N/A	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.
5.8.3.7	Vote capture devices SHALL be designed such that physical ports can be manually disabled by an authorized administrator.	N/A	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.
5.8.4	**Door Cover and Panel Security**		
5.8.4.1	Access points such as covers and panels SHALL be secured by locks or tamper evident or tamper resistant countermeasures and SHALL be implemented so that kiosk workers can monitor access to vote capture device components through these points.	N/A	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.

UOCAVA Req. No.	**Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix**	**Test Case Description**	**Wyle Comment**
5.8.5	**Secure Paper Record Receptacle**		
	If the voting system provides paper record containers then they SHALL be designed such that any unauthorized physical access results in physical evidence that an unauthorized event has taken place.	N/A	Wyle determined that this requirement is not applicable to a web based application
5.8.6	**Secure Physical Lock and Key**		
5.8.6.1	Voting equipment SHALL be designed with countermeasures that provide physical indication that unauthorized attempts have been made to access locks installed for security purposes.	N/A	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.
5.8.6.2	Manufacturers SHALL provide locking systems for securing vote capture devices that can make use of keys that are unique to each owner.	N/A	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.
5.8.7	**Media Protection**		
	These requirements apply to all media, both paper and digital, that contain personal privacy related data or other protected or sensitive types of information.		
5.8.7.1	The voting system SHALL meet the following requirements: a. All paper records (including rejected ones) printed at the kiosk locations SHALL be deposited in a secure container; b. Vote capture device hardware, software and sensitive information (e.g., electoral roll) SHALL be physically protected to prevent unauthorized modification or disclosure; and c. Vote capture device hardware components, peripherals and removable media SHALL be identified and registered by means of a unique serial number or other identifier.	N/A	Wyle determined that this requirement is not applicable to a web based application.
5.9	**Penetration Resistance**		
5.9.1	**Resistance to Penetration Attempts**		
5.9.1.1	The voting system SHALL be resistant to attempts to penetrate the system by any remote unauthorized entity.	Penetration Test Case Host Server Security Test Case	
5.9.1.2	The voting system SHALL be configured to minimize ports, responses and information disclosure about the system while still providing appropriate functionality.	Penetration Test Case Host Server Security Test Case	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix	Test Case Description	Wyle Comment
5.9.1.3	The voting system SHALL provide no access, information or services to unauthorized entities.	Penetration Test Case Administration Test Case	
5.9.1.4	All interfaces SHALL be penetration resistant including TCP/IP, wireless, and modems from any point in the system.	Penetration Test Case	
5.9.1.5	The configuration and setup to attain penetration resistance SHALL be clearly and completely documented.	Penetration Test Case	Based on the system documentation provided by the participants in this test campaign, Wyle was unable to validate this requirement. However, Wyle deems it necessary for future testing.
5.9.2.1	The scope of penetration testing SHALL include all the voting system components. The scope of penetration testing includes but is not limited to the following: System server; Vote capture devices; Tabulation device; All items setup and configured per Technical Data Package (TDP) recommendations; Local wired and wireless networks; and03/09/2011 Internet connections.	Penetration Test Case	
5.9.2.2	Penetration testing SHALL be conducted on a voting system set up in a controlled lab environment. Setup and configuration SHALL be conducted in accordance with the TDP, and SHALL replicate the real world environment in which the voting system will be used.	Penetration Test Case	Wyle was unable to validate this requirement, but deems it necessary for future testing.
5.9.2.3	The penetration testing team SHALL conduct white box testing using manufacturer supplied documentation and voting system architecture information. Documentation includes the TDP and user documentation. The testing team SHALL have access to any relevant information regarding the voting system configuration. This includes, but is not limited to, network layout and Internet Protocol addresses for system devices and components. The testing team SHALL be provided any source code included in the TDP.	Penetration Test Case	Wyle was unable to validate this requirement, but deems it necessary for future testing.

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix	Test Case Description	Wyle Comment
5.9.2.4	Penetration testing seeks out vulnerabilities in the voting system that might be used to change the outcome of an election, interfere with voter ability to cast ballots, ballot counting, or compromise ballot secrecy. The penetration testing team SHALL prioritize testing efforts based on the following: a. Threat scenarios for the voting system under investigation; b. Remote attacks SHALL be prioritized over in-person attacks; c. Attacks with a large impact SHALL be prioritized over attacks with a more narrow impact; and d. Attacks that can change the outcome of an election SHALL be prioritized over attacks that compromise ballot secrecy or cause non-selective denial of service.	Penetration Test Case	

ATTACHMENT B

TEST CASES

Test Case:	Test Case 10 Local Ballot Delivery System A
Test Objective:	**Test Configuration:**
Verify functional operation and basic security of the system with the client and server residing on the same device.	The client and server software are located on the same PC
Devices Utilized:	Server: Apple PowerPC G4 CPU, OS X 10.5.8 Client: Safari 5.0.4

Step	Procedure	Notes
0	Record start time and date, hardware models and serial numbers, software versions for system test. Record physical location of equipment (remote / local). Get voter names and credentials from the list provided by Vendor.	
10000	Log on by starting the Safari Browser and clicking on the '[redacted]' user button and log in as the first user available on the list.	[redacted]
30000	Perform authentication necessary to access ballot distribution pages.	Images saved.
40000	Complete forms, options required by server to download a ballot. Record your inputs.	Ballot received.
45000	Verify that the system's ballot summary screen matches the election for your location.	N/A
50000	Download the ballot.	Ballot saved as pdf.
65000	Close the window (click on red button) and log off the voting system -- do not exit safari.	Exited.
70000	Attempt to print a second ballot - attempt to vote the ballot and then print. Attempt to reprint the ballot using a different delivery option (mail, email, fax).	Only one ballot option is available. Ballot can have unlimited modifications and unlimited copies.
90000	Sign out or log off the voting system.	N/A
100000	Attempt to view all temporary files to verify no sensitive information is left on the voting device. (cookies, history pages)	Using browser back button reveals all log in information.
110000	Log in as the same voter.	There is not limit on the number of times that a voter can log in and download a ballot.
120000	Attempt to print or cast a second ballot.	There is not limit on the number of times that a voter can log in and download a ballot.
130000	Log out as this user.	N/A
135000	Use "Preview" by double-clicking on the file in the finder and then fill out the ballot and associated forms and print them.	N/A
140000	Log in as administrator. View and dump all reports. Verify that all events for all users that voted are logged.	Logs retained.
150000	Dump all logs and collect screen prints, etc. Record end time.	Logs retained.
160000	END	

1

Test Case:	Test Case 01 Host Server Administration (System A)
Test Objective:	**Test Configuration:**
This test case verifies the roles of system administrator and the ability to maintain user roles, passwords, logs and other voting system administrative functions.	Host server with two terminals.
Devices Utilized:	Server: Apple PowerPC G4 CPU, OS X 10.5.8, Desktop PC with IE browser (for admin access to server), Client PC: Safari 5.0.4 (for simulating voter activity)

Step	Procedure	Notes
0	Record time and date of test, record hardware models, serial numbers and software versions	
10000	Log in as a non-administrative (operating system) account but as a voting system administrator. (BTA/chang3m3)	Log in successful.
20000	Exercise every option to view the logs, errors, activity reports, admin users.	Only has log information.
30000	View user list and attempt to add user, assign role, delete user, and reassign roles to existing user.	N/A - not possible on this system
40000	Log in as voting system super-user role, create new user and verify default role is the least privileged	N/A - not possible on this system
50000	Log in as user just created (low privileges) user and attempt to change higher priority role and / or privileges.	N/A - not possible on this system
60000	Log out and log in as super user and attempt to view storage in server such that unencrypted passwords, etc. are detected??/	N/A - not possible on this system
70000	Reset password for existing user, perform password administration such as setting minimum required password length, type of characters, capitals, etc. per NIST 800-63. (user name cannot be part of password)	N/A - not possible on this system
80000	If possible, attempt to disable/ enable the network interface.	N/A - not possible on this system
90000	Verify password histories are maintained and that user cannot reuse passwords according to the password length requirement.	N/A - not possible on this system
100000	Verify that passwords automatically expire at a specified length of time and attempt to use a password containing the user name and verify that it is rejected. (may need to set expiration date on next day and then verify after that date)	N/A - not possible on this system
110000	As administrator (super user), record default settings for log control (rqmt 5.6.1.1) verify logs are append only and read-only for authorized roles ____ verify it is not possible to alter the log..	Logs are in order by date and time.
120000	Attempt to create log failure and verify that log events, such as errors or rotation are recorded. Attempt to clear log and verify that action is	Clearing log and exporting logs are not accessible at a non-system level.

	logged. Then export the log for storage (5.6.1.8)	
130000	View log and verify it is in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format and that it has not data violating privacy. Search log and exercise any analysis tools	N/A - not possible on this system
140000	Attempt to monitor real-time reporting of system events. Log in as super admin and view any logs / reports that may provide real-time monitoring of the system activity - especially of logged on users (Check for OS capability external to voting system.)	Login attempts are logged.
150000	Attempt to log in with an invalid administrator user ID Re-attempt until sufficient attempts cause the terminal to be locked out.(Login never locks)	There does not appear to be a limit on incorrect log in attempts.
155000	Log in, change the number of attempts threshold for locking out the terminal and then repeat the process.	N/A - not possible on this system
160000	Log in as a valid administrator and don't do anything - allow the system to time out. Then log back in and verity it requires reentry of the password.	Logged in 5/5/2011 8:47:51 AM. Admin is never logged out.
170000	Record date and time of test end, collect logs and all output records. Verify events are recorded with proper order and times verify entry includes system id, timestamp, event id, success/fail, and if applicable, user id and jurisdiction id	
180000	End of test – record time and date	

Result Test Sheet

Test Case: TC03 Crypto Test Sheet System A	
Test Objective:	**Test Configuration:**
This test case verifies that the cryptographic functionality implemented by the system meets/is NIST-approved and/or FIPS 140-2 compliant.	Full test System setup, fully functional and under normal operating conditions. Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link.
Devices Utilized:	Client: Dell optima Desktop at Wyle Laboratories. Server: make and model unknown

Step	Procedure	Notes
1000	Record time and date of test, record hardware models, serial numbers and software versions.	6/1/201, Win 7, IE 8 URL:
2000	Review System documentation for cryptographic algorithms and protocols implemented by the system and record them. Note: If keys are put into the voting system manually, read step 7 before continuing.	Could not perform. No documentation provided.
3000	Check to ensure that algorithms and protocols used have gone through the Cryptographic Algorithm Validation Program or FIPS 140-2 approved. If not, that the appropriate waiver has been applied for from NIST. Additionally, check tables in SP 800-57 and ensure algorithms are at 112 bit level.	Could only check protocols used on client browser side, due to not having access to the system. Connection: TLS 1.0 AES 128 bit, RSA 2048 bit Cert: Issuer – Go Daddy, class 2, sign algorithm Sha1RSA, hash Sha1
4000	Log into system with administrative privileges. Manually verify or pull using script the permissions on appropriate cryptographic applications and files.	Could not perform. No administrative credentials provided. Only application admin credentials provided.
4100	Verify that permissions are restricted and not writable by voting system application. Record and document all observations.	Could not perform. No access to system other than client side browser connection.
5000	Pull the hash values for the cryptographic keys from the system.	Could not perform. No access to system.
6000	Check hash lengths to ensure the crypto modules are using a correct strength algorithm.	Not performed, see step 5.
7000	If keys are input manually into system, vary the key by only changing one value slightly. (e.g. Key starts with a "T" use a "t" on second entry.) Follow any system instructions to load key before starting to pull logs and data.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
7100	If system only holds and allows one key/hash; pull hash; then re-log into system reenter key following system instructions; then re-pull hash.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
7200	If the system allows more than one hash; then follow systems instruction for a specific key set then re-enter same key set changing the key as described in main step; then pull hashes.	Not performed, see step 7.
7300	Compare the hashes with the slight change; there should be significant change in hash value. Record observations.	Not performed, see step 7.

Result Test Sheet

8000	Review voting system software source code. Verify that crypto modules are being called in the correct manner to meet NIST requirements and 112 bit encryption. **Note:** The application doing the encryption maybe FIPS 140-2 compliant but, the voting application (i.e. Java code call to crypto module.) could use wrong method to encrypt at proper strength.	Not performed, code not provided.
9000	Key Management, Perform this step if cryptographic keys are generated internally. Review voting system documentation to see what type encryption methods is deployed.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
9100	Review source code and take note to ensure that methods used comply with FIPS 140-2. This should be done by referring to annex A, C or D of 140-2. Record all observations and discrepancies.	Not performed, code not provided.
9200	Pull file permissions of those executable and library files in the system. Ensure they have restricted access and are properly controlled. Record all observations.	No access to system other than application usage. This step Not performed.
10000	Perform key entry procedures following voting system documentation. Verify that input and output are NIST compliant.	No access to system other than application usage. This step Not performed.
10100	If automated method is used input and output from system must be encrypted. Record observations.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
10200	If a manual method is used input and output from system maybe plaintext. Record observations. **Note:** Transportation and any other processes dealing with the input and output data should reviewed to verify proper security measures are being applied.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
11000	Perform Key zeroization procedures following voting system documentation. Verify that the key no longer exist on the system after completion of procedure. Record all observations.	Not performed, see step 10.
12000	Perform rekeying procedures following voting system documentation. Verify the system performs as documented and is compliant. Record all observations.	Not performed, see step 10.
13000	During Operational tests, ensure that the voting system supports rekeying during communications. This should be done by verifying protocols used and/or sniffing network traffic and examining the packets. Note: System documentation should but may not state the amount or limit of data encrypted with the same key. The key could change on a daily basis, when a pre-set volume of data has been transmitted or a given period of time has elapsed.	Verified protocols being used but, did not monitor traffic due to the whole system not being in Wyle testing lab.

Result Test Sheet

	Most systems, implement rekeying by forcing a new key exchange, typically through a separate protocol like Internet key exchange (IKE). (e.g. Wi-Fi Protected Access (WPA), does this by frequently replacing session keys through the Temporal Key Integrity Protocol (TKIP))	
14000	During Operational tests, ensure that the voting system uses NIST or FIPS approved protocols for communications. Record all observations. **Note:** This should be done by sniffing network traffic (i.e. Wireshark) and examining the packets.	Verified protocols being used from client side browser.
15000	End of test – record time and date	6/1/2011

Additional Notes:

- Only IE browser tested.
- Side issues – web browser can be any type and Adobe any version. This can lead to issues surrounding a compromised machine being used on client side. Should be further tested (possibly as part of pen test).

