County of Los Angeles VSAP 1.2 Interactive Sample Ballot RAVBMS Security and Telecommunications Test Report

CAF-19017-RSECTR-01

Vendor Name	County of Los Angeles
Vendor System	VSAP 1.2 Interactive Sample Ballot RAVBMS

Prepared by:

4720 Independence St.
Wheat Ridge, CO 80033
303-422-1566
www.SLICompliance.com

Accredited by the Election Assistance Commission (EAC) for Selected Voting System Test Methods or Services

Revision History

Date	Release	Author	Revision Summary
Nov.19, 2019	v1.0	J. Peterson	Initial Release
Dec. 12, 2019	v2.0	J. Peterson	Updated for new code release
Dec. 17, 2019	v3.0	J. Peterson	Updated for new code release
Dec 24, 2019	v4.0	J. Peterson	Updated for CA SOS comments

Disclaimer

The information reported herein must not be used by the client to claim product certification, approval, or endorsement by NVLAP, NIST, or any agency of the Federal Government.

Trademarks

- SLI is a registered trademark of SLI Compliance.
- All products and company names are used for identification purposes only and may be trademarks of their respective owners.

TABLE OF CONTENTS

INTRODUCTION

The California Voting Systems Standards (CVSS) were written in such a way to be applicable to a wide variety of voting technology. Therefore, the relevant portions of the CVSS are reviewed as the relate to the Remote Accessible Vote by Mail (RAVBM) system for the purposes of this report. The use of "voting system" shall apply to the RAVBM system.

This report outlines the testing SLI Compliance (SLI) followed when performing Security and Telecommunications Testing on the **Los Angeles County VSAP 1.2 Interactive Sample Ballot RAVBM System** (**VSAP 1.2 ISB RAVBMS**) against the California Voting System Standards (CVSS).

The VSAP 1.2 ISB RAVBMS enables the voter to mark their ballot using a secure web-based interface and generate and download a PDF representation of choice selections. Voters then print that ballot, and then return it to their clerk.

Phase I – Documentation Review

During Phase I testing of the **VSAP 1.2 ISB RAVBMS**, documentation was reviewed to verify and validate the following requirements:

- Top-level system design and architecture
- System documentation and procedures

During Phase I testing, documentation was reviewed to verify and validate in accordance with the following CVSS requirements:

- 5.5 Vote Secrecy on Direct Recording Electronic (DRE) and Electronic Ballot Marking (EBM) Systems
- 6.1.2 Data Transmissions
- 6.2 Design, Construction, and Maintenance Requirements
- 6.2.1 Confirmation
- 7.1.1 Elements of Security outside Manufacturers Control
- 7.2 Access control
- 7.2.1 General Access Control
- 7.2.2 General Access Control
- 7.4.5 Software Reference Information
- 7.4.6 Software Setup Validation
- 7.8 Testing – Security

See the applicable section below for more details on these requirements and the review results.

5.5 Vote Secrecy on DRE and EBM Systems

All DRE and EBM systems **shall** ensure vote secrecy by:

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

Results: 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 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.

Results: Review of the Technical Data Package (TDP) validated that the requirement was satisfactorily covered.

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.

Results: 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.

Results: 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 controls for the voting system and election management, including access controls
- Internal security procedures
- Adherence to, and enforcement of, operational procedures (e.g., effective password management)
- Security of physical facilities
- Organizational responsibilities and personnel screening

Results: Review of the Technical Data Package (TDP) validated that the requirement was satisfactorily covered.

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.

Results: Review of the Technical Data Package (TDP) validated that the requirement was satisfactorily covered.

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.

a. 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.
    i. Access control mechanisms on the EMS **shall** be capable of identifying and authenticating individuals permitted to perform operations on the EMS.
b. Voting system equipment **shall** provide controls that permit or deny access to the device's software and files.
c. The default access control permissions **shall** implement the minimum permissions needed for each role or group identified by a device.
d. The voting device **shall** prevent a lower-privileged process from modifying a higher-privileged process.
e. An administrator of voting system equipment **shall** authorize privileged operations.
f. Voting system equipment **shall** prevent modification to or tampering with software or firmware through any means other than the documented procedure for software upgrades.

Results: Review of the Technical Data Package (TDP) validated that the requirement was satisfactorily covered.

7.2.2 Access Control Identification

Identification requirements provide controls for accountability when operating and administering a voting system.

a. 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.

