ALEX PADILLA | SECRETARY OF STATE | STATE OF CALIFORNIA
OFFICE OF VOTING SYSTEMS TECHNOLOGY ASSESSMENT
1500 11th Street | Sacramento, CA 95814 | **Tel** 916.653.7244 | **Fax** 916.653.4620 | www.sos.ca.gov

Five Cedars Group
Alternate Format Ballot
Remote Accessible Vote by Mail System

Staff Report

Prepared by:
Secretary of State's Office of
Voting Systems Technology Assessment
August 28, 2017

Table of Contents

I. INTRODUCTION

1. Scope

This report presents the test results for all phases of the certification test of the Five Cedars Group, Alternate Format Ballot Remote Accessible Vote by Mail system. The purpose of the testing is to test the compliance of the voting system with the relevant California Voting System Standards, State and Federal laws. Testing also uncovers other findings, which do not constitute non-compliance, and those findings are reported to the voting system vendor to address the issues procedurally.

2. Summary of the Application

Five Cedars Group submitted an application for the Alternate Format Ballot (AFB) Remote Accessible Vote by Mail system, which is comprised of the following major components:

- HTML Alternate Format Ballot
- AFB Ballot Generator

In addition to the ballot, which includes the HTML source code, Five Cedars Group was required to submit the following: 1) the technical documentation package (TDP); 2) all the software components to field a complete working version of the ballot, including all peripheral devices, for the Functional Test Phase.

3. Contracting and Consultants

Upon receipt of a complete application, the Secretary of State released a Request for Proposal (RFP) for assistance with the Security Review, both Source Code and Security testing. The statement of work (SOW) also had an option for the Secretary of State to use the awarded contractor for Functional testing, if it deemed necessary.

Through the formal California contracting process, the Secretary of State awarded a contract to SLI Compliance (SLI), 4720 Independence Street, Wheat Ridge Colorado.

II. SUMMARY OF THE SYSTEM

1. HTML Alternate Format Ballot

The AFB is an HTML ballot that is generated from text files supplied to Five Cedars by a County that implements the AFB. The implementing County will be

responsible for identifying the correct ballot style for a given voter, and then downloading the AFB ballot to that voter. Currently, AFB ballots can only be generated from text files exported from the Hart system. Once downloaded, the AFB ballot is marked on the voter's home equipment, and then the voter prints a cast vote record (CVR) on their home printer. A cast vote record is a record of the ballot that has been cast, but is not an actual ballot. The AFB CVR is then mailed back to the jurisdiction using a vote by mail ballot envelope. The QR code on the cast vote record contains the following information: a random number which is also printed on the cast vote record in human readable format, the ballot style, a version number , and the codes for the contest choices. The QR code does not contain any voter information. The contest choices are printed in the format 1:3, where 1 represents the first contest on the ballot, and the three represents the third choice in the contest. The CVR is duplicated on ballot at the implementing County.

The computer downloading the AFB ballot can be disconnected from the internet after the ballot is delivered with no adverse results.

2. AFB Ballot Generator

The AFB Ballot Generator is a Windows application that reads County supplied Hart BOSS ballot definition files, creates logical internal data tables, which it uses to build the accessible HTML ballots. The program was written in Microsoft VB.NET using Framework 4.5. The ballots are built by populating a set of pre-built ballot HTML templates which are assembled into a single HTML file for each ballot style required. If the county has supplied XLF ballot translation files, the AFB Ballot Generator will use the translation pairs, and a set of the HTML templates already translated into the desired language, to build ballots in the desired language.

III. TESTING INFORMATION AND RESULTS

1. Background

Five Cedars Group submitted an application to the Secretary of State for certification of the Alternate Format Ballot on April 24, 2017. California assigned AFB the project number CA-AFB1.

California certification testing of the AFB system began in June 2017. The testing began with the Functional Testing, followed by Accessibility Testing, Source Code Review, and finally Security Review.

2. Functional Test Data and Results

The Functional Test of the Five Cedars AFB system was conducted by Secretary of State staff and Five Cedars staff at the Secretary of State's Office located at 1500 11th Street, Sacramento, California from June 5 through June 6, 2017.