Result Test Sheet

Test Case: 05 Discovery Penetration System A	
Test Objective:	**Test Configuration:**
This test seeks out vulnerabilities in the voting system, verifies the system's resistance to any remote unauthorized entity. That the system provides no access, information or services to unauthorized entities and is configured to minimize ports and information disclosure about the system.	Full System with host, remote terminal and communication devices. Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link. Full test System setup, fully functional and under normal operating conditions.
Devices Utilized:	BackTrack OS with Nessus Laptop

Step	Procedure	Notes
1000	Record time and date of test start, model and serial number of hardware, software with version numbers.	12:30 6/8/2011 HP Pavilion dv6 laptop running Backtrack 4 R2 as OS with Nessus installed. Nessus version : 4.4.1 feed ver. : 201105041534 Scanner MAC : 00:0f:00:3a:3b:c7 Scanner IP : 10.10.13.124 Metasploit v3.7.0 svn r12540
2000	Record IP and URL addresses to be tested.	[redacted]
3000	Scan IP and URL ranges with Nmap, unobtrusive.	Port 80, 443 open. Apple Mac OS X 10.6.X|10.5.X (86%) file: [redacted]
4000	Scan from inside target/s netmask range. Save results to file.	N/A
5000	Scan target/s from outside interfaces. Save results to file.	See step 3.
6000	If needed and applicable, scan IP and URL ranges with Nmap, aggressive. Save results to file.	Not required.
7000	Scan IP and URL ranges with Nessus, unleveraged "no credentials". Save scan result, in file name indicate unleveraged.	Scanned with Nessus polices (see files); Web Apps- [redacted] External- [redacted]
8000	Scan from inside target/s netmask range. Save results, indicating "inside" (e.g. system_noC_in.xml)	N/A
9000	If applicable, scan target/s from outside interfaces. Save results, indicating "outside" (e.g. system_noC_out.xml)	See step 7.
10000	Scan IP and URL ranges with Nessus, leveraged "with credentials". Save scan result, in file name indicating leveraged. Note: This type scan is usually done from "inside" only.	Not done, no credentials were provided.
11000	Probe target URL for further information. (i.e. URL manipulation, input/form field manipulation, SQL injection, etc.) Record all observations and displayed information.	Simple SQL injection not effective.
12000	Review all scan results and recorded information.	2 open ports, 11 low vulnerabilities, scans hung no OS detection
13000	Annotate record and organize all pertinent information (e.g. Ports, Protocols, Services, versioning, etc.) from	Done.

Result Test Sheet

	the results for second phase of Pen test.	
14000	From review of pertinent information, setup/develop and additional discovery scans/tests as needed.	Not needed.
15000	Perform any additional discovery scans or tests as needed. Save and record these results.	N/A
16000	Review all results, notes and finalize exploratory tests for second phase of testing.	With time restrictions went with port exploits as primary attack method. Also, attempt login with application credentials.
17000	End of test – record time and date	14:20 6/8/2011

Additional Notes:

- Nessus web scan hung at 90%. Restarted but due to time restrictions had to stop before completion.
- Metasploit port attacks were used (examples; webdav_upload_upload_asp, hagent_untrusted_hsdata, RealServer describe Buffer Overflow).
- None of attempted exploits succeeded. More detailed attempts against the OS or more detailed SQL attempts maybe successful but, require more time than was currently allocated.

Test Case:	Test Case 01 Host Server Administration System B
Test Objective:	**Test Configuration:**
This test case verifies the roles of system administrator and the ability to maintain user roles, passwords, logs and other voting system administrative functions.	Host server accessed through a secure link via the internet to URL (TBS)
Devices Utilized:	Client: Dell Optiplex 780, Server: provided by Microsoft Azure Cloud Service

Step	Procedure	
0	Record time and date of test, record hardware models, serial numbers and software versions	
10000	Log in with the administrative account provided by the vendor. (this is an "administrator" role with full privileges)	"wyle@[redacted]" pass: "wyle"
20000	Dump system Logs. Then view the logs and save. Attempt to change and/or reset the log. Verify they cannot be altered.	Only log available is for voter log in . Other logs are not developed.
30000	View user list and attempt to add user, assign role, delete user, and reassign roles to existing user.	Add User page currently does not function.
40000	Log in as voting system administrator (full privileges) role, create a new user and verify default role is the least privileged. Note information entered for this user and add one more user for each administrator role.	Add User page currently does not function.
50000	Perform a series of log-ins, one for each role, and attempt to exercise privileges not allowed for that role, verify each role can only view/modify the items there are authorized..	Only have one admin user. Add user function currently not working.
60000	Log out and log in as super user and attempt to view storage in server such that unencrypted passwords, etc are detected??/	User information can not currently be edited.
70000	Reset password for existing user, perform password administration such as setting minimum required password length, type of characters, capitals, etc. per NIST 800-63. (user name cannot be part of password)	Currently a password of one character is acceptable. No history of passwords is retained and password can match log in.
90000	Verify password histories are maintained and that user cannot reuse passwords according to the password length requirement. Attempt to use a password containing the user name and verify that it is rejected.	No history of passwords is retained and password can match log in.
100000	Verify that passwords automatically expire at a specified length of time. (may need to set expiration date on next day and then verify after that date)	There is not expiration for passwords.
110000	As administrator (super user), record default settings for log control (rqmt 5.6.1.1) verify logs are append only and read-only for authorized roles ____ verify it is not possible to alter the log..	Only log is for voter log in information. This log is appended.

120000	Attempt to create log failure and verify that log events, such as errors or rotation are recorded. Attempt to clear log and verify that action is logged. Then export the log for storage (5.6.1.8)	Log has recorded an attempted login failure.
130000	View log and verify it is in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format and that it has not data violating privacy. Search log and exercise any analysis tools	Log is not exportable.
140000	Attempt to monitor real-time reporting of system events. Log in as super admin and view any logs / reports that may provide real-time monitoring of the system activity - especially of logged on users (Check for OS capability external to voting system.)	Voter log is real time.
150000	Attempt to log in with an invalid administrator user ID Re-attempt until sufficient attempts cause the terminal to be locked out.	System does not lock out an admin.
155000	Log in, change the number of attempts threshold for locking out the terminal and then repeat the process.	System does not support this from an admin page.
160000	Log in as a valid administrator and don't do anything - allow the system to time out. Then log back in and verity it requires reentry of the password.	No timeout after an hour.
165000	Export the voting system log to external device for archiving	No export option.
170000	Record date and time of test end, collect logs and all output records. Verify events are recorded with proper order and times verify entry includes system id, timestamp, event id, success/fail, and if applicable, user id and jurisdiction id	No logs to record.
180000	End of test – record time and date	

Result Test Sheet

Test Case:	03 Crypto Test Sheet System B	
Test Objective:	**Test Configuration:**	
This test case verifies that the cryptographic functionality implemented by the system meets/is NIST-approved and/or FIPS 140-2 compliant.	Full test System setup, fully functional and under normal operating conditions. Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link.	
Devices Utilized:	Client: Dell optima Desktop at Wyle Laboratories. Server: make and model unknown	
Step	**Procedure**	**Notes**
1000	Record time and date of test, record hardware models, serial numbers and software versions.	17:50 6/14/2011, Win 7, IE 8 URL: [redacted]
2000	Review System documentation for cryptographic algorithms and protocols implemented by the system and record them. **Note:** If keys are put into the voting system manually, read step 7 before continuing.	Could not perform. No documentation provided.
3000	Check to ensure that algorithms and protocols used have gone through the Cryptographic Algorithm Validation Program or FIPS 140-2 approved. If not, that the appropriate waiver has been applied for from NIST. Additionally, check tables in SP 800-57 and ensure algorithms are at 112 bit level.	Could only check protocols used on client browser side, due to not having access to the system. Admin account page had NO cert! Connection: TLS 1.0 AES 128 bit, RSA 2048 bit Cert: Issuer – Go Daddy, class 3, sign algorithm Sha1RSA, hash Sha1
4000	Log into system with administrative privileges. Manually verify or pull using script the permissions on appropriate cryptographic applications and files.	Could not perform. No administrative credentials provided. Only application admin credentials provided.
4100	Verify that permissions are restricted and not writable by voting system application. Record and document all observations.	Could not perform. No access to system other than client side browser connection.
5000	Pull the hash values for the cryptographic keys from the system.	Could not perform. No access to system.
6000	Check hash lengths to ensure the crypto modules are using a correct strength algorithm.	Could not perform. No access to system.
7000	If keys are input manually into system, vary the key by only changing one value slightly. (e.g. Key starts with a "T" use a "t" on second entry.) Follow any system instructions to load key before starting to pull logs and data.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
7100	If system only holds and allows one key/hash; pull hash; then re-log into system reenter key following system instructions; then re-pull hash.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
7200	If the system allows more than one hash; then follow systems instruction for a specific key set then re-enter same key set changing the key as described in main step; then pull hashes.	Not performed, see step 7.
7300	Compare the hashes with the slight change; there should be significant change in hash value. Record observations.	Not performed, see step 7.

Result Test Sheet

8000	Review voting system software source code. Verify that crypto modules are being called in the correct manner to meet NIST requirements and 112 bit encryption. **Note:** The application doing the encryption maybe FIPS 140-2 compliant but, the voting application (i.e. Java code call to crypto module.) could use wrong method to encrypt at proper strength.	Not performed, code not provided.
9000	Key Management, Perform this step if cryptographic keys are generated internally. Review voting system documentation to see what type encryption methods is deployed.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
9100	Review source code and take note to ensure that methods used comply with FIPS 140-2. This should be done by referring to annex A, C or D of 140-2. Record all observations and discrepancies.	Not performed, code not provided.
9200	Pull file permissions of those executable and library files in the system. Ensure they have restricted access and are properly controlled. Record all observations.	No access to system other than application usage. This step Not performed.
10000	Perform key entry procedures following voting system documentation. Verify that input and output are NIST compliant.	No access to system other than application usage. This step Not performed.
10100	If automated method is used input and output from system must be encrypted. Record observations.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
10200	If a manual method is used input and output from system maybe plaintext. Record observations. **Note:** Transportation and any other processes dealing with the input and output data should reviewed to verify proper security measures are being applied.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
11000	Perform Key zeroization procedures following voting system documentation. Verify that the key no longer exist on the system after completion of procedure. Record all observations.	No access to system other than application usage. This step Not performed.
12000	Perform rekeying procedures following voting system documentation. Verify the system performs as documented and is compliant. Record all observations.	No access to system other than application usage. This step Not performed.
13000	During Operational tests, ensure that the voting system supports rekeying during communications. This should be done by verifying protocols used and/or sniffing network traffic and examining the packets. **Note:** System documentation should but may not state the amount or limit of data encrypted with the same key. The key could change on a daily basis, when a pre-set volume of data has been transmitted or a given period of time has elapsed.	Verified protocols being used but, did not monitor traffic due to the whole system not being in Wyle testing lab.

Result Test Sheet

	Most systems, implement rekeying by forcing a new key exchange, typically through a separate protocol like Internet key exchange (IKE). (e.g. Wi-Fi Protected Access (WPA), does this by frequently replacing session keys through the Temporal Key Integrity Protocol (TKIP))	
14000	During Operational tests, ensure that the voting system uses NIST or FIPS approved protocols for communications. Record all observations. **Note:** This should be done by sniffing network traffic (i.e. Wireshark) and examining the packets.	Verified protocols being used from client side browser.
15000	End of test – record time and date	18:48 6/14/2011

Additional Notes:

- Only IE browser tested.

Test Case: Test Case 04 Normal Ballot Delivery System B	
Test Objective:	**Test Configuration:**
One ballot will be delivered to the terminal and displayed and/or printed to exercise the normal processing path for delivery of ballot. The test will verify that: 1. The system delivers that ballot to the voter 2. The system implements authentication prior to allowing the voter access to the ballot. 3. The system adequately logs the event of transferring the ballot. 4. The ballot that is delivered is identical to the ballot that was provided by the Election Management System.	Host server accessed through a secure link via the internet to URL (TBS)
Devices Utilized:	Client: Dell Optiplex 780, Server: provided by Microsoft Azure Cloud Service

Step	Procedure	
0	Record start time and date, hardware models and serial numbers, software versions for system test. Record physical location of equipment (remote / local) :::HOT KEYS;<ctrl ;> for current date, <ctrl shift ;> for time.	
10000	Log on as a voter to the system (a non-administrator account on this terminal) .(during the following steps, record each action and response by the system so that at the end, we can verify that all significant events were logged)	Sample Voter (NP) 123 Sample Drive, Springfield 12345
30000	Perform authentication necessary to access ballot distribution pages.	Only requires a 5 digit pin.
40000	Select ballot from list and note which one you selected. Select Mail as delivery option.	Sample Voter (NP) 123 Sample Drive, Springfield 12345 received error message for coding error.
50000	Download the ballot package	Download ballots do not contain all the information necessary for returning the ballot.
60000	If voting is an option, then do NOT vote at this time and print the ballot.	Ballot not voted
70000	Attempt to print a second ballot - attempt to vote the ballot and then print. Attempt to reprint the ballot using a different delivery option (mail, email, fax) (Attempt to use browser back button to return to options)	No limit on reprints.
80000	Repeat step selection mark and print option	Same voter can vote again.
90000	Sign out or log off as this voter. Repeat step using mark and save option with new voter. (using email option)	Ballot marked and saved
100000	View all temporary files to verify no voting information is left on the voting device.	The browser back button allows someone to return to the previous ballot.
110000	Log in as the same voter	No limit in place to stop voters from voting multiple times.

120000	Attempt to print or cast a second ballot	Can get unlimited ballots.
140000	Log off -- and log in as administrator. View and dump logs. Verify that all events for all users that voted are logged. If on the same terminal as voter, then search for files/temporary storage that contains any voter information.	Log records voter actions.
150000	Examine and Dump all logs and collect screen prints, etc. On both the server and the client.	No other logs available.
160000	End of test – record time and date	

Result Test Sheet

Test Case: 05 Discovery Penetration System B	
Test Objective:	**Test Configuration:**
This test seeks out vulnerabilities in the voting system, verifies the system's resistance to any remote unauthorized entity. That the system provides no access, information or services to unauthorized entities and is configured to minimize ports and information disclosure about the system.	Full System with host, remote terminal and communication devices. Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link. Full test System setup, fully functional and under normal operating conditions.
Devices Utilized:	BackTrack OS with Nessus Laptop

Step	Procedure	Notes
1000	Record time and date of test start, model and serial number of hardware, software with version numbers.	16:35 6/14/2011 HP Pavilion dv6 laptop running Backtrack 4 R2 as OS with Nessus installed. Nessus version : 4.4.1 feed ver. : 201105041534 Scanner MAC : 00:0c:43:78:6e:ca Scanner IP : 10.10.13.124 Metasploit v3.7.0 svn r12540
2000	Record IP and URL addresses to be tested.	[redacted]
3000	Scan IP and URL ranges with Nmap, unobtrusive.	Port 21, 22, 80 and 443 open. Linux 2.6.18 (93%) file: [redacted]
4000	Scan from inside target/s netmask range. Save results to file.	N/A
5000	Scan target/s from outside interfaces. Save results to file.	See step 3.
6000	If needed and applicable, scan IP and URL ranges with Nmap, aggressive. Save results to file.	Not required.
7000	Scan IP and URL ranges with Nessus, unleveraged "no credentials". Save scan result, in file name indicate unleveraged.	Scanned with Nessus polices (see files); Web Apps- [redacted] External- [redacted]
8000	Scan from inside target/s netmask range. Save results, indicating "inside" (e.g. system_noC_in.xml)	N/A
9000	If applicable, scan target/s from outside interfaces. Save results, indicating "outside" (e.g. system_noC_out.xml)	See step 7.
10000	Scan IP and URL ranges with Nessus, leveraged "with credentials". Save scan result, in file name indicating leveraged. Note: This type scan is usually done from "inside" only.	Not done, no credentials were provided.
11000	Probe target URL for further information. (i.e. URL manipulation, input/form field manipulation, SQL injection, etc.) Record all observations and displayed information.	Simple SQL injection not effective. Did however gather good information, with more time could have possible gained access. See file error_withInfo.png for example.
12000	Review all scan results and recorded information.	4 open ports, 1 medium and 45 low vulnerabilities, Linux 2.6
13000	Annotate record and organize all pertinent information (e.g. Ports, Protocols, Services, versioning, etc.) from	Done.