Results: Review of the Technical Data Package (TDP) validated that the requirement was satisfactorily covered.

7.4.5 Software Reference Information

a. The manufacturer **shall** provide the 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.

    i. 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.

c. The manufacturers **shall** document to whom they provide voting system software.

Results: Review of the Technical Data Package (TDP) validated that the requirement was partially covered.

The documentation doesn't describe a process used to verify buttons on the software distributed is the software provided by the NSRL or designated repository. The documentation doesn't provide a procedure or functionality to verify that the software is the certified software by comparison.

7.4.6 Software Setup Validation

g. Setup validation methods **shall** verify the contents of all system storage locations (e.g., system registers, variables, files, etc.) containing election specific information (e.g., ballot style, candidate registers, measure registers, etc.).

Results: Review of the Technical Data Package (TDP) validated that the requirement was partially covered.

The documentation doesn't reference any type of digital verification on software prior to installation. No documentation on the method provided by external interface or equipment used to verify software on the system. No documentation about a mechanism for detecting unauthorized software.

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.

7.8.1 Access Control

The accredited testing laboratory **shall** conduct tests of system capabilities and review the access control policies and procedures submitted by the manufacturer to identify and verify the access control features implemented as a function of the system. 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:

a. A review of the manufacturer's access control policies, procedures and system capabilities to confirm that all requirements have been addressed completely

Results: Review of the Technical Data Package (TDP) validated that the requirement was satisfactorily covered.

It should be noted that after the initial connection with the RAVBMS server to acquire the ballot, the client side ballot is generated in the voter's ballot and further connectivity with the RAVBMS sever is severed, until the user is presented with the option to print or save the poll pass. At this point the server is contacted to download images for the save and print buttons on the final screen.

Phase II – Functional Security Testing

Phase II testing included:

- Testing of relevant software and operating system configuration for pertinent vulnerabilities
- Testing of hardware, including examination of unused hardware ports and security measures applied to those ports

During Phase II, tests were exercised in order to verify and validate functional security in accordance with the following CVSS requirements:

- 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

See the applicable section below for more details on these requirements and the review results.

An issue log of any errors, anomalies, or omissions encountered during Phase II testing was maintained.

5.5 Vote Secrecy on DRE and EBM Systems

All DRE and EBM systems **shall** ensure vote secrecy by:

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

Testing performed: Testing was to verify that the system fully erases the current session once a ballot is printed, as well as when the ballot is closed prior to being printed.

Results: Review of the requirement validated that the requirement was partially covered.

- Review of the VSAP 1.2 ISB RAVBMS product showed that after the ballot was printed and or downloaded the locally stored browser data of the voter's selections are purged.
- When the voter selects the option to store selection in the browser the voter's selections are stored in local persistent storage, allowing the voter to start and stop the ballot by closing and reopening the browser.
- When the voter selects the option to not store the selection in the browser the selections are only present in the browser's session storage allowing the voter to close the ballot and not retain the ballot selections.
- Was able to find and manipulate Selections of the marked ballot information in browser history or cache. This was true if the option to retain ballot selections was chosen.
- Unable to easily determine if the downloadable or printable poll pass contains the voter's selections as it comes in the form of a QR code, the human readable portion of the QR code doesn't provide the actual contents of the voter's ballot selections. The QR code contains the voter selections in a series of 2-character codes that pertain to the voter selections on the ballot comparing the 2 character codes.
- The ability to cancel the voter's ballot when the option to save selections was used is unapparent, due to the ability to save selections to local storage it should be noted that this could lead to the voter's selection being saved in a persistent manner even if the voter believes that closing the ballot will cancel his/her ballot marking attempt. If the user selects the ability to save selections on a public computer that voter's selections could be compromised.
- Unable to find specific data that ties ballot data to a specific voter.

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.

a. 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.

Testing performed: Testing was to verify any implemented access control mechanisms for permitted authorized access, as well as prevention of unauthorized access.

- VSAP 1.2 ISB RAVBMS system uses an N-tier architecture that consists of separate client applications, application server components, database components, and a central document repository.
- Authentication included methods for both the voter facing application as well as the administrative application.
- Security was tested on the architecture pieces, client application and administrative application, which were accessible remotely.
- Physical Security was not able to be observed as this was hosted at a data center.

Results: Review of the requirement validated that the requirement was satisfactorily covered.