The Secretary of State ran the Functional Test as if it were a voter using the system for the first time. Testing was conducted with four (4) laptop computers and one (1) printer provided by Five Cedars. OVSTA tested the Alternate Format Ballot using the following end user equipment:

Table 2A: Functional Test Equipment

Hardware	Software
Hewlett Packard (HP) Spectre laptop	Windows 10, Microsoft Narrator, JAWS version 18 screen reader, and a free reader from Australia called NVDA
Apple MacBook Air laptop	Apple accessibility software
Chromebook	ChromeVox version 53.0.2785.154 accessibility software
Apple iPad	Standard Apple accessibility software

The cast vote records were printed on a Canon P1100 ink jet printer.

The Five Cedars representative generated ballots with the Five Cedars Ballot Generator software. The ballots were generated from the San Mateo 2012 General Election using comma separated text files exported from the Hart BOSS 4.3 system. The seven text files exported from the San Mateo 2012 General Election were:

- Candidate.txt
- Candidate_detail.txt
- Contest.txt
- Contest_and_Precinct.txt
- Election.txt
- Party.txt
- Precinct.txt

The Five Cedars Ballot Generator software worked as expected and generated AFB ballots correctly. At this time, the Five Cedars system will only generate ballots from text files that are exported from a Hart BOSS 4.3 system.

The AFB ballot will allow over-votes, but warns the voter of the over-vote condition. The ballot also warns the voter of under-votes if you click on the "Test This Ballot" button. The AFB performed as expected against all California Secretary of State test cases, as well as the vendor supplied AFB test cases supplied by Five Cedars.

Table 2B: Test Environment and Results	
Test Environment	**Result**
HP Spectre laptop using Windows 10 and Narrator with Internet Explorer browser.	Performed as expected.
HP Spectre laptop using Windows 10 and Narrator with Microsoft Edge browser.	Narrator encountered many problems with the Microsoft EDGE browser.
HP Spectre laptop using Windows 10 and JAWS version 18 screen reader with Internet Explorer browser.	Performed as expected.
HP Spectre laptop using Windows 10 and JAWS version 18 screen reader with Microsoft Edge browser.	JAWS encountered many errors when using the Microsoft Edge browser.
HP Spectre laptop using Windows 10 and NVDA free reader with Internet Explorer browser.	Performed as expected.
HP Spectre laptop using Windows 10 and NVDA free reader with Microsoft Edge browser.	NVDA encountered many errors when using the Microsoft Edge browser.
Apple MacAir laptop running Sierra version 10.12.4, and the standard Apple accessible software	Performed as expected.

Apple iPad running IOS 11, and the standard Apple accessibility software	Performed as expected.
Chromebook laptop using ChromeVox version 53.0.2785.154 accessibility software.	Experienced one failure.
Dell laptop running Windows 7 with Narrator	Worked approximately 50% of the time.

The QR code was scanned from the cast vote record using an iPhone 4 smart phone running the following apps:

- Free QR Code Reader & BarCode Scanner from MixerBox Inc.
- QR Reader for iPhone by TapMedia Ltd.
- I-nigma QR Code and Data Matrix and 1D BarCode Reader from 3GVision.

The free QR code reader from MixerBox, Inc. would not read the QR code. The QR Reader for iPhone by TapMedia Ltd. would not read the QR code. The I-nigma QR code Reader from 3GVision read the QR code as expected with no problems or errors.

Findings

The computer downloading the AFB ballot can be disconnected from the internet after the ballot is downloaded with no adverse results.
The AFB performed as expected against all California Secretary of State test cases, as well as the vendor supplied AFB test cases supplied by Five Cedars.

3. Source Code Review

The Source Code Review for the Five Cedars AFB system was conducted by SLI. The Source Code Review includes proprietary source code. The AFB system code was tested to the applicable California Voting System Standards (CVSS) requirements, and any applicable industry standards, as detailed below.