Result Test Sheet

	the results for second phase of Pen test.	
14000	From review of pertinent information, setup/develop and additional discovery scans/tests as needed.	Not needed.
15000	Perform any additional discovery scans or tests as needed. Save and record these results.	N/A
16000	Review all results, notes and finalize exploratory tests for second phase of testing.	With time restrictions went with port exploits as primary attack method. Also, attempt login with application credentials.
17000	End of test – record time and date	18:37 6/14/2011

Additional Notes:

- More time on pen test or closer to the parameters of requirement to white box testing and access to system would most likely occur.
- Metasploit port attacks were used (examples; webdav_upload_upload_asp, hagent_untrusted_hsdata, RealServer describe Buffer Overflow).
- None of attempted exploits succeeded. More detailed attempts against the OS or more detailed SQL attempts maybe successful but, require more time than was currently allocated.

Test Case: Test Case 01 Host Server Administration System C	
Test Objective:	**Test Configuration:**
This test case verifies the roles of system administrator and the ability to maintain user roles, passwords, logs and other voting system administrative functions.	Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link.
Devices Utilized:	Client: Dell optima Desktop at Wyle Laboratories. Server: make and model unknown

Step	Procedure	Notes
1000	Record time and date of test, record hardware models, serial numbers and software versions	
2000	Log in with the administrative account provided by the vendor. (This is an "administrator" role vs. the less privileged "operator" role.	Login admin Wyleadmin / #20wyle11#
3000	Dump system logs. Then view the logs and compare them to the report listed in the "audit" screen.	The Audit screen showed events that are not in the event log.
4000	View user list and add one user with "administrator" privileges and two with "operator" privileges. Note the name, password and role for each user. Verify default role is "operator". Create one password containing the user name.	Entered name "Wyle Tester", username "Wyletester", password "wyle", no role selected. It responded with "password strength not correct" tried "wyle11" and still not good, tried "Wyle11" - no, tried "wylelabs" no, tried "wylelab11" - it took that and gave me administrator role as default. Entered Wyle operator, user name "wyleoperator", password "wyleoperator". got "password strength not correct" entered password of "wyleoperator11" same result, tried "wyleoperator1A" Password strength not correct, tried "Wyleoperator11" not good enough, tried "WWyleoperator 11" tried changed last name to "Wyleoperator", password to "Wyleoperator" and it failed again. Tried password "WWyleoperator11", no; tried "wylelab11" - it took it. Apparently it does not allow "user name" in the password. Added wyle "operatortwo", username "operatortwo", password "wylelab12" as operator role.
5000	Exercise the search options on the "user management" screen. Search for "user name", for "role", for all and for combination of user name and role.	Searched on name "Wyle" and it found the correct users. It found users ok when I selected "administrator role" and for "operator role". Selected name of "Wyle testers" with no role criteria and it did not find it. Selected "tester" and it found it. Selected "operator" and it found the two with last names containing "operator".
6000	Edit an administrator with "operator" role by changing all fields, note the changes and save them. Select a user with "administrator" privilege and modify the username and save	Changed entry for "wyle operatortwo", to "replace1 replace2", replaceusername, "Twylelab11", "Twylelab11" and role change to administrator. It accepted the changes.
7000	Log in as user just created (operator) user and attempt to change higher priority role and / or privileges.	Logged out and logged back in as "operatortwo", "wylelab11". It did not allow access to "user management". Could not change roles or any information about "operatortwo".

8000	As operator, attempt to perform each administrator function and note which ones are allowed to take on "operator" role.	Attempted to access the "security question" - was logged out. Tried two more times and was logged out each time. Could not perform any of the functions on the bottom of the administrative screen where a administrator password is required.
9000	Log out and log back in as an administrator with "administrator" role.	Logged in.
10000	Reset password for existing user, perform password administration such as setting minimum required password length, type of characters, capitals, etc. per NIST 800-63. (user name cannot be part of password)	Password is not configurable from admin screen.
11000	If possible, attempt to disable/ enable the network interface.	Not possible from here.
12000	Verify password histories are maintained and that user cannot reuse passwords according to the password length requirement.	There is nothing in place to limit reusing historical passwords.
13000	Verify that passwords automatically expire at a specified length of time and attempt to use a password containing the user name and verify that it is rejected. (may need to set expiration date on next day and then verify after that date)	Passwords containing the user names are not accepted. Need to verify what the password timeout period is.
14000	As administrator (super user), record default settings for log control (rqmt 5.6.1.1) verify logs are append only and read-only for authorized roles ____ verify it is not possible to alter the log. (do this for both the "audit" and "export" logs)	Audit log is not exportable. Exporting log contains admin log functions.
15000	Attempt to create log failure and verify that log events, such as errors or rotation are recorded. Attempt to clear log and verify that action is logged. Then export the log for storage (5.6.1.8) (do for both "audit" and "export" logs.	Logs only admin functions.
16000	Export log data into a publicly documented format and verify that it contains no data violating voter privacy. Search log -- do for both "audit" and "export" logs.	Audit log is not exportable. Exporting log contains admin log functions.
17000	Monitor real-time reporting of system events. View logs and if necessary, log in as a voter and verify that log is updated with voter actions.	Logs only admin functions and successful login attempts. No voter logins are recorded.
18000	Log out and then attempt to log in with an invalid administrator user ID Re-attempt until sufficient attempts cause the terminal to be locked out.	Attempted to log in as "wyle". Logged in 12 times with incorrect password. User was never locked out.
19000	Log in, change the number of attempts threshold for locking out the terminal and then repeat the process.	This function not configurable.
20000	Log in as a valid administrator and don't do anything - allow the system to time out. Then log back in and verity it requires reentry of the password.	System logs out after 5 minutes.

21000	Log in, allow the time to drop to 1 minute and then select an action or click on a button, anything that causes the system to reset the time.	Select another page - restarts counter at 5 minutes
22000	Record date and time of test end, collect logs and all output records. Verify events are recorded with proper order and times verify entry includes system id, timestamp, event id, success/fail, and if applicable, user id and jurisdiction id	Logs recorded and reviewed
23000	End of test – record time and date	

Result Test Sheet

Test Case:	03 Crypto Test Sheet System C
Test Objective:	**Test Configuration:**
This test case verifies that the cryptographic functionality implemented by the system meets/is NIST-approved and/or FIPS 140-2 compliant.	Full test System setup, fully functional and under normal operating conditions. Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link.
Devices Utilized:	Client: Dell optima Desktop at Wyle Laboratories. Server: make and model unknown

Step	Procedure	Notes
1000	Record time and date of test, record hardware models, serial numbers and software versions.	6/1/2011, Win 7, IE 8 URL:
2000	Review System documentation for cryptographic algorithms and protocols implemented by the system and record them. **Note:** If keys are put into the voting system manually, read step 7 before continuing.	Could not perform. No documentation provided.
3000	Check to ensure that algorithms and protocols used have gone through the Cryptographic Algorithm Validation Program or FIPS 140-2 approved. If not, that the appropriate waiver has been applied for from NIST. Additionally, check tables in SP 800-57 and ensure algorithms are at 112 bit level.	Could only check protocols used on client browser side, due to not having access to the system. Connection: TLS 1.0 AES 128 bit, RSA 1024 bit Cert: Issuer – VeriSign, class 3, sign algorithm Sha1RSA, hash Sha1
4000	Log into system with administrative privileges. Manually verify or pull using script the permissions on appropriate cryptographic applications and files.	Could not perform. No administrative credentials provided. Only application admin credentials provided.
4100	Verify that permissions are restricted and not writable by voting system application. Record and document all observations.	Could not perform. No access to system other than client side browser connection.
5000	Pull the hash values for the cryptographic keys from the system.	Could not perform. No access to system.
6000	Check hash lengths to ensure the crypto modules are using a correct strength algorithm.	Could not perform. No access to system.
7000	If keys are input manually into system, vary the key by only changing one value slightly. (e.g. Key starts with a "T" use a "t" on second entry.) Follow any system instructions to load key before starting to pull logs and data.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
7100	If system only holds and allows one key/hash; pull hash; then re-log into system reenter key following system instructions; then re-pull hash.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
7200	If the system allows more than one hash; then follow systems instruction for a specific key set then re-enter same key set changing the key as described in main step; then pull hashes.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
7300	Compare the hashes with the slight change; there should be significant change in hash value. Record observations.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.

Result Test Sheet

8000	Review voting system software source code. Verify that crypto modules are being called in the correct manner to meet NIST requirements and 112 bit encryption. **Note:** The application doing the encryption maybe FIPS 140-2 compliant but, the voting application (i.e. Java code call to crypto module.) could use wrong method to encrypt at proper strength.	Not performed, code not provided.
9000	Key Management, Perform this step if cryptographic keys are generated internally. Review voting system documentation to see what type encryption methods is deployed.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
9100	Review source code and take note to ensure that methods used comply with FIPS 140-2. This should be done by referring to annex A, C or D of 140-2. Record all observations and discrepancies.	Not performed, code not provided.
9200	Pull file permissions of those executable and library files in the system. Ensure they have restricted access and are properly controlled. Record all observations.	No access to system other than application usage. This step Not performed.
10000	Perform key entry procedures following voting system documentation. Verify that input and output are NIST compliant.	No access to system other than application usage. This step Not performed.
10100	If automated method is used input and output from system must be encrypted. Record observations.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
10200	If a manual method is used input and output from system maybe plaintext. Record observations. **Note:** Transportation and any other processes dealing with the input and output data should reviewed to verify proper security measures are being applied.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
11000	Perform Key zeroization procedures following voting system documentation. Verify that the key no longer exist on the system after completion of procedure. Record all observations.	No access to system other than application usage. This step Not performed.
12000	Perform rekeying procedures following voting system documentation. Verify the system performs as documented and is compliant. Record all observations.	No access to system other than application usage. This step Not performed.
13000	During Operational tests, ensure that the voting system supports rekeying during communications. This should be done by verifying protocols used and/or sniffing network traffic and examining the packets. **Note:** System documentation should but may not state the amount or limit of data encrypted with the same key. The key could change on a daily basis, when a pre-set volume of data has been transmitted or a given period of time has elapsed.	Verified protocols being used but, did not monitor traffic due to the whole system not being in Wyle testing lab.

Result Test Sheet

	Most systems, implement rekeying by forcing a new key exchange, typically through a separate protocol like Internet key exchange (IKE). (e.g. Wi-Fi Protected Access (WPA), does this by frequently replacing session keys through the Temporal Key Integrity Protocol (TKIP))	
14000	During Operational tests, ensure that the voting system uses NIST or FIPS approved protocols for communications. Record all observations. **Note:** This should be done by sniffing network traffic (i.e. Wireshark) and examining the packets.	Verified protocols being used from client side browser.
15000	End of test – record time and date	6/1/2011

Additional Notes:

- Only IE browser tested.
- Side issue – No browser restriction, web browser can be any type. This can lead to issues surrounding a compromised machine being used on client side.

Result Test Sheet

Test Case:	05 Discovery Penetration System C
Test Objective:	**Test Configuration:**
This test seeks out vulnerabilities in the voting system, verifies the system's resistance to any remote unauthorized entity. That the system provides no access, information or services to unauthorized entities and is configured to minimize ports and information disclosure about the system.	Full System with host, remote terminal and communication devices. Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link. Full test System setup, fully functional and under normal operating conditions.
Devices Utilized:	BackTrack OS with Nessus Laptop

Step	Procedure	Notes
1000	Record time and date of test start, model and serial number of hardware, software with version numbers.	15:10 6/1/2011 HP Pavilion dv6 laptop running Backtrack 4 R2 as OS with Nessus installed. Nessus version : 4.4.1 feed ver. : 201105041534 Scanner MAC : 00:02:16:09:de:66 Scanner IP : 10.10.13.123 Metasploit v3.7.0 svn r12540
2000	Record IP and URL addresses to be tested.	[redacted]
3000	Scan IP and URL ranges with Nmap, unobtrusive.	Port 80, 443 open. Server 2008 (90%) file: [redacted]
4000	Scan from inside target/s netmask range. Save results to file.	N/A
5000	Scan target/s from outside interfaces. Save results to file.	See step 3.
6000	If needed and applicable, scan IP and URL ranges with Nmap, aggressive. Save results to file.	Not required.
7000	Scan IP and URL ranges with Nessus, unleveraged "no credentials". Save scan result, in file name indicate unleveraged.	Scanned with Nessus polices (see files); Web Apps- [redacted] External- [redacted]
8000	Scan from inside target/s netmask range. Save results, indicating "inside" (e.g. system_noC_in.xml)	N/A
9000	If applicable, scan target/s from outside interfaces. Save results, indicating "outside" (e.g. system_noC_out.xml)	See step 7.
10000	Scan IP and URL ranges with Nessus, leveraged "with credentials". Save scan result, in file name indicating leveraged. Note: This type scan is usually done from "inside" only.	Not done, no credentials were provided.
11000	Probe target URL for further information. (i.e. URL manipulation, input/form field manipulation, SQL injection, etc.) Record all observations and displayed information.	Simple SQL injection not effective.
12000	Review all scan results and recorded information.	2 open ports, 22 low vulnerabilities, Windows Server 2008 R2
13000	Annotate record and organize all pertinent information (e.g. Ports, Protocols, Services, versioning, etc.) from	Done.

Result Test Sheet

	the results for second phase of Pen test.	
14000	From review of pertinent information, setup/develop and additional discovery scans/tests as needed.	Not needed.
15000	Perform any additional discovery scans or tests as needed. Save and record these results.	N/A
16000	Review all results, notes and finalize exploratory tests for second phase of testing.	With time restrictions went with port exploits as primary attack method. Also, attempt login with application credentials.
17000	End of test – record time and date	17:40 6/1/2011

Additional Notes:

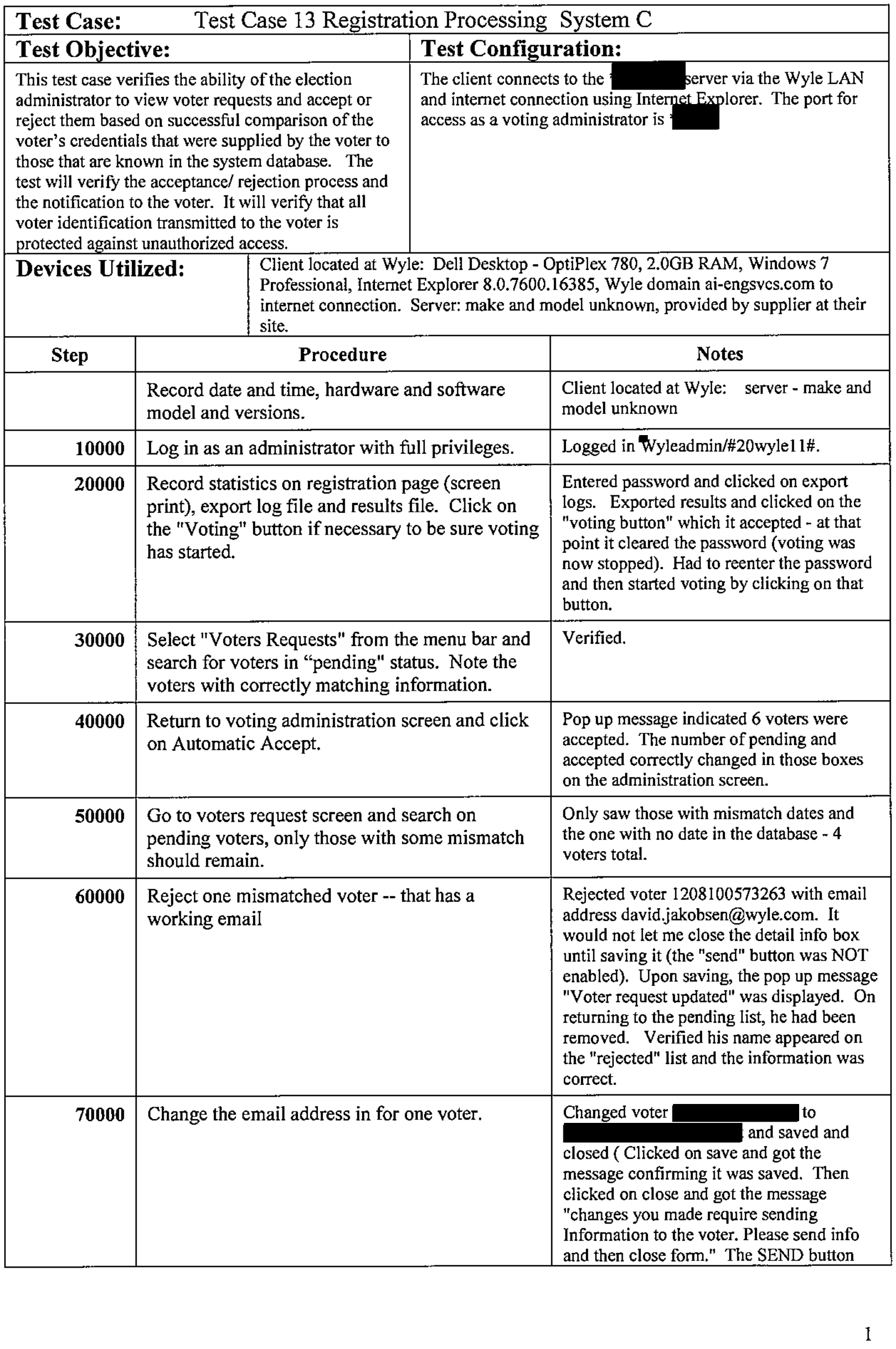
- Metasploit port attacks were used (examples; webdav_upload_upload_asp, hagent_untrusted_hsdata, RealServer describe Buffer Overflow).
- None of attempted exploits succeeded. More detailed attempts against the OS or more detailed SQL attempts maybe successful but, require more time than was currently allocated.