7.2.2 Access Control Identification

Identification requirements provide controls for accountability when operating and administering a voting system.

a. 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.

Testing performed: Testing was to verify that the system allows only appropriate access to specific functions and data.

Results: Review of the requirement validated that the requirement was satisfactorily covered.

- VSAP 1.2 ISB RAVBMS system uses a client server system to authenticate registered voters and serve up the correct ballot for a particular voter. Using predefined ballot rules and voters that can be imported by the jurisdiction.
- Role based access controls are in place for administrative login purposes.

7.2.4 Access Control Authorization

a) Voting systems shall ensure that only authorized roles, groups, or individuals have access to election data.

b) Voting systems shall explicitly authorize subject's access based on access control lists or policies.

c) Voting systems **shall** explicitly deny subject's access based on access control lists or policies

Testing performed: Testing was to verify that the system prevents unauthorized access attempts.

Results:

Review of the requirement validated that the requirement was satisfactorily covered.

- All access to the system is controlled by last name, date of birth, and street number.
- All administrative access is controlled by username/password combinations and there is a role based administrative access in place.
- The ability to assign voters different electoral groups/ electoral districts gives the ability to assign ballots to voters given specific rules.

7.4.5 Software Reference Information

b. 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.

Testing performed: Testing was to verify that the voting system administrator has the capability to confirm the installed system.

Results: Review of the requirement validated that the requirement was partially covered.

Review of the requirement failed to validate that the system has checks in place to verify software integrity through secure hashing.

- No methods or procedures for verification if the system is running certified unmodified code were presented.

7.4.6 Software Setup Validation

c. Setup validation methods **shall** include a software verification method that ensures that the voting system software has not been modified illegitimately.

i. The voting systems **shall** include any supporting software and hardware necessary to conduct the software verification method.

ii. The manufacturer **shall** document the process used to conduct the software verification method.

iii. The software verification method **shall** not modify the voting system software on the voting system.

Testing performed: Testing was to verify that the installation and verification process for each system component is robust and maintains the integrity of the voting system.

Results: Review of the requirement validated that the requirement was partially covered.

Review of the requirement was not able to validate a documented method to verify the system's version or ability to verify software integrity. It is noted that the system has an undocumented process in place to verify software integrity through secure hashing, and as of the time of this work paper the full process for validation of the deployed software or version is not available in a documented form.

- The VSAP 1.2 ISB RAVBMS product does not have built in hash verification method for the system which provides a method to verify that the source code is not running modified code.
- Testing was unable to successfully modify the server code to verify if a protection method was in place and viable.
- The system doesn't have a documented way to verify the version of the software.

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.

Testing performed: Testing was to confirm that if the system utilizes electrical or optical transmission, proper security measures are utilized for the content being transmitted.

Results: Review of the requirement validated that the requirement was partially covered.

Review of the requirement confirmed that the system utilizes electrical or optical transmission, no receipt is utilized to verify delivery.

- It was noted in the tested configuration that the ISB pre-processor administrative interface was not setup to utilize SSL communications

- The voter initially generates a blank ballot which does not contain voting selections.
- Once the blank ballot is delivered, all interactions remain local during all voter selection activities in the voter's environment.
- As soon as the voter saved and or prints the poll pass the browser's cached information is purged from the browser. No selections were observed being transmitted from the voter's machine.

7.8 Testing – Security

The state-approved testing agency (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.

Testing performed: Confirm that the system:

- Does not have nor require internet access once the ballot has been downloaded;
- There are no external connections from the ballot to any outside server or service during voter ballot selection.

Results: Review of the requirement validated that the requirement was satisfactorily covered.

Review of the requirement confirmed that VSAP 1.2 ISB RAVBMS does not have, nor require, internet access once the ballot has been downloaded. During the voter selection process there are no external connections from the ballot to any outside server or service.

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:

b. Specific tests designed by the S-ATA to verify the correct operation of all documented access control procedures and capabilities, including tests designed to circumvent controls provided by the manufacturer. These tests **shall** include:

   i. 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

   ii. 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.

Testing performed: Testing was to verify the documented procedures, as well as attempts to defeat the implemented access control security on each system component.

- Attempted XSS attacks, SQL Injection attacks, Directory listings / scans, attempted to pull directory file lists, scanned for default http login pages, scanned for robots txt file, pulled SSL certificate information.
- Performed a full WMAP Web vulnerability scan.
- Burp Suite to fully scan, spider and intercept both the Voter facing application and the Administrative application.
- Nessus scan performed.