SLI conducted a source code review of the source code for compliance to the CVSS. The source code was reviewed for adherence to the applicable standards in sections 5 and 7 of the CVSS. The expected outcome was that no issue would be found. The actual outcome was a determination that for the "Dead Code" (CVSS 5.2.7.e) requirement found in the source code base reviewed, two discrepancies were written against the code base, and for the

“Sufficient Header Comments” (CVSS 5.2.6.a-h) requirement found in the source code base reviewed, three discrepancies were written against the code base.

The source code was reviewed for adherence to other applicable coding format conventions and standards including best practices for the coding language used. The expected outcome for this review was that no issue would be found. The actual outcome for this review was a determination that the source code was clean and met all CVSS and applicable standards requirements in this category.

An analysis of the program logic and branching structure was conducted. The expected outcome was that no issue would be found. The actual outcome was a determination that the program logic and branching structure was reasonable and sufficient for the functionality implemented.

An evaluation of whether the system is designed in a way that allows meaningful analysis, was conducted, including:

- Whether the architecture and code is amenable to an external review.
- Whether code analysis tools can be usefully applied.
- Whether the code complexity is at a level that obfuscates its logic.

The expected outcome was that no issue would be found. The actual outcome was a determination that the architecture and code is amenable to external review and that the code complexity does not obfuscate the logic. Code analysis tools could be applied to this code base, but it is of a small quantity that manual review was as useful, if not more so.

The AFB source code was searched for exposures to commonly exploited vulnerabilities including buffer overflows and SQL issues.

- The expected outcome for this review was that no exposures to commonly exploited vulnerabilities would be found in the AFB source code.
- The actual outcome for this review was a determination that no exposures to commonly exploited vulnerabilities were found in the AFB source code.

The AFB source code was evaluated for the use and correct implementation of cryptography and key management. The expected outcome for this review was that cryptography and key management would be found to be correctly implemented in the AFB source code, as per the CVSS. The actual outcome for this review was a determination that cryptography and key management is correctly implemented in the AFB source code.

The AFB source code was analyzed for its ability to appropriately accommodate error and exception handling. The expected outcome for this review was that no issues with error and exception handling would be found in the AFB source code. The actual outcome for this review was a determination that no error and exception handling issues were found in the AFB source code.

The AFB source code was evaluated in two areas for the likelihood of security failures being detected.

a. Evaluate whether audit mechanisms are reliable and tamper resistant. The expected outcome for this review was that audit mechanisms in the AFB source code would be found to be reliable and tamper resistant. The actual outcome for this review that no issues were found – audit mechanisms in the AFB source code were found to be reliable and tamper resistant.

b. Evaluate whether data that might be subject to tampering is properly validated and authenticated The expected outcome for this review was that any data in the AFB source code that might be subject to tampering would be properly validated and authenticated. The actual outcome for this review was that no issues were found – any data in the AFB source code that might be subject to tampering is properly validated and authenticated.

The AFB source code was evaluated for the risk that a user can escalate his or her capabilities beyond those authorized. The expected outcome for this review was that in the AFB source code, a user cannot escalate his or her capabilities beyond those authorized. The actual outcome for this review was a determination that in the AFB source code, a user cannot escalate his or her capabilities beyond those authorized.

The AFB source code was evaluated for embedded, exploitable code (such as “Easter eggs”) that can be triggered to affect the system. The expected outcome for this review was that no embedded, exploitable code (such as “Easter eggs”) that can be triggered to affect the system would be found to be resident in the AFB source code. The actual outcome for this review was a determination that no embedded, exploitable code (such as “Easter eggs”) that can be triggered to affect the system was found to be resident in the AFB source code.

The AFB source code was evaluated that no code for dynamic memory access features which would permit the replacement of certificated executable code or control data or insertion of exploitable code or data would be found. The expected outcome for this review was that code for dynamic memory access features which would permit the replacement of certificated executable code or control data or insertion of exploitable code or data would not be found in the AFB source code. The actual outcome for this review was a determination that

no code for dynamic memory access features which would permit the replacement of certificated executable code or control data or insertion of exploitable code or data was found in the AFB source code.

The AFB source code was evaluated for use of runtime scripts, instructions, or other control data that can affect the operation of security relevant functions or the integrity of the data. The expected outcome for this review was that no use of runtime scripts, instructions, or other control data would be found in the AFB source code. The actual outcome for this review was a determination that no use of runtime scripts, instructions, or other control data that can affect the operation of security relevant functions or the integrity of the data was found in the AFB source code.