Test Case:	Test Case 12 Voter Registration Request System C
Test Objective:	**Test Configuration:**
This test case verifies that a voter can securely register to vote on-line. The test includes authentication that the voter is the voter that he/she claims to be and that the request is queued for processing by an election administrator.	The client connects to the ******* server via the Wyle LAN and internet connection using Internet Explorer. The port for access as a voting administrator is *****
Devices Utilized:	Client located at Wyle: Dell Desktop - OptiPlex 780, 2.0GB RAM, Windows 7 Professional, Internet Explorer 8.0.7600.16385, Wyle domain ai-engsvcs.com to internet connection. Server: make and model unknown, provided by [redacted] at their site.

Step	Procedure	Notes
0	Record date and time, equipment with model numbers, server software versions.	-
10000	Log into the administrator screen, record statistics on screen (take a screen print) and select an unregistered voter for testing. (you will be selecting a number of voters from the list) Set "registration" voting on by clicking on the button to start it)	Logged in to admin screen as Wyleadmin/#20wyle11#, Dumped log to get initial content. Searched on "rejected voters" and stored snip of a list of available voters.
20000	Go to the voter registration screen -- ([redacted]) and using the voter credentials log in with the correct name, voter ID	At that screen, selected "vote" -- then went back and selected "Register".
27500	Select a voter that has not yet registered by searching on a name in the "electors" search screen.	Using [redacted] logged onto registration screen.
30000	Complete the registration screen by providing a valid email (yours) that you can access and a secret question with answer and the correct birth year for this voter. Submit that form. And click finish on the review screen -- close the browser.	Saved screen shot.
40000	Repeat the registration process with the same voter on each screen	Attempted to use the browser back button to re-enter registration information, but it gave me a "webpage has expired" message. I attempted to login under the "register" option, it gave the "Request with given NRC Id is already created" message. I then went back to the initial screen and selected the "voting" option. It rejected my log on with "Elector with given ID in not an eligible voter."
50000	Select a different voter from the unregistered voters in the database.	Selected unregistered voter [redacted]
60000	Using this voter, enter the ID, voter name correctly but enter an incorrect year.	Entered with year 2000. The vote request was accepted.
70000	Select a different voter from the unregistered voters in the database	Selected [redacted]
80000	Using this voter, enter the ID and Year correctly, but misspell the first name. Complete the registration process.	The previous screen was up, I pressed the browser back button and got the "web page expired" message. So then hit the browser "reload" button and it brought up the login

		screen - blank, no information from the previous voter. Entered voter as specified above - system rejected registration with a wrong first name -- "There is no elector with given parameters".
85000	Select a non-registered voter with no birth date in the database and do a valid registration.	Selected voter [redacted] [redacted] no birth date. I entered a birth date of [redacted]. It confirmed that it has received the request.
90000	Select a different voter from the unregistered voters in the database	Selected [redacted]
100000	Using this voter, enter the ID and year correctly but misspell the last name and complete the registration process.	It rejected the request -- "there is no elector with given parameters"
110000	Select a different voter from the unregistered voters in the database	Selected [redacted]
120000	Enter invalid data into the login screen, click on Reset form	Entered invalid ID number -- it required me to enter the correct number of digits before it would give the green check mark. Selected "Reset" - form cleared all of the fields.
130000	Enter valid login information -- and proceed to the next screen.	Done.
140000	Enter information in the next form and use the reset button to clear the fields.	Done.
150000	Press the submit button with all fields clear	All fields lit up with red indicating they were required.
160000	Complete the form correctly except for year of birth and submit the form	It would not accept input. System required me to enter date in order to accept it
170000	Complete the form correctly except for the secret question / answer	Entered a valid date and removed the question -- it would not accept the form and highlighted the missing question box.
180000	Select the email option, complete the form but do not enter an email address	System would not accept the form without an email address.
190000	Select the email option, complete the form, but incorrectly enter the email confirmation address	System flagged the confirmation address and did not accept the form.
200000	Complete the form enter an incorrect year, do not enter an email address and select the "regular mail" option and submit the form but when the review screen appears, select "go back".	PM Erased the email addresses and clicked on the regular mail button. The email address remained in red with the notation that "this information is mandatory, please enter your email address". Scrolled up and it appeared. Clicked "extend" but it timed out while attempting to write the exception. Picked regular mail submitted it and selected "go back". The system went all the way back to the login screen and cleared all fields.
210000	Revise the year so that all data is correct and submit the registration request.	Re-enter log data. For voter [redacted] regular mail, selected "finish" on review screen and got confirmation message.

220000	Log off as a voter.	Done.
225000	From the list of unregistered voters, logon and enter requests for 8 more voters. Enter valid requests with matching information on at least 5 and incorrect dates on 3. Use a variety of email addresses - one of them with only one voter associated.	Enter voters -- [redacted]
230000	Log in as administrator, record statistics and view logs and verify that the requests have been queued. -- view pending requests and verify content of each request entered in this test.	Stored images of statistics screen and pending voters screen. Unable to view log requests on-line. The pending voters and the information for each one was correct.
250000	End of test record date and time of end.	



Test Case: Test Case 13 Registration Processing System C

Test Objective:

This test case verifies the ability of the election administrator to view voter requests and accept or reject them based on successful comparison of the voter's credentials that were supplied by the voter to those that are known in the system database. The test will verify the acceptance/ rejection process and the notification to the voter. It will verify that all voter identification transmitted to the voter is protected against unauthorized access.

Test Configuration:

The client connects to the [redacted] server via the Wyle LAN and internet connection using Internet Explorer. The port for access as a voting administrator is [redacted]

Devices Utilized: Client located at Wyle: Dell Desktop - OptiPlex 780, 2.0GB RAM, Windows 7 Professional, Internet Explorer 8.0.7600.16385, Wyle domain ai-engsvcs.com to internet connection. Server: make and model unknown, provided by supplier at their site.

Step	Procedure	Notes
	Record date and time, hardware and software model and versions.	Client located at Wyle: server - make and model unknown
10000	Log in as an administrator with full privileges.	Logged in Wyleadmin/#20wyle11#.
20000	Record statistics on registration page (screen print), export log file and results file. Click on the "Voting" button if necessary to be sure voting has started.	Entered password and clicked on export logs. Exported results and clicked on the "voting button" which it accepted - at that point it cleared the password (voting was now stopped). Had to reenter the password and then started voting by clicking on that button.
30000	Select "Voters Requests" from the menu bar and search for voters in "pending" status. Note the voters with correctly matching information.	Verified.
40000	Return to voting administration screen and click on Automatic Accept.	Pop up message indicated 6 voters were accepted. The number of pending and accepted correctly changed in those boxes on the administration screen.
50000	Go to voters request screen and search on pending voters, only those with some mismatch should remain.	Only saw those with mismatch dates and the one with no date in the database - 4 voters total.
60000	Reject one mismatched voter -- that has a working email	Rejected voter 1208100573263 with email address david.jakobsen@wyle.com. It would not let me close the detail info box until saving it (the "send" button was NOT enabled). Upon saving, the pop up message "Voter request updated" was displayed. On returning to the pending list, he had been removed. Verified his name appeared on the "rejected" list and the information was correct.
70000	Change the email address in for one voter.	Changed voter [redacted] to [redacted] and saved and closed (Clicked on save and got the message confirming it was saved. Then clicked on close and got the message "changes you made require sending Information to the voter. Please send info and then close form." The SEND button

1

		was not enabled, but you can only exit by hitting the "cancel" button. Apparently when it "cancels" it does not update the Pending voter list because that list still had the old address. It was updated when edit was clicked again. Closed the detail box by clicking on "close". The new address now correctly appeared.
80000	Accept that same voter as a registered voter.	Changed his status to Accepted. The system enabled the "send" button and required saving and sending the information.
90000	For that same voter change the status to "rejected".	Searched on his Id number in accepted and found him. Clicked on edit and it brought up his "voter Request" detail info box with the "send" button enabled. Changed the status to rejected and it disabled the "send" button. Clicked on "save" and it acknowledged successful save. It allowed selecting close ok and did not require a send.
100000	Manual review and accept remaining voters.	Done.
105000	Click on the "sent mail" item in the menu bar and verify the accuracy of the sent mails.	Viewed the sent mail list and it appeared ok
110000	Search for accepted voters with today's date and record the list (screen print)	Done.
120000	View and screen print or print logs and reports. Collect pins created for all voters -- save emails and archive all information collected. Printed duplicate email report.	Done.
130000	End of test – record time and date	Completed test…

Test Case: Test Case 14 Normal Voting System C	
Test Objective:	**Test Configuration:**
One ballot will be delivered to the terminal and voted and cast on-line. 1. The system accurately delivers the content for that ballot to the voter 2. The system implements authentication prior to allowing the voter access to the ballot. 3. The system adequately logs the event of transferring the ballot information 4. The system records the voters choices accurately and securely 5. The system only records the vote after the voter has performed the action to "cast" it 6. The system protects the cast vote against any viewing or access by anyone until the day that the jurisdiction has authorized for the voting to be opened. 7. The browser does not allow access to sensitive data through storage in cookies or temporary files. 8. The voter is protected from inadvertently exposing sensitive information.	The client connects to the *****server via the Wyle LAN and internet connection using Internet Explorer. The port for access as a voting administrator is ******
Devices Utilized:	Client located at Wyle: Dell Desktop - OptiPlex 780, 2.0GB RAM, Windows 7 Professional, Internet Explorer 8.0.7600.16385, Wyle domain ai-engsvcs.com to internet connection. Server: make and model unknown, provided by supplier at their site.

Step	Procedure	Notes
0	Locate the PIN(s) provided by email / standard mail. For email user verify that the PIN is securely wrapped in a PDF lock and requires a key (vote rid) to open	1208100538567 pin 134502.
10000	Record start time and date, hardware models and serial numbers, software versions for system test. Record physical location of equipment (remote / local).	Client located at Wyle: Dell Desktop - OptiPlex 780, 2.0GB RAM, Windows 7 Professional, Internet Explorer 8.0.7600.16385, [redacted]server - make and model unknown.
20000	If necessary, log into the system as an administrator and search for "accepted" voters within the dates that "Registration Processing Test Case" was used to accept registration requests. (screen print of the list)	Step completed in previous testing. Using list registeredvVotersListforTest.xls.
30000	Login with a valid voter ID number and PIN.	[redacted]
40000	Click on the "Accept" button to accept the voter oath.	Selected "I agree" Selected "No, I do not want audio ballot".
50000	Click on the "help" button in the top right hand corner.	Selected Help screen.
60000	Return to the contest screen and vote for one (or as many as specified for the contest) continue through all the contests and vote according to the instructions for each contest.	First contest Voted for Neil R. ELLIS. Second contest voted for first 6 candidates. Third contest for first 2 candidates. Selected Review Ballot.
70000	From the review screen go back and change one	Selected go back and original candidate is

	vote. Record the final review screen(s) content and "cast" the ballot.	missing. Must revote complete ballot.
80000	Try to use the browser "back" button to vote again. Then attempt to vote a second ballot with the same id and PIN numbers.	Selecting back after voting returns you to the login selection page.
90000	Log in with a different PIN and voter ID. Go to the first contest and over vote (vote for more than instructed). If possible, leave the over vote and move to the next contest	[redacted] Over-voted first contest.
100000	Under vote a contest, leave it under voted and proceed to the next contest. Vote remaining contests with valid vote	Under-voted second contest.
110000	Record the votes as they appear on the review screen and verify they are as voted. Then cast the ballot	Reviewed and cast under and over vote ballot.
120000	Log in as the same voter	[redacted]
130000	Attempt to print or cast a second ballot	User already voted.
140000	Log out as this user	Selecting Continue will log user out.
160000	Log in as administrator. View and dump all reports. Verify that all events for all users that voted are logged.	Upon checking the log, no information was logged regarding this activity.
170000	Dump all logs and collect screen prints, etc.	All files recorded.
180000	End of test – record time and date	

Test Case:	Test Case 01 Host Server Administration System D
Test Objective:	**Test Configuration:**
This test case verifies the roles of system administrator and the ability to maintain user roles, passwords, logs and other voting system administrative functions.	Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link via (Link TBS) and uses the voter page accessed at URL
Devices Utilized:	Client: Dell Optiplex 780, Server: Vendor supplied, make and model TBS.

