County of Los Angeles
VSAP Interactive Sample Ballot 4.0 RAVBM
Security and Telecommunications Test Report

CAF-25015-STTP-01

Vendor Name	County of Los Angeles
Vendor System	VSAP ISB 4.0 RAVBM

Prepared by:

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

www.SLICompliance.com

Revision History

Date	Release	Author	Revision Summary
Jan. 23, 2026	v1.0	A. Nestico	Initial Release

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

This report outlines the testing SLI Compliance (SLI) followed when performing Security and Telecommunications Testing on the **Los Angeles County VSAP 4.0 Interactive Sample Ballot Remote Acessible Vote by Mail System** (**VSAP ISB 4.0 RAVBM**) system against the pertinent security modifications.

The **VSAP ISB 4.0 RAVBM** system enables the voter to mark their paper cast vote record using a secure web-based interface and generate and download a PDF representation of their selections. Voters then print their paper cast vote record and return it to their clerk.

Functional Security Testing

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

- 7.2.1 General Access Control
- 7.2.2 Access Control Identification
- 7.2.4 Access Control Authorization
- 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 testing was maintained.

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 performed to verify any implemented access control mechanisms functioned correctly for permitted authorized access, as well as prevention of unauthorized access.

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 performed 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.

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 performed to verify that the system prevents unauthorized access attempts.

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

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 performed 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 satisfactorily covered.

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

- The voter initially generates a blank paper cast vote record which does not contain voting selections.
- Once the blank paper cast vote record is delivered, all interactions remain local during all voter selection activities in the voter’s environment.

- As soon as the voter saves 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 websites.

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 paper cast vote record has been downloaded;
- There are no external connections from the paper cast vote record 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 ISB 4.0 RAVBM** does not have, nor require, internet access once the ballot selections have been downloaded. During the voter selection process there are no external connections from the ballot selections 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 performed 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.
- Used 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 Technical Data Package (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: Testing was performed to confirm that this system does not utilize telecommunications for the transmission of official voting data and that the system delivers a blank paper cast vote record 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 and that it delivers a blank paper cast vote record that does not contain voter data or choice selections.

Telecommunications and Data Transmission Testing

Testing of system communications, including encryption of data, as well as protocols and procedures for access authorization.

Tests were exercised in order to verify and validate telecommunications and data transmission in accordance with the following CVSS requirement:

- 6.1.2 Data Transmission

An issue log of any errors, anomalies, or omissions encountered during 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 performed to determine if there were any basic web server vulnerabilities in the initial serving of the in-browser application that houses the **VSAP ISB 4.0 RAVBM** paper cast vote record .

This testing was for the verification of transmissions to and from the **VSAP ISB 4.0 RAVBM** paper cast vote record that is served from a hosted webserver to the voter.

Web vulnerability scans were performed on the **VSAP ISB 4.0 RAVBM** webserver to determine if there were any basic web server vulnerabilities in the initial serving of the in-browser application that houses the **VSAP ISB 4.0 RAVBM** paper cast vote record.

Results: Review of the requirement validated that the requirement was partially covered. The following vulnerability was identified:

- Strict Transport Security Not Enforced: The application fails to prevent users from connecting to it over unencrypted connections. (Severity - Low)

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.

7.8 Testing Results – Security

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
- Election official insider
- Vendor Insider

1. Strict transport security not enforced

The application fails to prevent users from connecting to it over unencrypted connections.

Summary

The **VSAP ISB 4.0 RAVBM** allows voters to access paper cast vote record remotely as controlled by the jurisdiction. The paper cast vote record, 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 paper cast vote record 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 low severity vulnerability that has minimal impact on the overall security of the applications being tested.

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 ISB 4.0 RAVBM Security and Telecommunications Test Report