The AFB source code was evaluated that no code for dynamic memory access features which would permit the replacement of certificated executable code or control data or insertion of exploitable code or data would be found. The expected outcome for this review was that code for dynamic memory access features which would permit the replacement of certificated executable code or control data or insertion of exploitable code or data would not be found in the AFB source code. The actual outcome for this review was an determination that no code for dynamic memory access features which would permit the replacement of certificated executable code or control data or insertion of exploitable code or data was found in the AFB source code.

The AFB source code was evaluated for design and implementation to ensure that sound, generally accepted engineering practices are followed, checking to verify that code is defensively written against bad data, errors in other modules, changes in environment, user errors, and other adverse conditions. The expected outcome for this review was that generally accepted engineering practices are followed and the code is defensively written in the AFB source code. The expected outcome for this review was a determination that in the AFB source code, generally accepted engineering practices are followed and the code is defensively written against bad data, errors in other modules, changes in environment, user errors, and any other potential adverse conditions.

Discrepancies

Ten discrepancies for the “Sufficient Header comments” requirement were found in the AFB source code base reviewed, as a result, ten discrepancies were written against the code base.

Vulnerabilities

For any vulnerabilities discovered, SLI was tasked with identifying the particular

standards applicable to each vulnerability. To the extent possible, reported vulnerabilities included an indication of whether the exploitation of the vulnerability would require access by:

- A Voter. Voters usually have low knowledge of the Remote Accessible Vote by Mail Machine System (RAVBMS) design and configuration. Some may have more advanced knowledge. A voter may carry out attacks designed by others.
- An Elections official insider. Elections official have a wide range of knowledge of the RAVBMS design and configuration. An official may have unrestricted access to the RAVBMS for long periods of time. Their designated activities include:
    - Set up and pre-election procedures;
    - Election operation;
    - Post-election processing of results; and
    - Archiving and storage operations.
- A Vendor insider: A vendor insider has great knowledge of the RAVBMS design and configuration. They have unlimited access to the RAVBMS before it is delivered to the purchaser and, thereafter, may have unrestricted access when performing warranty and maintenance service and when providing election administration services.

No vulnerabilities were found within the source code reviewed, as a result, no findings were written against the code base.

Findings

Ten discrepancy findings were located within the AFB system.

No potential vulnerabilities were identified within the AFB code base.

Within the AFB code base, all findings were low risk vulnerabilities that would require an in-depth knowledge of the code base and how it operates to be able to successfully subvert the system. To exploit them successfully, it would require modifying the code.

4. Security

Security testing was done at SLI. Testing was implemented without any prior knowledge of the source code.

The testing was divided into three phases.

- Phase I included a review of all pertinent documents for appropriate processes and procedures for implementing a secure system. This included review of the system design and architecture.
- Phase II included testing of relevant software, operating systems and hardware configurations.
- Phase III included testing of all telecommunications aspects of the system.

Phase I

Table 4A: Documentation Review	
Testing Performed	**Results**
5.5 Vote Secrecy on Electronic Ballot Marking (EBM) Systems a. Immediately after the ballot is recorded to persistent electronic storage or printed, erasing the selections from the device's display, working memory, and all other storage, including all forms of temporary storage. b. Immediately after the voter chooses to cancel his or her ballot, erasing the selections from the display and all other storage, including buffers and other temporary storage.	Review of the Technical Data Package (TDP) validated that the requirement was satisfactorily covered.
6.1.2 Data Transmissions These requirements apply to the use of telecommunications to transmit data for the preparation of the system for an election, the execution of an election, and the preservation of the system data and audit trails during and following an election. While this section does not assume a specific model of voting system operations and does not assume a specific model for the use of telecommunications to support such operations, it does address the following types of data, where applicable: • **Voter Authentication**: Coded information that confirms the identity of a voter for security purposes for a system that transmits votes individually. • **Ballot Definition**: Information that describes to a	Review of the Technical Data Package (TDP) validated that the requirement was satisfactorily covered.