Step	Procedure	
0	Record time and date of test, record hardware models, serial numbers and software versions	
10000	Log in with the administrative account provided by the vendor. (this is an "administrator" role with full privileges)	Demo /Demo
20000	Dump system Logs. Then view the logs and save. Attempt to change and/or reset the log. Verify they cannot be altered.	Logs can be exported and imported into excel.
30000	View user list and attempt to add user, assign role, delete user, and re-assign roles to existing user.	Admin can modify all user information.
40000	Log in as voting system administrator (full privileges) role, create a new user and verify default role is the least privileged. Note information entered for this user and adds one more user for each administrator role.	Created "Wylelabs" with the password "wylelab".
50000	Perform a series of log-ins, one for each role, and attempt to exercise privileges not allowed for that role, verify each role can only view/modify the items there are authorized..	Was unable to log in as "Wylelabs".
60000	Log out and log in as super user and attempt to view storage in server such that unencrypted passwords, etc are detected??/	Passwords are encrypted.
70000	Reset password for existing user, perform password administration such as setting minimum required password length, type of characters, capitals, etc. per NIST 800-63. (user name cannot be part of password)	Changed password for 33W44 to "wyle".
90000	Verify password histories are maintained and that user cannot reuse passwords according to the password length requirement. Attempt to use a password containing the user name and verify that it is rejected.	Does not appear to be a limit on historical passwords.
100000	Verify that passwords automatically expire at a specified length of time. Need to set expiration date on next day and then verify after that date.	Passwords do not expire.
110000	As administrator (super user), record default settings for log control (rqmt 5.6.1.1) verify logs are append only and read-only for authorized roles ____ verify it is not possible to alter the log..	Logs are exported into an excel format.
120000	Attempt to create log failure and verify that log	Log in failures do not appear in the logs.

	events, such as errors or rotation are recorded. Attempt to clear log and verify that action is logged. Then export the log for storage (5.6.1.8)	
130000	View log and verify it is in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format and that it has no data violating voter privacy. Search log and exercise any analysis tools	Logs are in an excel format.
140000	Attempt to monitor real-time reporting of system events. Log in as super admin and view any logs / reports that may provide real-time monitoring of the system activity - especially of logged on users (Check for OS capability external to voting system.)	N/A
150000	Attempt to log in with an invalid administrator user ID Re-attempt until sufficient attempts cause the terminal to be locked out.	There does not appear to be a limit on invalid logins.
155000	Log in, change the number of attempts threshold for locking out the terminal and then repeat the process.	This function is not configurable using the admin screen.
160000	Log in as a valid administrator and don't do anything - allow the system to time out. Then log back in and verity it requires reentry of the password.	Logged in to author tools. NO ADMIN TIMEOUT.
165000	Export the voting system log to external device for archiving.	Logs export into excel format.
170000	Record date and time of test end, collect logs and all output records. Verify events are recorded with proper order and times verify entry includes system id, timestamp, event id, success/fail, and if applicable, user id and jurisdiction id	Logs recorded.
180000	End of test – record time and date	

Result Test Sheet

Test Case:	03 Crypto Test Sheet System D
Test Objective:	**Test Configuration:**
This test case verifies that the cryptographic functionality implemented by the system meets/is NIST-approved and/or FIPS 140-2 compliant.	Full test System setup, fully functional and under normal operating conditions. Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link.
Devices Utilized:	Client: Dell optima Desktop at Wyle Laboratories. Server: make and model unknown

Step	Procedure	Notes
1000	Record time and date of test, record hardware models, serial numbers and software versions.	6/1/2011 Win 7, IE 8, System VM running CentOS 5.4 URL: [redacted]
2000	Review System documentation for cryptographic algorithms and protocols implemented by the system and record them. **Note:** If keys are put into the voting system manually, read step 7 before continuing.	System documentation reviewed, listed: HTTPS AES-256-bit (2048-bit keyed) SSL - Ballot Transmission Salted MD5, SHA256 Hashes (256-bit) - Credential Storage PKCS#7, 2048-bit RSA (3DES symmetric ephemeral ciphers) - Ballot Encryption
3000	Check to ensure that algorithms and protocols used have gone through the Cryptographic Algorithm Validation Program or FIPS 140-2 approved. If not, that the appropriate waiver has been applied for from NIST. Additionally, check tables in SP 800-57 and ensure algorithms are at 112 bit level.	Check protocols used on client browser side. Connection: Local intranet / Not protected Cert: Non-Registered, version 1, Sha1RSA, RSA 1024 bit
4000	Log into system with administrative privileges. Manually verify or pull using script the permissions on appropriate cryptographic applications and files.	Due to issues with VM this step not performed.
4100	Verify that permissions are restricted and not writable by voting system application. Record and document all observations.	Not performed, see step 4.
5000	Pull the hash values for the cryptographic keys from the system.	Not performed, see step 4.
6000	Check hash lengths to ensure the crypto modules are using a correct strength algorithm.	Not performed, see step 4.
7000	If keys are input manually into system, vary the key by only changing one value slightly. (e.g. Key starts with a "T" use a "t" on second entry.) Follow any system instructions to load key before starting to pull logs and data.	Documentation supports this process however, due to issues with VM this could not be tested and verified.
7100	If system only holds and allows one key/hash; pull hash; then re-log into system reenter key following system instructions; then re-pull hash.	Documentation did not provide any information on this process.
7200	If the system allows more than one hash; then follow systems instruction for a specific key set then re-enter same key set changing the key as described in main step; then pull hashes.	Documentation did not provide any information on this process.

I

Result Test Sheet

7300	Compare the hashes with the slight change; there should be significant change in hash value. Record observations.	Due to issues with VM this step not performed.
8000	Review voting system software source code. Verify that crypto modules are being called in the correct manner to meet NIST requirements and 112 bit encryption. **Note:** The application doing the encryption maybe FIPS 140-2 compliant but, the voting application (i.e. Java code call to crypto module.) could use wrong method to encrypt at proper strength.	Not performed, code not provided.
9000	Key Management, Perform this step if cryptographic keys are generated internally. Review voting system documentation to see what type encryption methods is deployed.	Reviewed documentation see step 2. Additional information; key lengths for: Ballot Transmission - HTTPS AES-256-bit (2048-bit keyed) SSL Credential Storage - Salted MD5, SHA256 Hashes (256-bit) Ballot Encryption - PKCS#7, 2048-bit RSA (3DES symmetric ephemeral ciphers)
9100	Review source code and take note to ensure that methods used comply with FIPS 140-2. This should be done by referring to annex A, C or D of 140-2. Record all observations and discrepancies.	Not performed, code not provided.
9200	Pull file permissions of those executable and library files in the system. Ensure they have restricted access and are properly controlled. Record all observations.	Due to issues with VM this could not be tested.
10000	Perform key entry procedures following voting system documentation. Verify that input and output are NIST compliant.	Due to issues with VM and lack of detail in the documentation this could not be tested and verified.
10100	If automated method is used input and output from system must be encrypted. Record observations.	The documentation states that '[redacted] This process was not clearly defined and was not tested.
10200	If a manual method is used input and output from system maybe plaintext. Record observations. **Note:** Transportation and any other processes dealing with the input and output data should reviewed to verify proper security measures are being applied.	Not performed, see step 7for explanation.
11000	Perform Key zeroization procedures following voting system documentation. Verify that the key no longer exist on the system after completion of procedure. Record all observations.	Not performed, see step 7for explanation.
12000	Perform rekeying procedures following voting system documentation. Verify the system performs as documented and is compliant. Record all observations.	Due to issues with VM this step not performed.
13000	During Operational tests, ensure that the voting system supports rekeying during communications.	Verified protocols being used.

Result Test Sheet

	This should be done by verifying protocols used and/or sniffing network traffic and examining the packets. **Note:** System documentation should but may not state the amount or limit of data encrypted with the same key. The key could change on a daily basis, when a pre-set volume of data has been transmitted or a given period of time has elapsed. Most systems, implement rekeying by forcing a new key exchange, typically through a separate protocol like Internet key exchange (IKE). (e.g. Wi-Fi Protected Access (WPA), does this by frequently replacing session keys through the Temporal Key Integrity Protocol (TKIP))	
14000	During Operational tests, ensure that the voting system uses NIST or FIPS approved protocols for communications. Record all observations. **Note:** This should be done by sniffing network traffic (i.e. Wireshark) and examining the packets.	Verified protocols being used from client side browser.
15000	End of test – record time and date	6/1/2011

Additional Notes:

- Only IE browser tested.
- Side issues – network configuration of the VM caused issues, as well as initial VM settings/options. These had to be adjusted to run on Lab system. Unexplained issues would happen after some of the adjustments were made to get the system up and running.

Test Case:	Test Case 04 Normal Ballot Delivery System D
Test Objective:	**Test Configuration:**
One ballot will be delivered to the terminal and displayed and/or printed to exercise the normal processing path for delivery of ballot. The test will verify that: 1. The system delivers that ballot to the voter 2. The system implements authentication prior to allowing the voter access to the ballot. 3. The system adequately logs the event of transferring the ballot. 4. The ballot that is delivered is identical to the ballot that was provided by the Election Management System.	Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link via voter page at URL Administrative access required via URL (TBS) to monitor and collect test results.
Devices Utilized:	Client: Dell Optiplex 780, Server: Vendor supplied, make and model TBS.

Step	Procedure	Notes
0	Record start time and date, hardware models and serial numbers, software versions for system test. Record physical location of equipment (remote / local)	
10000	Log on as a voter to the system (a non-administrator account on this terminal) .(during the following steps, record each action and response by the system so that at the end, we can verify that all significant events were logged)	Successful login as non-admin.
30000	Perform authentication necessary to access ballot distribution pages.	Ballot displayed.
60000	Mark the ballot and save the marked ballot.	Ballot marked.
80000	Review the ballot and verify the choices are as intended. , then change a choice and print the marked ballot.	Ballot verified.
90000	Sign out or log off as this voter.	Log off successful.
100000	If a browser is used, attempt to view all temporary files to verify no voting information is left on the voting device.	All screens are cached. Files have been saved.
110000	Log in as the same voter	Ballot already submitted.
120000	Attempt to print or cast a second ballot	Access denied due to already voting.
140000	Log off -- and log in as administrator. View and dump logs. Verify that all events for all users that voted are logged. If on the same terminal as voter, then search for files/temporary storage that contains any voter information.	No user log exists.
150000	Examine and Dump all logs and collect screen prints, etc. On both the server and the client.	Logs do not contain all information.
160000	End of test –record time and date	

Result Test Sheet

Test Case:	05 Discovery Penetration System D
Test Objective:	**Test Configuration:**
This test seeks out vulnerabilities in the voting system, verifies the system's resistance to any remote unauthorized entity. That the system provides no access, information or services to unauthorized entities and is configured to minimize ports and information disclosure about the system.	Full System with host, remote terminal and communication devices. Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link. Full test System setup, fully functional and under normal operating conditions.
Devices Utilized:	BackTrack OS with Nessus Laptop

Step	Procedure	Notes
1000	Record time and date of test start, model and serial number of hardware, software with version numbers.	12:35 6/3/2011 HP Pavilion dv6 laptop running Backtrack 4 R2 as OS with Nessus installed. Nessus version : 4.4.1 feed ver. : 201105041534 Scanner MAC : 00:e0:6a:3c:fc:68 Scanner IP : 10.10.13.124 Metasploit v3.7.0 svn r12540
2000	Record IP and URL addresses to be tested.	10.10.13.10 (Need URL)
3000	Scan IP and URL ranges with Nmap, unobtrusive.	Port 22, 80 and 443 open. Linux 2.6.x (100%) VM running file: [redacted]
4000	Scan from inside target/s netmask range. Save results to file.	N/A
5000	Scan target/s from outside interfaces. Save results to file.	See step 3.
6000	If needed and applicable, scan IP and URL ranges with Nmap, aggressive. Save results to file.	Not required.
7000	Scan IP and URL ranges with Nessus, unleveraged "no credentials". Save scan result, in file name indicate unleveraged.	Scanned with Nessus polices (see files); External- [redacted]
8000	Scan from inside target/s netmask range. Save results, indicating "inside" (e.g. system_noC_in.xml)	N/A
9000	If applicable, scan target/s from outside interfaces. Save results, indicating "outside" (e.g. system_noC_out.xml)	See step 7.
10000	Scan IP and URL ranges with Nessus, leveraged "with credentials". Save scan result, in file name indicating leveraged. Note: This type scan is usually done from "inside" only.	Not done, with time restrictions, 8 medium vulnerabilities found unleveraged and remote access by root successful decided vendor had enough to address major problems.
11000	Probe target URL for further information. (i.e. URL manipulation, input/form field manipulation, SQL injection, etc.) Record all observations and displayed information.	Simple SQL injection not effective.
12000	Review all scan results and recorded information.	3 open ports, 8 medium and 42 low vulnerabilities, Linux Kernel 2.6 on CentOS 5, VM machine (00:0c:29:9d:38:86 : VMware, Inc.)

Result Test Sheet

13000	Annotate record and organize all pertinent information (e.g. Ports, Protocols, Services, versioning, etc.) from the results for second phase of Pen test.	Done.
14000	From review of pertinent information, setup/develop and additional discovery scans/tests as needed.	Not needed.
15000	Perform any additional discovery scans or tests as needed. Save and record these results.	N/A
16000	Review all results, notes and finalize exploratory tests for second phase of testing.	With time restrictions went with port exploits as primary attack method. Also, attempt login with application credentials. **NOTE:** Login with Root successful, deposited Hacker.txt in root directory.
17000	End of test – record time and date	15:31 6/3/2011

Additional Notes:

- Was able to login with Root remotely. Opened command shell from 10.10.13.124:56693 to 10.10.13.10:22 at 14:25 6/3/2011. Root should never have remote access.
- Metasploit port attacks were used (examples; webdav_upload_upload_asp, hagent_untrusted_hsdata, RealServer describe Buffer Overflow).
- None of attempted exploits succeeded. More detailed attempts against the OS or more detailed SQL attempts maybe successful but, require more time than was currently allocated.

Test Case:	Test Case 01 Host Server Administration System E
Test Objective:	**Test Configuration:**
This test case verifies the roles of system administrator and the ability to maintain user roles, passwords, logs and other voting system administrative functions.	Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link via (Link TBS) and uses the voter page accessed at URL
Devices Utilized:	Client: Dell Optiplex 780, Server: Vendor supplied, make and model TBS.

Step	Procedure	Notes
0	Record time and date of test, record hardware models, serial numbers and software versions	
10000	Log in with the administrative account provided by the vendor. (this is an "administrator" role with full privileges)	User Name “*******S” Psw “[redacted]”. Login successful.
20000	Dump system Logs. Then view the logs and save. Attempt to change and/or reset the log. Verify they cannot be altered.	Logs cannot be modified using administrator access. Member Login Log is the only log that is not exportable.
30000	View user list and attempt to add user, assign role, delete user, and re-assign roles to existing user.	Admin can modify and add all members.
40000	Log in as voting system administrator (full privileges) role, create a new user and verify default role is the least privileged. Note information entered for this user and add one more user for each administrator role.	Created user “WyleLabs” Psw “wylelab”. Note! The only way to validate the field requirements is to enter an invalid value. Role is defined by assigning the new user to a specific precinct.
50000	Perform a series of log-ins, one for each role, and attempt to exercise privileges not allowed for that role, verify each role can only view/modify the items there are authorized..	New Admin can only see specific precinct information. Admin at this level can only add admin's at the same level.
60000	Log out and log in as super user and attempt to view storage in server such that unencrypted passwords, etc. are detected	Login as User Name “*****OS” Psw “[redacted]”. Login successful.
70000	Reset password for existing user, perform password administration such as setting minimum required password length, type of characters, capitals, etc. per NIST 800-63. (user name cannot be part of password)	Modified password for admin sale_5713 pwd “wylelabs”. Password must be "6-20 bit characters or digits is allowed." Password field accepts special characters. NOTE! Password can match the user name!
90000	Verify password histories are maintained and that user cannot reuse passwords according to the password length requirement. Attempt to use a password containing the user name and verify that it is rejected.	NOTE! Password can match the user name! And there is nothing to stop reuse of old passwords.
100000	Verify that passwords automatically expire at a specified length of time. Need to set expiration date on next day and then verify after that date.	There does not appear to be a function for expiring passwords.