Results: Review of the requirement validated that the requirement was satisfactorily covered.

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 S-ATA **shall** review, and conduct tests of, the data interception and prevention safeguards specified by the manufacturer in its TDP. The S-ATA **shall** evaluate safeguards provided by the manufacturer to ensure their proper operation, including the proper response to the detection of efforts to monitor data or otherwise compromise the system.

Testing performed: Confirm that this system does not utilize telecommunications for the transmission of official voting data and that the system delivers a blank ballot that does not contain voter data or choice selections.

Results: Review of the requirement validated that the requirement was satisfactorily covered.

Review of the requirement verified that this system does not utilize telecommunications for the transmission of official voting data. Delivery of blank ballot that does not contain voter data or choice selections.

Phase III – Telecommunications and Data Transmission Testing

Phase III consisted of the testing of system communications, including encryption of data, as well as protocols and procedures for access authorization

During Phase III, tests were exercised in order to verify and validate telecommunications and data transmission in accordance with the following CVSS requirements:

- 6.1.2 Data Transmission
- 6.2 Design, Construction, and Maintenance Requirements
    - 6.2.1 Confirmation

See the applicable section below for more details on these requirements and the review results.

An issue log of any errors, anomalies, or omissions encountered during Phase III testing was maintained.

6.1.2 Data Transmission

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 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.

Testing performed: Testing was to determine if there were any basic web server vulnerabilities in the initial serving of the in-browser application that houses the VSAP 1.2 ISB RAVBMS ballot.

Results: Review of the requirement validated that the requirement was partially covered.

This testing was for the verification of transmissions to and from the VSAP 1.2 ISB RAVBMS voting ballot that is served from a hosted webserver, to the voter.

- Web Vulnerability scans were performed on the VSAP 1.2 ISB RAVBMS webserver to determine if there were any basic web server vulnerabilities in the initial serving of the in-browser application that houses the VSAP 1.2 ISB RAVBMS ballot.

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.

Testing performed: Testing was to confirm that this system

- Consists of a ballot produces a Poll Pass that is then taken to a vote center for processing on an actual ballot.
- Does not utilize specific telecommunications channels once the ballot has been downloaded and opened on the end voter's machine.

Results: Review of the requirement validated that the requirement was Satisfactorily covered.

Review of the requirement confirmed that VSAP 1.2 ISB RAVBMS system consists of a generated ballot which is typically used for mail in ballot marking. VSAP 1.2 ISB RAVBMS does not utilize specific telecommunications channels once the ballot has been downloaded and opened on the voter's machine.

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.

Testing performed: Testing was to confirm that the system notifies the user of successful or unsuccessful data transmission.

Results: This requirement was determined to be not applicable.

- The VSAP 1.2 ISB RAVBMS ballot marking system only allows the voter to mark and confirm marked ballots prior to printing and or saving out a ballot package.
- There are no live connections from the application to a remote server after the voter receives the generated ballot, except for one call from the browser to the server for graphics during the save/print functionality.
- All selections are cleared after browser has been closed, when the voter has completed the ballot marking process, and the poll pass has been printed and or saved.

Potential Vulnerabilities

For any potential vulnerabilities discovered, SLI was tasked with identifying the particular standards applicable to each vulnerability.

To the extent possible, reported vulnerabilities include an indication of whether the exploitation of the vulnerability would require access by a:

- Voter: Usually has low knowledge of the voting machine design and configuration. Some may have more advanced knowledge. May carry out attacks designed by others. They have access to the machine(s) for less than an hour.
- Poll worker: Usually has low knowledge of the voting machine design and configuration. Some may have more advanced knowledge. May carry out

attacks designed by others. They have access to the machine(s) for up to one week, but all physical security has been put into place before the machines are received.

- Elections official insider: Wide range of knowledge of the voting machine design and configuration. May have unrestricted access to the machine 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.
- Vendor insider: With great knowledge of the voting machine design and configuration. They have unlimited access to the machine 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.

SLI will not verify or demonstrate exploitability of the vulnerability but the report of the vulnerability will identify factors involved in the exploitation.

Any vulnerability theories developed by the security team shall, to the extent possible, be referred to the Secretary of State staff.

7.4.5 Software Reference Information

a. The manufacturer **shall** provide the 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.

   i. 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.

b. 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.

c. The manufacturers **shall** document to whom they provide voting system software.