voting machine the content and appearance of the ballots to be used in an election. • **Vote Count**: Information representing the tabulation of votes at any level within the control of the jurisdiction, such as the polling place, precinct or central count. **List of Voters**: A listing of the individual voters who have cast ballots in a specific election. Additional data transmissions used to operate a voting system in the conduct of an election, but not explicitly listed above, are also subject to the requirements of this section.	
6.2 Design, Construction, and Maintenance Requirements Design, construction, and maintenance requirements for telecommunications represent the operational capability of both system hardware and software. These capabilities **shall** be considered basic to all data transmissions.	Review of the Technical Data Package (TDP) validated that the requirement was satisfactorily covered.
6.2.1 Confirmation Confirmation occurs when the system notifies the user of the successful or unsuccessful completion of the data transmission, where successful completion is defined as accurate receipt of the transmitted data. To provide confirmation, the telecommunications components of a voting system shall notify the user of the successful or unsuccessful completion of the data transmission. In the event of unsuccessful transmission the user shall be notified of the action to be taken.	Review of the Technical Data Package (TDP) validated that the requirement was satisfactorily covered.
7.1.1 Elements of Security Outside Manufacturers Control The requirements of this section apply to the capabilities of a voting system that must be provided by the manufacturer. However, an effective security program requires well defined security practices by the purchasing jurisdiction and the personnel managing and operating the system. These practices include: • Administrative and management --including access controls.	Review of the Technical Data Package (TDP) validated that the requirement was satisfactorily covered.

• Internal security procedures. • Adherence to, and enforcement of, operational procedures (e.g., effective password management). • Security of physical facilities. • Organizational responsibilities and personnel screening.	
7.2 Access control Access controls are procedures and system capabilities that detect or limit access to system components in order to guard against loss of system integrity, availability, confidentiality, and accountability. Access controls provide reasonable assurance that system resources such as data files, application programs, and computer-related facilities and equipment are protected against unauthorized operation, modification, disclosure, loss or impairment. Unauthorized operations include modification of compiled or interpreted code, run-time alteration of flow control logic or of data, and abstraction of raw or processed voting data in any form other than a standard output report by an authorized operator. Access controls may include physical controls, such as keeping computers in locked rooms to limit physical access, and technical controls, such as security software programs designed to prevent or detect unauthorized access to sensitive files. The access controls described in this section are limited to those controls required to be provided by system manufacturers.	Review of the Technical Data Package (TDP) validated that the requirement was satisfactorily covered.
7.2.1 General Access Control • Voting system equipment **shall** provide access control mechanisms designed to permit authorized access to the voting system and to prevent unauthorized access to the voting system. Access control mechanisms on the EMS **shall** be capable of identifying and authenticating individuals permitted to perform operations on the EMS. • Voting system equipment **shall** provide controls that permit or deny access to the device's software and files. • The default access control permissions **shall**	Review of the Technical Data Package (TDP) validated that the requirement was satisfactorily covered.

implement the minimum permissions needed for each role or group identified by a device. • The voting device **shall** prevent a lower-privileged process from modifying a higher-privileged process. • An administrator of voting system equipment **shall** authorize privileged operations. • Voting system equipment **shall** prevent modification to or tampering with software or firmware through any means other than the documented procedure for software upgrades.	
7.2.2 General Access Control Identification requirements provide controls for accountability when operating and administering a voting system. • The voting system **shall** identify users and processes to which access is granted and the specific functions and data to which each entity holds authorized access.	Review of the Technical Data Package (TDP) validated that the requirement was satisfactorily covered.
7.4.5 Software Reference Information The manufacturer **shall** provide the National Software Reference Library (NSRL), any California certified escrow facility, pursuant to Title 2, Division 7, Chapter 6 of the California Code of Regulation, and the Office of the Secretary of State with a copy of the software installation disk, including the executable binary images of all third party software. Further, the manufacturer **shall** deposit the source code, tools, and documentation, to allow the complete and successful compilation of a system in its production/operation environment. The manufacturer **shall** document that the process used to verify the software distributed on unalterable storage media is the certified software by using the reference information provided by the NSRL or other designated repository before installing the software. The manufacturers **shall** document to whom they provide voting system software.	Review of the Technical Data Package (TDP) validated that the requirement was satisfactorily covered.
7.4.6 Software Setup Validation Setup validation methods **shall** verify the contents of all	Review of the Technical Data Package (TDP)