110000	As administrator (super user), record default settings for log control (rqmt 5.6.1.1) verify logs are append only and read-only for authorized roles ____ verify it is not possible to alter the log..	Login logs are appended and non-editable.
120000	Attempt to create log failure and verify that log events, such as errors or rotation are recorded. Attempt to clear log and verify that action is logged. Then export the log for storage (5.6.1.8)	System does not log login failures and the log is not exportable. It could not be determined how long the log information is retained.
130000	View log and verify it is in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format and that it has no data violating voter privacy. Search log and exercise any analysis tools	The logs that can be exported are in an .XLS format.
140000	Attempt to monitor real-time reporting of system events. Log in as super admin and view any logs / reports that may provide real-time monitoring of the system activity - especially of logged on users (Check for OS capability external to voting system.)	Login access is recorded via Ballot Events and Member login log. It could not be determined how long the log information is retained.
150000	Attempt to log in with an invalid administrator user ID Re-attempt until sufficient attempts cause the terminal to be locked out.	User Name "******OS" Psw "[redacted]". Login successful. It does not appear that there is a limit on the number of incorrect login attempts.
155000	Log in, change the number of attempts threshold for locking out the terminal and then repeat the process.	It does not appear that there is a limit on the number of incorrect login attempts.
160000	Log in as a valid administrator and don't do anything - allow the system to time out. Then log back in and verity it requires reentry of the password.	User Name "*****OS" Psw "[redacted]". Login successful 4/26/2011 2:17:18 PM System has not logged out. 4/26/2011 2:27:18 PM System never logs admin out.
165000	Export the voting system log to external device for archiving.	Members login log is not exportable.
170000	Record date and time of test end, collect logs and all output records. Verify events are recorded with proper order and times verify entry includes system id, timestamp, event id, success/fail, and if applicable, user id and jurisdiction id	All logs retained.
180000	End of test -- record time and date.	

Result Test Sheet

Test Case: 03 Crypto Test Sheet System E	
Test Objective:	**Test Configuration:**
This test case verifies that the cryptographic functionality implemented by the system meets/is NIST-approved and/or FIPS 140-2 compliant.	Full test System setup, fully functional and under normal operating conditions. Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link.
Devices Utilized:	Client: Dell optima Desktop at Wyle Laboratories. Server: make and model unknown

Step	Procedure	Notes
1000	Record time and date of test, record hardware models, serial numbers and software versions.	Win 7, IE 8 URL:
2000	Review System documentation for cryptographic algorithms and protocols implemented by the system and record them. Note: If keys are put into the voting system manually, read step 7 before continuing.	Documentation provided did not provide any additional information than what was gathered in step 3.
3000	Check to ensure that algorithms and protocols used have gone through the Cryptographic Algorithm Validation Program or FIPS 140-2 approved. If not, that the appropriate waiver has been applied for from NIST. Additionally, check tables in SP 800-57 and ensure algorithms are at 112 bit level.	Could only check protocols used on client browser side, due to not having access to the system. Connection: TLS 1.0 3DES 168 bit, RSA 2048 bit Cert: Issuer – Go Daddy, class 3, sign algorithm Sha1RSA, hash Sha1
4000	Log into system with administrative privileges. Manually verify or pull using script the permissions on appropriate cryptographic applications and files.	Could not perform. No administrative credentials provided. Only application admin credentials provided.
4100	Verify that permissions are restricted and not writable by voting system application. Record and document all observations.	Could not perform. No access to system other than client side browser connection.
5000	Pull the hash values for the cryptographic keys from the system.	Could not perform. No access to system.
6000	Check hash lengths to ensure the crypto modules are using a correct strength algorithm.	Not performed, see step 5.
7000	If keys are input manually into system, vary the key by only changing one value slightly. (e.g. Key starts with a "T" use a "t" on second entry.) Follow any system instructions to load key before starting to pull logs and data.	Documentation provided did not provide information on this process. No access to system other than application usage. This step Not performed.
7100	If system only holds and allows one key/hash; pull hash; then re-log into system reenter key following system instructions; then re-pull hash.	Documentation provided did not provide information on this process. No access to system other than application usage. This step Not performed.
7200	If the system allows more than one hash; then follow systems instruction for a specific key set then re-enter same key set changing the key as described in main step; then pull hashes.	Not performed, see step 7.
7300	Compare the hashes with the slight change; there	Not performed, see step 7.

Result Test Sheet

	should be significant change in hash value. Record observations.	
8000	Review voting system software source code. Verify that crypto modules are being called in the correct manner to meet NIST requirements and 112 bit encryption. **Note:** The application doing the encryption maybe FIPS 140-2 compliant but, the voting application (i.e. Java code call to crypto module.) could use wrong method to encrypt at proper strength.	Not performed, code not provided.
9000	Key Management, Perform this step if cryptographic keys are generated internally. Review voting system documentation to see what type encryption methods is deployed.	Unknown, system documentation provided did not provide information on this process. No access to system other than application usage. This step Not performed.
9100	Review source code and take note to ensure that methods used comply with FIPS 140-2. This should be done by referring to annex A, C or D of 140-2. Record all observations and discrepancies.	Not performed, code not provided.
9200	Pull file permissions of those executable and library files in the system. Ensure they have restricted access and are properly controlled. Record all observations.	No access to system other than application usage. This step Not performed.
10000	Perform key entry procedures following voting system documentation. Verify that input and output are NIST compliant.	No access to system other than application usage. This step Not performed.
10100	If automated method is used input and output from system must be encrypted. Record observations.	Unknown, system documentation provided did not provide information on this process. No access to system other than application usage. This step Not performed.
10200	If a manual method is used input and output from system maybe plaintext. Record observations. **Note:** Transportation and any other processes dealing with the input and output data should reviewed to verify proper security measures are being applied.	Unknown, system documentation provided did not provide information on this process. No access to system other than application usage. This step Not performed.
11000	Perform Key zeroization procedures following voting system documentation. Verify that the key no longer exist on the system after completion of procedure. Record all observations.	Not performed, see step 10.
12000	Perform rekeying procedures following voting system documentation. Verify the system performs as documented and is compliant. Record all observations.	Not performed, see step 10.
13000	During Operational tests, ensure that the voting system supports rekeying during communications. This should be done by verifying protocols used and/or sniffing network traffic and examining the packets. **Note:** System documentation should but may not state the amount or limit of data encrypted with the same key.	Verified protocols being used but, did not monitor traffic due to the whole system not being in Wyle testing lab.

Result Test Sheet

	The key could change on a daily basis, when a pre-set volume of data has been transmitted or a given period of time has elapsed. Most systems, implement rekeying by forcing a new key exchange, typically through a separate protocol like Internet key exchange (IKE). (e.g. Wi-Fi Protected Access (WPA), does this by frequently replacing session keys through the Temporal Key Integrity Protocol (TKIP))	
14000	During Operational tests, ensure that the voting system uses NIST or FIPS approved protocols for communications. Record all observations. Note: This should be done by sniffing network traffic (i.e. Wireshark) and examining the packets.	Verified protocols being used from client side browser.
15000	End of test – record time and date	6/1/2011

Additional Notes:

- Only IE browser tested.
- Side issues – Web browsers listed in documentation have browser versions with known security issues.

Test Case:	Test Case 04 Normal Ballot Delivery System E
Test Objective:	**Test Configuration:**
One ballot will be delivered to the terminal and displayed and/or printed to exercise the normal processing path for delivery of ballot. The test will verify that: 1. The system delivers that ballot to the voter 2. The system implements authentication prior to allowing the voter access to the ballot. 3. The system adequately logs the event of transferring the ballot. 4. The ballot that is delivered is identical to the ballot that was provided by the Election Management System.	Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link via voter page at URL Administrative access required via URL (TBS) to monitor and collect test results.
Devices Utilized:	Client: Dell Optiplex 780, Server: Vendor supplied, make and model TBS.

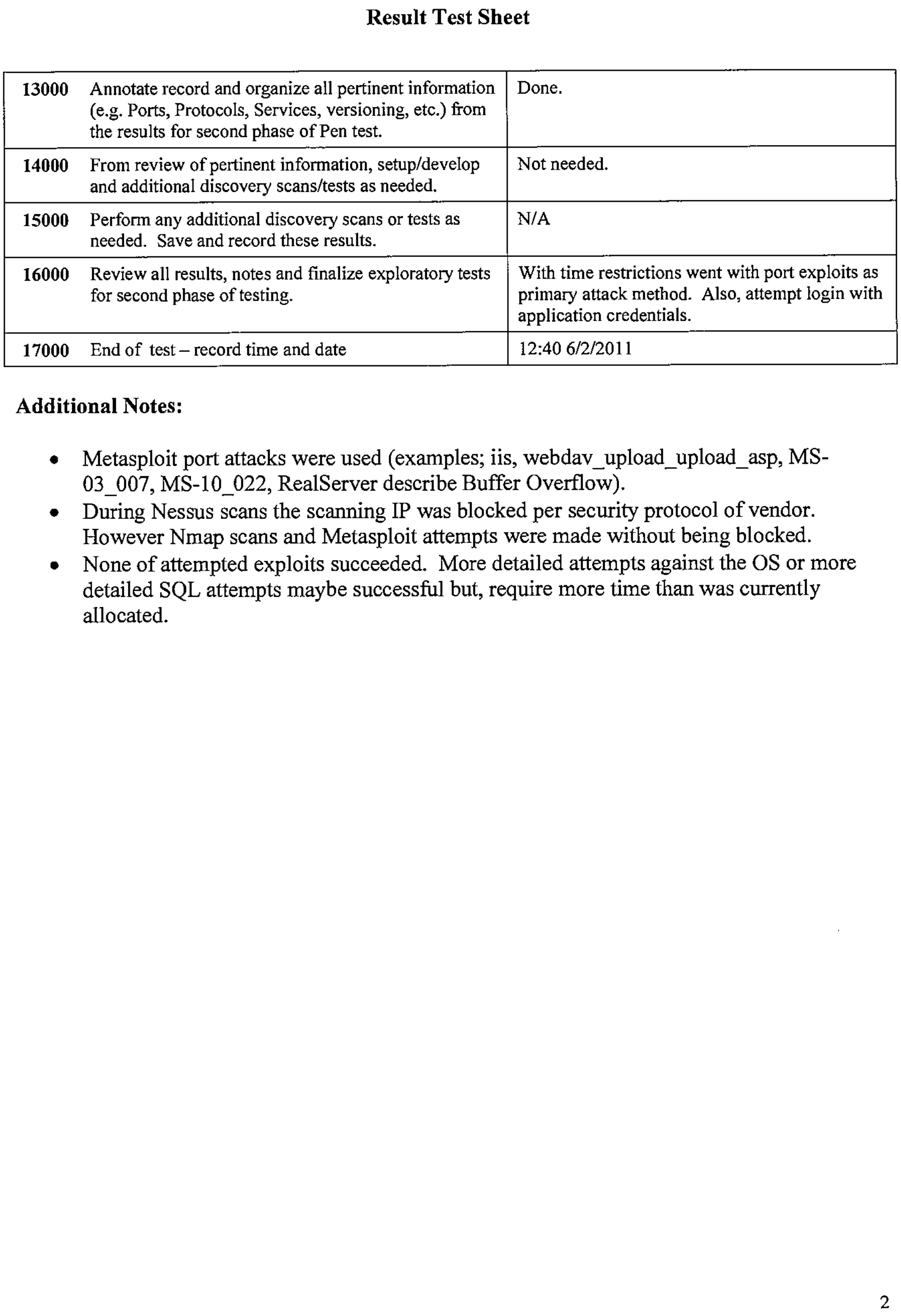
Step	Procedure	Notes
0	Record start time and date, hardware models and serial numbers, software versions for system test. Record physical location of equipment (remote / local)	
10000	Log on as a voter to the system (a non-administrator account on this terminal)... (during the following steps, record each action and response by the system so that at the end, we can verify that all significant events were logged)	Login with *PIN: NIPVYVBGINMW7I8*
30000	Perform authentication necessary to access ballot distribution pages.	All information to validate is in unencrypted email.
40000	Log in and Print the blank ballot	Blank ballot saved.
50000	Log in and download another ballot.	Blank ballot saved
60000	Mark the ballot and save the marked ballot.	Marked ballot saved.
80000	Review the ballot and verify the choices are as intended, then change a choice and print the marked ballot.	Validated ballot.
90000	Sign out or log off as this voter.	Browsers closed after finished.
100000	If a browser is used, attempt to view all temporary files to verify no voting information is left on the voting device.	Browsers closed after finished.
105000	Review the printed ballot and saved ballot and verify that the ballot is marked so that multiple copies cannot be submitted.	Each ballot has an identification number.

110000	Log in as the same voter	Login with pin: NIPVYVBGINMW7I8.
120000	Attempt to print or cast a second ballot	A voter can vote as many times as they want. A new number is on each ballot.
140000	Log off -- and log in as administrator. View and dump logs. Verify that all events for all users that voted are logged. If on the same terminal as voter, then search for files/temporary storage that contains any voter information.	Ballot log exported.
150000	Examine and Dump all logs and collect screen prints, etc. On both the server and the client. Record end time	Ballot log exported.

Result Test Sheet

Test Case: 05 Discovery Penetration System E	
Test Objective:	**Test Configuration:**
This test seeks out vulnerabilities in the voting system, verifies the system's resistance to any remote unauthorized entity. That the system provides no access, information or services to unauthorized entities and is configured to minimize ports and information disclosure about the system.	Full System with host, remote terminal and communication devices. Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link. Full test System setup, fully functional and under normal operating conditions.
Devices Utilized:	BackTrack OS with Nessus Laptop

Step	Procedure	Notes
1000	Record time and date of test start, model and serial number of hardware, software with version numbers.	09:26 6/2/2011 HP Pavilion dv6 laptop running Backtrack 4 R2 as OS with Nessus installed. Nessus version : 4.4.1 feed ver. : 201105041534 Scanner MAC : 00:0d:ab:ef:a9:2e Scanner IP : 10.10.13.124 Metasploit v3.7.0 svn r12540
2000	Record IP and URL addresses to be tested.	[redacted]
3000	Scan IP and URL ranges with Nmap, unobtrusive.	Port 443 open. Server 2003 (87%) file: kon.xml
4000	Scan from inside target/s netmask range. Save results to file.	N/A
5000	Scan target/s from outside interfaces. Save results to file.	See step 3.
6000	If needed and applicable, scan IP and URL ranges with Nmap, aggressive. Save results to file.	Not required.
7000	Scan IP and URL ranges with Nessus, unleveraged "no credentials". Save scan result, in file name indicate unleveraged.	Scanned with Nessus polices (see files); Web Apps- [redacted] External-[redacted] During scans IP was blocked.
8000	Scan from inside target/s netmask range. Save results, indicating "inside" (e.g. system_noC_in.xml)	N/A
9000	If applicable, scan target/s from outside interfaces. Save results, indicating "outside" (e.g. system_noC_out.xml)	See step 7.
10000	Scan IP and URL ranges with Nessus, leveraged "with credentials". Save scan result, in file name indicating leveraged. Note: This type scan is usually done from "inside" only.	Not done, no credentials were provided.
11000	Probe target URL for further information. (i.e. URL manipulation, input/form field manipulation, SQL injection, etc.) Record all observations and displayed information.	Simple SQL injection not effective.
12000	Review all scan results and recorded information.	1 open ports, 23 low vulnerabilities, Windows Server 2003



Result Test Sheet

13000	Annotate record and organize all pertinent information (e.g. Ports, Protocols, Services, versioning, etc.) from the results for second phase of Pen test.	Done.
14000	From review of pertinent information, setup/develop and additional discovery scans/tests as needed.	Not needed.
15000	Perform any additional discovery scans or tests as needed. Save and record these results.	N/A
16000	Review all results, notes and finalize exploratory tests for second phase of testing.	With time restrictions went with port exploits as primary attack method. Also, attempt login with application credentials.
17000	End of test – record time and date	12:40 6/2/2011

Additional Notes:

- Metasploit port attacks were used (examples; iis, webdav_upload_upload_asp, MS-03_007, MS-10_022, RealServer describe Buffer Overflow).
- During Nessus scans the scanning IP was blocked per security protocol of vendor. However Nmap scans and Metasploit attempts were made without being blocked.
- None of attempted exploits succeeded. More detailed attempts against the OS or more detailed SQL attempts maybe successful but, require more time than was currently allocated.

