County of Los Angeles'
VSAP 1.2
Interactive Sample Ballot RAVBMS
Software Test Report
for California

CAF-19016-*SCRTR-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

Copyright ©2019 by SLI Compliance[SM], a Division of Gaming Laboratories International, LLC

Revision History

Date	Release	Author	Revision Summary
November 15, 2019	1.0	*M. Santos*	Initial Release
December 19, 2019	2.0	*M. Santos*	Updated for additional code release
December 27, 2019	3.0	*M. Santos*	Updated for CASOS 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

This report outlines the testing SLI Compliance (SLI) followed when performing Software Testing on the County of Los Angeles' VSAP 1.2 Interactive Sample Ballot Remote Access Vote by Mail System (VSAP 1.2 ISB RAVBMS) against the California Voting System Standards (CVSS).

The VSAP 1.2 ISB RAVBMS code versions for this release are

- ISB Preprocessor: 14608564ea5d
- ISB Client App: f14e4029238d

Coding languages involved in the VSAP ISB RAVBMS 1.2 application are shown in Table 1.

Table 1 – County of Los Angeles VSAP ISB RAVBMS 1.2 System Languages

Language	Lines of Code	Standard
Java Script	72,752	1. California Voting System Standards

Source Code Review Tools utilized by SLI included:

- Understand: a commercial application used to review code to stated requirements

REVIEW SPECIFICATIONS

The following are the specifications for source code testing conducted on the VSAP 1.2 ISB RAVBMS.

Software Test Review

The VSAP 1.2 ISB RAVBMS includes proprietary software, the code base was tested to the applicable CVSS requirements.

Review of the code included:

- Evaluating adherence to the applicable standards in sections 5 and 7 of the CVSS.
- Evaluating adherence to other applicable coding format conventions and standards including best practices for the coding language used.
- Analyzing the program logic and branching structure.

- Evaluating whether the system is designed in a way that allows meaningful analysis, 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

Security considerations reviewed against the code base included:

- Searching for exposures to commonly exploited vulnerabilities.
- Evaluating the use and correct implementation of cryptography and key management.
- Analyzing error and exception handling.
- Evaluating the likelihood of security failures being detected including:
  - whether audit mechanisms are reliable and tamper resistant
  - whether data that might be subject to tampering is properly validated and authenticated
- Evaluating the risk that a user can escalate his or her capabilities beyond those authorized.
- Evaluating the 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
  - Other adverse conditions
- Evaluating for embedded, exploitable code (such as “Easter eggs”) that can be triggered to affect the system.
- Evaluating the 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.
- Evaluating the code 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.

REVIEW RESULTS

Discrepancies

Discrepancies are reported such that the California Secretary of State is provided with a basis for evaluating the extent to which the source code meets applicable standards.

VSAP 1.2 ISB RAVBMS Software Test Review

- Evaluate adherence to the applicable standards in sections 5 and 7 of the CVSS
  - The expected outcome for this review was that no issue would be found.
  - The actual outcome for this review was a determination that no issue was found.
- Evaluate 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 no issue was found.
- Analyze the program logic and branching structure
  - The expected outcome for this review was that no issue would be found.
  - The actual outcome for this review was a determination that no issue was found.
- Evaluate whether the system is designed in a way that allows meaningful analysis, 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 for this review was that no issue would be found.
    - The actual outcome for this review was a determination that no issue was found.

Security considerations reviewed against the code base included:

- Evaluate the use and correct implementation of cryptography and key management
    - The expected outcome for this review was that no issue would be found.
    - The actual outcome for this review was a determination that no issue was found.
- Analyze error and exception handling
    - The expected outcome for this review was that no issue would be found.
    - The actual outcome for this review was a determination that no issue was found.
- Evaluate the likelihood of security failures being detected including:
    - The expected outcome for this review was that audit mechanisms would be determined to be reliable and tamper resistant, and that any data that might be subject to tampering is properly validated and authenticated.
    - The actual outcome for this review was a determination that audit mechanisms are properly implemented to be reliable and tamper resistant and evident, as well as that data that might be subject to tampering is properly validated and authenticated.
- Evaluate the risk that a user can escalate his or her capabilities beyond those authorized
    - The expected outcome for this review was that no issue would be found.
    - The actual outcome for this review was a determination that no issue was found.
- Evaluate the 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
    - Other adverse conditions
        - The expected outcome for this review was that no issue would be found.
        - The actual outcome for this review was a determination that no issue was found.

- Evaluate 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 issue would be found.
    - The actual outcome for this review was a determination that no issue was found.
- Evaluate the code 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 issue would be found.
    - The actual outcome for this review was a determination that no issue was found.

No software code requirements were found to be at issue within the VSAP 1.2 ISB RAVBM source code base reviewed. As a result, no 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 include an indication of whether the exploitation of the vulnerability would require access by:

- Voter: Usually has low knowledge of the voting technology design and configuration. Some may have more advanced knowledge. May carry out attacks designed by others.
- Elections official insider: Wide range of knowledge of the voting technology design and configuration. May have unrestricted access to voting technology 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 voting technology design and configuration. They have unlimited access to voting technology 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 source code review team members shall, to the extent possible, be referred to the Secretary of State staff.

VSAP 1.2 ISB RAVBMS Software Code Vulnerability Review

The source code was reviewed for exposures to commonly exploited vulnerabilities, such as buffer overflows, integer overflow, inappropriate casting or arithmetic.

- The expected outcome was that no issue would be found.
- The actual outcome was a determination that no issues were found.

The source code was reviewed for evaluation of potential vulnerabilities and related issues (code quality and standards compliance), considering that an exploitable issue in a component that is not in itself security relevant could be used to subvert more critical data. This is an issue whenever the architecture of the system does not provide strong separation of the components.

- The expected outcome for this review was that no issue would be found.
- The actual outcome for this review was a determination that no issues were found.

The source code was reviewed for evaluation for dynamic memory access features which would permit the replacement of certificated executable code or control data or insertion of exploitable code or data.

- The expected outcome for this review was that no issue would be found.
- The actual outcome for this review was a determination that no issues were found.

No vulnerabilities were identified within the **VSAP 1.2 ISB RAVBMS** code base.

Final Report

No discrepancy findings were determined for the **VSAP 1.2 ISB RAVBMS** code base.

No vulnerabilities were identified within the **VSAP 1.2 ISB RAVBMS** code base.

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

End of **VSAP 1.2 ISB RAVBMS** Software Test Report