system storage locations (e.g., system registers, variables, files, etc.) containing election specific information (e.g., ballot style, candidate registers, measure registers, etc.).	validated that the requirement was satisfactorily covered.
7.8 Testing – Security The S-ATA **shall** design and perform test procedures that test the security capabilities of the voting system against the requirements. These procedures **shall** focus on the ability of the system to detect, prevent, log, and recover from the broad range of security risks identified. These procedures **shall** also examine system capabilities and safeguards claimed by the manufacturer in the TDP to go beyond these risks. The range of risks tested is determined by the design of the system and potential exposure to risk. Regardless of system design and risk profile, all systems **shall** be tested for effective access control and physical data security. The S-ATA may meet these testing requirements by confirming proper implementation of proven commercial security software. In this case, the manufacturer must provide the published standards and methods used by the U.S. Government to test and accept this software, or it may provide references to free, publicly available publications of these standards and methods, such as government web sites. At its discretion, the S-ATA may conduct or simulate attacks on the system to confirm the effectiveness of the system's security capabilities.	Review of the Technical Data Package (TDP) validated that the requirement was satisfactorily covered.

Phase II

In this phase, functional tests were exercised in order to verify and validate security requirements, following are the requirements with their accompanying results:

- 5.5 Vote Secrecy on DRE and EBM Systems
- 7.2.1 General Access Control
- 7.2.2 Access Control Identification
- 7.2.4 Access Control Authorization
- 7.4.5 Software Reference Information

- 7.4.6 Software Setup Validation
- 7.6 Telecommunications and Data Transmission
- 7.8 Testing – Security
- 7.8.1 Access Control
- 7.8.2 Data Interception and Disruption

Table 4B: Phase II Functional Security Test		
CVSS Requirement	**Testing Performed**	**Result**
5.5 Vote Secrecy on Electronic Ballot Marking (EBM) Systems • Immediately after the ballot is recorded to persistent electronic storage or printed, erasing the selections from the device's display, working memory, and all other storage, including all forms of temporary storage. • Immediately after the voter chooses to cancel his or her ballot, erasing the selections from the display and all other storage, including buffers and other temporary storage.	Testing was performed to verify how the system handled a ballot being printed and the browser closed, as well as when the ballot is closed prior to being printed. Attempts were made to resume a ballot, as well as to determine if any ballot information resided in history or cache.	AFB performed as expected and the requirement is met.
7.2.1 General Access Control General requirements address the high-level functionality of a voting system. These are the fundamental access control requirements upon which other requirements in this section are based. • Voting system equipment **shall** provide access control mechanisms designed to permit authorized access to the voting system and to prevent unauthorized access to the voting system.	Review of the requirement and attempted validation concludes that the Five Cedars AFB product does not have any built in access control mechanisms. Paradigm used is for the jurisdiction to host ballot files on their voter registration system.	For this particular product and suggested delivery system this requirement is not applicable.
7.2.2 Access Control Identification Identification requirements provide controls for accountability when	Review of the requirement and attempted validation concludes that the Five	For this particular product and suggested

operating and administering a voting system. • The voting system **shall** identify users and processes to which access is granted and the specific functions and data to which each entity holds authorized access.	Cedars AFB product does not have any built in access control identification mechanisms. Paradigm used is for the jurisdiction to host ballot files on their voter registration system.	delivery system this requirement is not applicable.
7.2.4 Access Control Authorization Voting systems **shall** explicitly deny subject's access based on access control lists or policies.	Review of the requirement and attempted validation concludes that the Five Cedars AFB product does not have any built in access control authorization mechanisms. Paradigm used is for the jurisdiction to host ballot files on their voter registration system.	For this particular product and suggested delivery system this requirement is not applicable.
7.4.5 Software Reference Information The voting system equipment **shall** be designed to allow the voting system administrator to verify that the software is the certified software by comparing it to reference information produced by the NSRL or other designated repository.	Review of the requirement and attempted validation concludes that the system does not have checks in place to validate that any software is the certified software, as there is no software involved, simply custom made HTML ballots.	For this particular product and suggested delivery system this requirement is not applicable.
7.4.6 Software Setup Validation • Setup validation methods **shall** include a software verification method that ensures that the voting system software has not been modified illegitimately. o The voting systems **shall**	Review of the requirement and attempted validation concludes that the system doesn't have checks in place to validate that the AFB ballot system is the correct system, as there	N/A