Test Case:	Test Case 12 Voter Registration Request System E

Test Objective:	**Test Configuration:**
This test case verifies that a voter can securely register to vote on-line. The test includes authentication that the voter is the voter that he/she claims to be and that the request is queued for processing by an election administrator	The client connects to the [redacted] server via the Wyle LAN and internet connection using Internet Explorer. The port for access as a voting administrator is [redacted] and for access to register as a voter is [redacted].

Devices Utilized:	Client located at Wyle: Dell Desktop - OptiPlex 780, 2.0GB RAM, Windows 7 Professional, Internet Explorer 8.0.7600.16385, Wyle domain ai-engsvcs.com to internet connection. Server: make and model unknown, provided by supplier at their site.

Step	Procedure	
0	Record date and time, equipment with model numbers, server software versions.	
10000	Log into the administrator screen, record statistics on screen (take a screen print) and Export UOCAVA list.	User Name ******OS Psw [redacted]. Login successful Exported [redacted]
20000	Go to the voter registration screen -- (https://vote4newjersey.us/BallotRequest/Register.aspx) and using the voter credentials log in with the correct name, voter ID	[redacted]
30000	Complete the registration screen by providing a valid email (yours) that you can access and a secret question with answer and the correct birth year for this voter. Submit that form. And click finish on the review screen -- close the browser.	[redacted]
40000	Repeat the registration process with the same voter on each screen	Registration completed - email saved.
50000	Select a different voter from the UOCAVA list.	[redacted]
60000	Using this voter, enter the ID, voter name correctly but enter other incorrect information.	Voter was unable to register. First time due to birthdate not being correct. Re-ran with correct information for name and birthdate. When two people have identical information the system should show both options. I was unable to test this since none of the voters in the supplied list met this requirement.
80000	From the UOCAVA lists, logon and enter requests for 8 more voters. Enter valid requests with matching information on at least 5 and incorrect dates on 3. Use a variety of email addresses - one of them with only one voter associated.	a: [redacted] b: [redacted] c: d: f: g: h:
90000	Export the logs and reports.	Logs recorded.
100000	End of test -- record time and date	Note! Pressing the back button on the browser will allow you to see information from a previous applicant.

Test Case:	Test Case 13 Registration Processing System E

Test Objective:	**Test Configuration:**
This test case verifies the ability of the election administrator to view voter requests and accept or reject them based on successful comparison of the voter's credentials that were supplied by the voter to those that are known in the system database. The test will verify the acceptance/ rejection process and the notification to the voter. It will verify that all voter identification transmitted to the voter is protected against unauthorized access.	The client connects to the [redacted] server via the Wyle LAN and internet connection using Internet Explorer. The port for access as a voting administrator is C and for access to register as a voter is https://[redacted]

Devices Utilized:	Client located at Wyle: Dell Desktop - OptiPlex 780, 2.0GB RAM, Windows 7 Professional, Internet Explorer 8.0.7600.16385, Wyle domain ai-engsvcs.com to internet connection

Step	Procedure	Notes
0	Record date and time, hardware and software model and versions.	
10000	Log in as an administrator with full privileges.	User Name is "Wyle2011", password is "Wyle2011". Logged in as precinct admin.
20000	Record statistics on registration page (screen print), export log file and results file, Click on the "Voting" button if necessary to be sure voting has started.	Request ballots image saved.
30000	Select "Ballot Requests" from the menu bar and search for voters in "NEW" status. Note the voters with correctly matching information.	Done.
50000	Reject one mismatched voter -- that has a working email address	Rejected [redacted] Email received [redacted] has invalid information.
60000	Manual review and accept remaining voters.	Changed everyone's precinct from [redacted] to [redacted]. Since [redacted] was not loaded.
70000	Search for accepted voters with today's date and record the list (screen print)	List saved.
80000	View and screen print or print logs and reports. Collect pins created for all voters -- save emails and archive all information collected. Printed duplicate emailed report.	Emails saved.
90000	End of test -- record time and date.	

ATTACHMENT C

STATISTICAL ANALYSIS OF UOCAVA EVSW’S

Note: This Attachment is landscape orientation and requires 11x17 page size.

UOCAVA	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements		System A	System B	System C	System D	System E	Results								
Req. No.	Functional Requirements Matrix	Wyle Comment														
Section 5	**Security**															
5.1	**Access Control**							29	21	10	15		41.67%	17.50%	15.83%	25.00%
	This section states requirements for the identification of authorized system users, processes and devices and the authentication or verification of those identities as a prerequisite to granting access to system processes and data. It also includes requirements to limit and control access to critical system components to protect system and data integrity, availability, confidentiality, and accountability. This section applies to all entities attempting to physically enter voting system facilities or to request services or data from the voting system.							Pass	Fail	Not Tested	N/A		Pass	Fail	Not Tested	N/A
5.1.1	**Separation of Duties**							7	0	3	5		47%	0%	20%	33%
5.1.1.1	The voting system SHALL allow the definition of personnel roles with segregated duties and responsibilities on critical processes to prevent a single person from compromising the integrity of the system.	Some system's not tested due to not have lab access to hardware for validation.	Not Tested	Not Tested	Pass	Pass	Pass	3	0	2	0		60%	0%	40%	0%
5.1.1.2	The voting system SHALL ensure that only authorized roles, groups, or individuals have access to election data.	Some system's not tested due to not have lab access to hardware for validation.	Not Tested	Pass	Pass	Pass	Pass	4	0	1	0		80%	0%	20%	0%
5.1.1.3	The voting system SHALL require at least two persons from a predefined group for validating the election configuration information, accessing the cast vote records, and starting the tabulation process.	Current web based system do not do tabulation so this requirement was not applicable to our testing. The majority of election configuration is done independent of the Web application and is therefore not a critical function of our testing.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.1.2	**Voting System Access**							22	21	7	10		37%	35%	12%	17%
	The voting system SHALL provide access control mechanisms designed to permit authorized access and to prevent unauthorized access to the system.		Pass	Pass	Pass	Pass	Pass	5	0	0	0		100%	0%	0%	0%
5.1.2.1	The voting system SHALL identify and authenticate each person, to whom access is granted, and the specific functions and data to which each person holds authorized access.	Some system's not tested due to not have lab access to hardware for validation.	Not Tested	Pass	Pass	Pass	Pass	4	0	1	0		80%	0%	20%	0%
5.1.2.2	The voting system SHALL allow the administrator group or role to configure permissions and functionality for each identity, group or role to include account and group/role creation, modification, and deletion.	Some system's not tested due to not have lab access to hardware for validation.	Not Tested	Not Tested	Pass	Pass	Pass	3	0	2	0		60%	0%	40%	0%

5.1.2.3	The voting system's default access control permissions SHALL implement the least privileged role or group needed.	Some system's not tested due to not have lab access to hardware for validation.	Not Tested	Not Tested	Fail	Pass	Fail	1	2	2	0		20%	40%	40%	0%
5.1.2.4	The voting system SHALL prevent a lower-privilege process from modifying a higher-privilege process.	Some system's not tested due to not have lab access to hardware for validation.	Not Tested	Not Tested	Pass	Pass	Pass	3	0	2	0		60%	0%	40%	0%
5.1.2.5	The voting system SHALL NOT require its execution as an operating system privileged account and SHALL NOT require the use of an operating system privileged account for its operation.	Wyle's testing was based on utilization of a web based application. Therefore this did not apply directly. But, it was noted that in some systems tested the OS administration privileges were required to configure election information.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.1.2.6	The voting system SHALL log the identification of all personnel accessing or attempting to access the voting system to the system event log.		Pass	Fail	Fail	Fail	Pass	2	3	0	0		40%	60%	0%	0%
5.1.2.7	The *(voting system)* SHALL provide tools for monitoring access to the system. These tools SHALL provide specific users real time display of persons accessing the system as well as reports from logs.		Pass	Fail	Fail	Fail	Fail	1	4	0	0		20%	80%	0%	0%
5.1.2.8	Vote capture device located at the remote voting location and the central server SHALL have the capability to restrict access to the voting system after a preset number of login failures.		Fail	Fail	Fail	Fail	Fail	0	5	0	0		0%	100%	0%	0%
5.1.2.9	The voting system SHALL log a notification when any account has been locked out.		Fail	Fail	Fail	Fail	Fail	0	5	0	0		0%	100%	0%	0%
5.1.2.10	Authenticated sessions on critical processes SHALL have an inactivity time-out control that will require personnel re-authentication when reached. This time-out SHALL be implemented for administration and monitor consoles on all voting system devices.		Fail	Fail	Pass	Pass	Pass	3	2	0	0		60%	40%	0%	0%
5.1.2.11	Authenticated sessions on critical processes SHALL have a screen-lock functionality that can be manually invoked.	This requirement was deemed N/A due to the web based application being accessible from a privately controlled PC and not a public Voting site.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.2	**Identification and Authentication**							26	24	9	6		40%	37%	14%	9%
5.2.1	**Authentication**							26	24	9	6		40%	37%	14%	9%
5.2.1.1	Authentication mechanisms supported by the voting system SHALL support authentication strength of at least 1/1,000,000.		Not Tested	Pass	Pass	Fail	Pass	3	1	1	0		60%	20%	20%	0%

5.2.1.2	The voting system SHALL authenticate users per the minimum authentication methods outlined below.	Some system's not tested due to not have lab access to hardware for validation.	Not Tested	Not Tested	Fail	Pass	Fail	1	2	2	0		20%	40%	40%	0%
5.2.1.3	The voting system SHALL provide multiple authentication methods to support multi-factor authentication.		Fail	Fail	Pass	Pass	Pass	3	2	0	0		60%	40%	0%	0%
5.2.1.4	When private or secret authentication data is stored by the voting system, it SHALL be protected to ensure that the confidentiality and integrity of the data are not violated.	Some system's not tested due to not have lab access to hardware for validation.	Not Tested	Pass	Pass	Pass	Pass	4	0	1	0		80%	0%	20%	0%
5.2.1.5	The voting system SHALL provide a mechanism to reset a Password if it is forgotten, in accordance with the system access/security policy.		Fail	Pass	Fail	Fail	Fail	1	4	0	0		20%	80%	0%	0%
5.2.1.6	The voting system SHALL allow the administrator group or role to specify Password strength for all accounts including minimum Password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters per NIST 800-63 Electronic Authentication Guideline Standards.	Some system's not tested due to not have lab access to hardware for validation.	Not Tested	Fail	Fail	Fail	Fail	0	4	1	0		0%	80%	20%	0%
5.2.1.7	The voting system SHALL enforce Password histories and allow the administrator to configure the history length when Passwords are stored by the system.	Some system's not tested due to not have lab access to hardware for validation.	Not Tested	Fail	Fail	Fail	Fail	0	4	1	0		0%	80%	20%	0%
5.2.1.8	The voting system SHALL ensure that the user name is not used in the Password.	Some system's not tested due to not have lab access to hardware for validation.	Not Tested	Not Tested	Pass	Fail	Fail	1	2	2	0		20%	40%	40%	0%
5.2.1.9	The voting system SHALL provide a means to automatically expire Passwords.	Some system's not tested due to not have lab access to hardware for validation.	Not Tested	Fail	Fail	Fail	Fail	0	4	1	0		0%	80%	20%	0%
5.2.1.10	The voting system servers and vote capture devices SHALL identify and authenticate one another using NIST - approved cryptographic authentication methods at the 112 bits of security.		Pass	Fail	Pass	Pass	Pass	4	1	0	0		80%	20%	0%	0%
5.2.1.11	Remote voting location site Virtual Private Network (VPN) connections (i.e., vote capture devices) to voting servers SHALL be authenticated using strong mutual cryptographic authentication at the 112 bits of security.	This requirement was deemed N/A due to the web based application being accessible from a privately controlled PC and not a public Voting site.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.2.1.12	Message authentication SHALL be used for applications to protect the integrity of the message content using a schema with 112 bits of security.		N/A	Pass	Pass	Pass	Pass	4	0	0	1		80%	0%	0%	20%
5.2.1.13	IPsec, SSL, or TLS and MAC mechanisms SHALL all be configured to be compliant with FIPS 140-2 using approved algorithm suites and protocols.		Pass	Pass	Pass	Pass	Pass	5	0	0	0		100%	0%	0%	0%
5.3	**Cryptography**							5	12	18	0		11%	27%	62%	0%
5.3.1	**General Cryptography Requirements**							4	11	0	0		27%	73%	0%	0%
5.3.1.1	All cryptographic functionality SHALL be implemented using NIST-approved cryptographic algorithms/schemas, or use published and credible cryptographic algorithms/schemas/protocols.		Fail	Fail	Fail	Fail	Fail	0	5	0	0		0%	100%	0%	0%
5.3.1.2	Cryptographic algorithms and schemas SHALL be implemented with a security strength equivalent to at least 112 bits of security to protect sensitive voting information and election records.		Fail	Fail	Fail	Fail	Fail	0	5	0	0		0%	100%	0%	0%

5.3.1.3	Cryptography used to protect information in-transit over public telecommunication networks SHALL use NIST-approved algorithms and cipher suites. In addition the implementations of these algorithms SHALL be NIST-approved (Cryptographic Algorithm Validation Program).		Pass	Fail	Pass	Pass	Pass	4	1	0	0		80%	20%	0%	0%
5.3.2	**Key Management**															
	The following requirements apply to voting systems that generate cryptographic keys internally.							1	2	37	0		0%	4%	96%	0%
5.3.2.1	Cryptographic keys generated by the voting system SHALL use a NIST-approved key generation method, or a published and credible key generation method.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Not Tested	Not Tested	0	0	5	0		0%	0%	100%	0%
5.3.2.2	Compromising the security of the key generation method (e.g., guessing the seed value to initialize the deterministic random number generator (RNG)) SHALL require as least as many operations as determining the value of the generated key.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Not Tested	Not Tested	0	0	5	0		0%	0%	100%	0%
5.3.2.3	If a seed key is entered during the key generation process, entry of the key SHALL meet the key entry requirements in 5.3.3.1. If intermediate key generation values are output from the cryptographic module, the values SHALL be output either in encrypted form or under split knowledge procedures.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Not Tested	Not Tested	0	0	5	0		0%	0%	100%	0%
5.3.2.4	Cryptographic keys used to protect information in-transit over public telecommunication networks SHALL use NIST-approved key generation methods. If the approved key generation method requires input from a random number generator, then an approved (FIPS 140-2) random number generator SHALL be used.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Not Tested	Not Tested	0	0	5	0		0%	0%	100%	0%
5.3.2.5	Random number generators used to generate cryptographic keys SHALL implement one or more health tests that provide assurance that the random number generator continues to operate as intended (e.g., the entropy source is not stuck).	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Fail	Not Tested	0	1	4	0		0%	20%	80%	0%
5.3.3	**Key Establishment**															
	Key establishment may be performed by automated methods (e.g., use of a public key algorithm), manual methods (use of a manually transported key loading device), or a combination of automated and manual methods.							1	1	18	0		5%	5%	90%	0%
5.3.3.1	Secret and private keys established using automated methods SHALL be entered into and output from a voting system in encrypted form. Secret and private keys established using manual methods may be entered into or output from a system in plaintext form.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Fail	Not Tested	0	1	4	0		0%	20%	80%	0%
5.3.4.1	Cryptographic keys stored within the voting system SHALL NOT be stored in plaintext. Keys stored outside the voting system SHALL be protected from disclosure or modification.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Pass	Not Tested	1	0	4	0		20%	0%	80%	0%
5.3.4.2	The voting system SHALL provide methods to zeroize all plaintext secret and private cryptographic keys within the system.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Not Tested	Not Tested	0	0	5	0		0%	0%	100%	0%
5.3.4.3	The voting system SHALL support the capability to reset cryptographic keys to new values.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Not Tested	Not Tested	0	0	5	0		0%	0%	100%	0%
5.4	**Voting System Integrity Management**															
	This section addresses the secure deployment and operation of the voting system, including the protection of removable media and protection against malicious software.							3	2	10	20		9%	6%	29%	57%
5.4.1	**Protecting the Integrity of the Voting System**							3	2	10	20		9%	6%	29%	57%