No documented verification methods provided to ensure that the server that provides the application to the voter to generate his/her ballots is running unmodified code.

For the vulnerability in question, the level of access required to take advantage of this potential vulnerability would be inclusive to the following actors:

- Voter, who can attempt to modify the server code remotely.
- Election official insider, who could attempt to modify the server code remotely.
- Vendor Insider, who could attempt to locally modify the server code.

7.8 Testing – Security

For the vulnerabilities in question, the level of access required to take advantage of this potential vulnerability would be inclusive to the following actors:

- Voter
- Election official insider
- Vendor Insider

1**. Link Manipulation (DOM-Based)**
DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

2. **Unencrypted communications**
The application allows users to connect to it over unencrypted connections. An attacker suitably positioned to view a legitimate user's network traffic could record and monitor their interactions with the application and obtain any information the user supplies.

3. **Strict transport security not enforced**
The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users.

4. **Cross-domain script include**
When an application includes a script from an external domain, this script is executed by the browser within the security context of the invoking application. The script can therefore do anything that the application's own scripts can do, such as

accessing application data and performing actions within the context of the current user.

5. **Frameable response (potential ClickJacking)**
If a page fails to set an appropriate X-Frame-Options or Content-Security-Policy HTTP header, it might be possible for a page controlled by an attacker to load it within an iframe. This may enable a clickjacking attack, in which the attacker's page overlays the target application's interface with a different interface provided by the attacker. By inducing victim users to perform actions such as mouse clicks and keystrokes, the attacker can cause them to unwittingly carry out actions within the application that is being targeted. This technique allows the attacker to circumvent defenses against cross-site request forgery and may result in unauthorized actions.

Summary

The VSAP 1.2 ISB RAVBMS application is an application that allows voters to access Ballots remotely as controlled by the jurisdiction. The ballot once generated and accessed, is self-contained within the individual voter's browser. This means that once the initial server call for the application is processed the entire application runs in the current browser session. Since the application doesn't utilize incoming or outgoing connections once the ballot is loaded, this reduces the possibility of interception or manipulation through network attack vectors.

This however poses a risk of server-side compromise, to help mitigate this the vendor should provide high level documentation about the processes, procedures, and security to mitigate these risks. This documentation was not provided in an official documented form. The documentation should include but is not limited to:

- Secure hosting
- Physical security of hosting sites
- Network security
- Inventory and configuration management
- Access control
- Monitoring and logging
- Verification and validation of the certified software used for the deployment

Security testing of the server-side hosting security included, application scanning, and Nessus vulnerability scanning. The results of this scanning turned up a small selection of low and informational vulnerabilities that have minimal impact on the overall security of the applications being tested.

When the voter option to the security privacy question is “No” the voter privacy is ensured by removing client-side storage of marked selections in browser history, allowing the voter to verify a poll pass for saving or printing.

The ability to tamper with the client-side application is always present due to the fact there are no server-side verifications or validations in place after the ballot has been generated. In this context however the ability to affect large numbers of ballots is reliant upon server-side compromise (initial VSAP 1.2 ISB RAVBMS ballot launch) which may also include DDoS attacks and the failure of the vote by mail ballot system. The voter is given the ability to proof and confirm ballot selections within the VSAP 1.2 ISB RAVBMS interactive ballot system.

VSAP 1.2 ISB RAVBMS offers the voter the option to cache ballot selections, this allows the voter to close the browser and then return to the ballot at a later time and resume where the voter left off. This functionality only persists until the voter confirms and saves or prints their poll pass. At this point the browser’s persistent storage of selections is cleared. While this particular functionality doesn’t constitute a vulnerability by itself it does leave the cached browser selections vulnerable to unauthorized disclosure.

The VSAP 1.2 ISB RAVBMS doesn’t save or print out a full ballot it prints out a poll pass, which is then has to be returned to the elections official or taken to a polling place for duplication onto a traditional ballot. The poll pass is printed in the form of a QR code, that has the selections of each contest formatted in a 2-character code that corresponds with the candidate selection. Once the poll pass has been created there is no easily determined way that the QR-Code contains the proper selection until the voter uses the vote center to transfer vote selections to an official ballot.

As per the direction given by the California Secretary of State, this security testing report does not include any recommendation as to whether or not the system should be approved.

End of LAC VSAP 1.2 ISB RAVBMS Security and Telecommunications Test Report