include any supporting software and hardware necessary to conduct the software verification method. o The manufacturer **shall** document the process used to conduct the software verification method. o The software verification method **shall** not modify the voting system software on the voting system.	is no software involved, simply custom made HTML ballots.	
7.6 Telecommunications and Data Transmission There are four areas that must be addressed by telecommunications and data transmission security capabilities: access control, data integrity, detection and prevention of data interception, and protection against external threats.	Review of the requirement confirmed that the system utilizes electrical or optical transmission, and that the ballot may be sent via SSL or in other unspecified mediums. It was determined that no technology is utilized to verify unaltered receipt by the voter. What is sent/served is a blank ballot that does not contain any voter data or voting selections. Main security protocol is that once the blank ballot is delivered, there are no more communications between the voter and the ballot delivery system, all interactions remain local to the voter's environment.	For this particular product and suggested delivery system this requirement is not applicable.
7.8 Testing Security The S-ATA **shall** design and perform test procedures that test the security capabilities of the voting system against the requirements. These	Confirmed that the AFB HTML ballot doesn't require internet access once the ballot has been downloaded. Confirmed there are no external	AFB performed as expected and the requirement was met.

procedures **shall** focus on the ability of the system to detect, prevent, log, and recover from the broad range of security risks identified. These procedures **shall** also examine system capabilities and safeguards claimed by the manufacturer in the TDP to go beyond these risks. The range of risks tested is determined by the design of the system and potential exposure to risk. Regardless of system design and risk profile, all systems **shall** be tested for effective access control and physical data security. The S-ATA may meet these testing requirements by confirming proper implementation of proven commercial security software. In this case, the manufacturer must provide the published standards and methods used by the U.S. Government to test and accept this software, or it may provide references to free, publicly available publications of these standards and methods, such as government web sites. At its discretion, the S-ATA may conduct or simulate attacks on the system to confirm the effectiveness of the system's security capabilities.	connections from the ballot to any outside server or service. With the exception of printing the Summary there are no external connections from the ballot.	
7.8.1 Access Control For those access control features built in as components of the voting system, the S-ATA **shall** design tests to confirm that these security elements work as specified. Specific activities to be conducted by the S-ATA **shall** include: Specific tests designed by the S-ATA to verify the correct operation of all documented access control	Review of the requirement and attempted validation determined that the Five Cedars AFB product contains no access control capabilities beyond those of which the jurisdiction plans to implement. The requirement for security of the interactive ballots are based upon the already in place	N/A

procedures and capabilities, including tests designed to circumvent controls provided by the manufacturer. These tests **shall** include: o Performing the activities that the jurisdiction will perform in specific accordance with the manufacturer's access control policy and procedures to create a secure system, including procedures for software and firmware installation. o Performing tests intended to bypass or otherwise defeat the resulting security environment. These tests **shall** include simulation of attempts to physically destroy components of the voting system in order to validate the correct operation of system redundancy and backup capabilities. This review applies to the full scope of system functionality. It includes functionality for defining the ballot and other pre-voting functions, as well as functions for casting and storing votes, vote canvassing, vote reporting, and maintenance of the system's audit trail.	Absentee/Mail-in ballot system and the security of the delivery method (Email, HTTPS, File sharing).	
7.8.2 Data Interception and Disruption For systems that use telecommunications, as provided for in section 6 of the Standards and consistent with California law, to transmit official voting data, the SATA **shall** review, and conduct tests of, the	Review of the requirement verified that this system does not utilize telecommunications for the transmission of official voting data. Only delivery of blank ballot that does not contain	AFB performed as expected and the requirement was met**.**