5.4.1.1	The integrity and authenticity of each individual cast vote SHALL be protected from any tampering or modification during transmission.	Current web based system do not do tabulation so this requirement was not applicable to our testing.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.4.1.2	The integrity and authenticity of each individual cast vote SHALL be preserved by means of a digital signature during storage.	Current web based system do not do tabulation so this requirement was not applicable to our testing.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.4.1.3	Cast vote data SHALL NOT be permanently stored on the vote capture device.		Pass	Pass	Pass	Fail	Fail	3	2	0	0		60%	40%	0%	0%
5.4.1.4	The integrity and authenticity of the electronic ballot box SHALL be protected by means of a digital signature.	Current web based system do not do tabulation so this requirement was not applicable to our testing.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.4.1.5	The voting system SHALL use malware detection software to protect against known malware that targets the operating system, services, and applications.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Not Tested	Not Tested	0	0	5	0		0%	0%	100%	0%
5.4.1.6	The voting system SHALL provide a mechanism for updating malware detection signatures.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Not Tested	Not Tested	0	0	5	0		0%	0%	100%	0%
5.4.1.7	The voting system SHALL provide the capability for kiosk workers to validate the software used on the vote capture devices as part of the daily initiation of kiosk operations.	Wyle deems this requirement N/A due to the Web Based architecture.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.5	**Communications Security**															
	This section provides requirements for communications security. These requirements address ensuring the integrity of transmitted information and protecting the voting system from external communications-based threats.							8	4	33	5		18%	8%	67%	8%
5.5.1	**Data Transmission Security**							3	3	19	5		10%	10%	63%	17%
5.5.1.1	Voting systems that transmit data over communications links SHALL provide integrity protection for data in transit through the generation of integrity data (digital signatures and/or message authentication codes) for outbound traffic and verification of the integrity data for inbound traffic.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Not Tested	Not Tested	0	0	5	0		0%	0%	100%	0%
5.5.1.2	Voting systems SHALL use at a minimum TLS 1.0, SSL 3.1 or equivalent protocols, including all updates to both protocols and implementations as of the date of the submission (e.g., RFC 5746 for TLS 1.0).	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Not Tested	Not Tested	0	0	5	0		0%	0%	100%	0%
5.5.1.3	Voting systems deploying VPNs SHALL configure them to only allow FIPS-compliant cryptographic algorithms and cipher suites.	Wyle deems this requirement N/A due to the Web Based architecture. VPN systems will only be utilized at a system server level.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.5.1.4	Each communicating device SHALL have a unique system identifier.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Pass	Fail	1	1	3	0		20%	20%	60%	0%
5.5.1.5	Each device SHALL mutually strongly authenticate using the system identifier before additional network data packets are processed.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Fail	Fail	0	2	3	0		0%	40%	60%	0%
5.5.1.6	Data transmission SHALL preserve the secrecy of voters’ ballot selections and SHALL prevent the violation of ballot secrecy and integrity.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Pass	Pass	2	0	3	0		40%	0%	60%	0%
5.5.2	**External Threats**							5	1	14	0		25%	5%	70%	0%
	Voting systems SHALL implement protections against external threats to which the system may be susceptible.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Pass	Not Tested	1	0	4	0		20%	0%	80%	0%

5.5.2.1	Voting system components SHALL have the ability to enable or disable physical network interfaces.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Pass	Not Tested	Pass	Pass	3	0	2	0		60%	0%	40%	0%
5.5.2.2	The number of active ports and associated network services and protocols SHALL be restricted to the minimum required for the voting system to function.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Pass	Not Tested	1	0	4	0		20%	0%	80%	0%
5.5.2.3	The voting system SHALL block all network connections that are not over a mutually authenticated channel.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Fail	Not Tested	0	1	4	0		0%	20%	80%	0%
5.6	**Logging**							38	36	1	10		29%	65%	1%	6%
5.6.1	**Log Management**							34	15	1	10		57%	25%	2%	17%
5.6.1.1	The voting system SHALL implement default settings for secure log management activities, including log generation, transmission, storage, analysis, and disposal.	Some system's not tested due to not having lab access to hardware for validation.	Not Tested	Pass	Pass	Pass	Pass	4	0	1	0		80%	0%	20%	0%
5.6.1.2	Logs SHALL only be accessible to authorized roles.		Pass	Pass	Pass	Pass	Pass	5	0	0	0		100%	0%	0%	0%
5.6.1.3	The voting system SHALL restrict log access to append-only for privileged logging processes and read-only for authorized roles.		Pass	Pass	Pass	Pass	Pass	5	0	0	0		100%	0%	0%	0%
5.6.1.4	The voting system SHALL log logging failures, log clearing, and log rotation.		Pass	Fail	Fail	Fail	Fail	1	4	0	0		20%	80%	0%	0%
5.6.1.5	The voting system SHALL store log data in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format.		Fail	Fail	Fail	Pass	Fail	1	4	0	0		20%	80%	0%	0%
5.6.1.6	The voting system SHALL ensure that each jurisdiction’s event logs and each component’s logs are separable from each other.	Some system's not tested due to not having lab access to hardware for validation.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.6.1.7	The voting system SHALL include an application or program to view, analyze, and search event logs.		Fail	Fail	Pass	Pass	Pass	3	2	0	0		60%	40%	0%	0%
5.6.1.8	All logs SHALL be preserved in a useable manner prior to voting system decommissioning.		Pass	Fail	Pass	Pass	Pass	4	1	0	0		80%	20%	0%	0%
5.6.1.9	Logs SHALL NOT contain any data that could violate the privacy of the voter’s identity.		Pass	Fail	Pass	Pass	Pass	4	1	0	0		80%	20%	0%	0%
5.6.1.10	Timekeeping mechanisms SHALL generate time and date values, including hours, minutes, and seconds.		Fail	Fail	Pass	Pass	Pass	3	2	0	0		60%	40%	0%	0%
5.6.1.11	The precision of the timekeeping mechanism SHALL be able to distinguish and properly order all log events.		Fail	Pass	Pass	Pass	Pass	4	1	0	0		80%	20%	0%	0%
5.6.1.12	Only the system administrator SHALL be permitted to set the system clock.	Some system's not tested due to not having lab access to hardware for validation.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.6.2	**Communication Logging**							1	9	0	0		10%	90%	0%	0%
5.6.2.1	All communications actions SHALL be logged.		Fail	Fail	Fail	Fail	Fail	0	5	0	0		0%	100%	0%	0%
5.6.2.2	The communications log SHALL contain at least the following entries:		Fail	Pass	Fail	Fail	Fail	1	4	0	0		20%	80%	0%	0%
5.6.3	**System Event Logging**															
	This section describes requirements for the voting system to perform event logging for system maintenance troubleshooting, recording the history of system activity, and detecting unauthorized or malicious activity. The operating system, and/or applications software may perform the actual event logging. There may be multiple logs in use for any system component.							3	12	0	0		20%	80%	0%	0%
	The voting system SHALL log the following data for each event: a. System ID;															

5.6.3.1	b. Unique event ID and/or type; c. Timestamp; d. Success or failure of event, if applicable;		Pass	Fail	Fail	Pass	Fail	2	3	0	0		40%	60%	0%	0%
5.6.3.2	All critical events SHALL be recorded in the system event log.		Fail	Fail	Fail	Fail	Pass	1	4	0	0		20%	80%	0%	0%
5.6.3.3	At a minimum the voting system SHALL log the events described in the table below.		Fail	Fail	Fail	Fail	Fail	0	5	0	0		0%	100%	0%	0%
5.7	**Incident Response**							0	0	0	10		0	0	0	1
5.7.1	**Incident Response Support**							0	0	0	10		0%	0%	0%	100%
5.7.1.1	Manufacturers SHALL document what types of system operations or security events (e.g., failure of critical component, detection of malicious code, unauthorized access to restricted data) are classified as critical.	Wyle determined that this requirement is not applicable to a web based application. But it is a requirement for a web server and therefore could not be tested at this time.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.7.1.2	An alarm that notifies appropriate personnel SHALL be generated on the vote capture device, system server, or tabulation device, depending upon which device has the error, if a critical event is detected.	Wyle determined that this requirement is not applicable to a web based application. A system server notification should be sent to administrators when issues arise with the web server.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.8	**Physical and Environmental Security**							4	0	6	60		1.8%	0.0%	2.7%	95.6%
5.8.1	**Physical Access**							4	0	6	35		9%	0%	13%	78%
5.8.1.1	Any unauthorized physical access SHALL leave physical evidence that an unauthorized event has taken place.	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.8.2.1	The voting system SHALL disable physical ports and access points that are not essential to voting operations, testing, and auditing.	Some system's not tested due to not having lab access to hardware for validation.	Not Tested	Not Tested	Not Tested	Not Tested	Pass	1	0	4	0		20%	0%	80%	0%
5.8.3.1	If a physical connection between the vote capture device and a component is broken, the affected vote capture device port SHALL be automatically disabled.	Wyle determined that this requirement is not applicable to a web based application. A physical connection will only be made during a single instance of vote casting.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.8.3.2	The voting system SHALL produce a visual alarm if a connected component is physically disconnected.	Wyle determined that this requirement is not applicable to a web based application.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.8.3.3	An event log entry that identifies the name of the affected device SHALL be generated if a vote capture device component is disconnected.	Wyle determined that this requirement is not applicable to a web based application.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.8.3.4	Disabled ports SHALL only be re-enabled by authorized administrators.	Some system's not tested due to not having lab access to hardware for validation.	Not Tested	Not Tested	Pass	Pass	Pass	3	0	2	0		60%	0%	40%	0%

5.8.3.5	Vote capture devices SHALL be designed with the capability to restrict physical access to voting device ports that accommodate removable media with the exception of ports used to activate a voting session.	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.8.3.6	Vote capture devices SHALL be designed to give a physical indication of tampering or unauthorized access to ports and all other access points, if used as described in the manufacturer's documentation.	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.8.3.7	Vote capture devices SHALL be designed such that physical ports can be manually disabled by an authorized administrator.	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.8.4	**Door Cover and Panel Security**							0	0	0	5		0%	0%	0%	100%
5.8.4.1	Access points such as covers and panels SHALL be secured by locks or tamper evident or tamper resistant countermeasures and SHALL be implemented so that kiosk workers can monitor access to vote capture device components through these points.	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.8.5	**Secure Paper Record Receptacle**							0	0	0	5		0%	0%	0%	100%
	If the voting system provides paper record containers then they SHALL be designed such that any unauthorized physical access results in physical evidence that an unauthorized event has taken place.	Wyle determined that this requirement is not applicable to a web based application	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.8.6	**Secure Physical Lock and Key**							0	0	0	10		0	0%	0%	100%
5.8.6.1	Voting equipment SHALL be designed with countermeasures that provide physical indication that unauthorized attempts have been made to access locks installed for security purposes.	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.8.6.2	Manufacturers SHALL provide locking systems for securing vote capture devices that can make use of keys that are unique to each owner.	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.8.7	**Media Protection**															
	These requirements apply to all media, both paper and digital, that contain personal privacy related data or other protected or sensitive types of information.							0	0	0	5		0%	0%	0%	100%
5.8.7.1	The voting system SHALL meet the following requirements: a. All paper records (including rejected ones) printed at the kiosk locations SHALL be deposited in a secure container; b. Vote capture device hardware, software and sensitive information (e.g., electoral roll) SHALL be physically protected to prevent unauthorized modification or disclosure; and c. Vote capture device hardware components, peripherals and removable media SHALL be identified and registered by means of a unique serial number or other identifier.	Wyle determined that this requirement is not applicable to a web based application.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.9	**Penetration Resistance**							18	10	8	9		40%	22%	18%	20%
5.9.1	**Resistance to Penetration Attempts**							18	10	8	9		40.0%	22.2%	17.8%	20.0%
5.9.1.1	The voting system SHALL be resistant to attempts to penetrate the system by any remote unauthorized entity.		Pass	Pass	Pass	Fail	Pass	4	1	0	0		80%	20%	0%	0%

5.9.1.2	The voting system SHALL be configured to minimize ports, responses and information disclosure about the system while still providing appropriate functionality.		Pass	Fail	Pass	Pass	Pass	4	1	0	0		80%	20%	0%	0%
5.9.1.3	The voting system SHALL provide no access, information or services to unauthorized entities.		Pass	Fail	Pass	Fail	Pass	3	2	0	0		60%	40%	0%	0%
5.9.1.4	All interfaces SHALL be penetration resistant including TCP/IP, wireless, and modems from any point in the system.		Pass	Pass	Pass	Fail	Pass	4	1	0	0		80%	20%	0%	0%
5.9.1.5	The configuration and setup to attain penetration resistance SHALL be clearly and completely documented.	Based on the system documentation provided by the participants in this test campaign, Wyle was unable to validate this requirement. However, Wyle deems it necessary for future testing.	Not Tested	Not Tested	Not Tested	Fail	Not Tested	0	1	4	0		0%	20%	80%	0%
5.9.2.1	The scope of penetration testing SHALL include all the voting system components. The scope of penetration testing includes but is not limited to the following: System server; Vote capture devices; Tabulation device; All items setup and configured per Technical Data Package (TDP) recommendations; Local wired and wireless networks; and03/09/2011 Internet connections.		Pass	Pass	Pass	Fail	Fail	3	2	0	0		60%	40%	0%	0%
5.9.2.2	Penetration testing SHALL be conducted on a voting system set up in a controlled lab environment. Setup and configuration SHALL be conducted in accordance with the TDP, and SHALL replicate the real world environment in which the voting system will be used.	Wyle was unable to validate this requirement, but deems it necessary for future testing.	N/A	N/A	N/A	Fail	N/A	0	1	0	4		0%	20%	0%	80%
5.9.2.3	The penetration testing team SHALL conduct white box testing using manufacturer supplied documentation and voting system architecture information. Documentation includes the TDP and user documentation. The testing team SHALL have access to any relevant information regarding the voting system configuration. This includes, but is not limited to, network layout and Internet Protocol addresses for system devices and components. The testing team SHALL be provided any source code included in the TDP.	Wyle was unable to validate this requirement, but deems it necessary for future testing.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.9.2.4	Penetration testing seeks out vulnerabilities in the voting system that might be used to change the outcome of an election, interfere with voter ability to cast ballots, ballot counting, or compromise ballot secrecy. The penetration testing team SHALL prioritize testing efforts based on the following: a. Threat scenarios for the voting system under investigation; b. Remote attacks SHALL be prioritized over in-person attacks;	Wyle was unable to validate this requirement, but deems it necessary for future testing.	Not Tested	Fail	Not Tested	Not Tested	Not Tested	0	1	4	0		0%	20%	80%	0%

	c. Attacks with a large impact SHALL be prioritized over attacks with a more narrow impact; and d. Attacks that can change the outcome of an election SHALL be prioritized over attacks that compromise ballot secrecy or cause non-selective denial of service.															

Average summary	Pass	Fail	Not Tested	N/A
	24%	22%	24%	30%