County of Los Angeles VSAP Tally 1.0 Central Tabulation System Source Code Review Test Report for California

LAC-18001-SCRTR-01

Prepared for:

Vendor Name	County of Los Angeles
Vendor System	VSAP Tally 1.0

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 ©2018 by SLI Compliance^{SM}, a Division of Gaming Laboratories International, LLC

Revision History

Date	Release	Author	Revision Summary
7.11.2018	1.0	*M. Santos*	Initial Release
7.12.2018	1.1	*M. Santos*	Update for code version listing
7.16.2018	1.2	*M. Santos*	Updates 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 Tally 1.0 (VSAP Tally 1.0) system against the California Voting System Standards (CVSS).

The VSAP Tally 1.0 system consists of a central, high-speed, optical scan ballot counter (tabulator) and is used for processing ballots. This ballot counter unit is based on commercial off the shelf (COTS) hardware coupled with custom-made ballot processing application software. It is used for high-speed, accurate, and reliable centralized scanning and counting of paper ballots.

The VSAP Tally 1.0 code version for this release is "v1.1.2.2".

REVIEW SPECIFICATIONS

The following are the specifications for source code testing conducted on the VSAP Tally 1.0 system.

Source Code Review

The VSAP Tally 1.0 system includes proprietary software and firmware. The VSAP Tally 1.0 voting system code base was tested to the applicable CVSS requirements.

Review of the code included:

- Evaluate adherence to the applicable standards in sections 5 and 7 of the CVSS
- Evaluate adherence to other applicable coding format conventions and standards including best practices for the coding language used
- Analyze the program logic and branching structure
- Evaluate whether the system is designed in a way that allows meaningful analysis, including:
  - o Whether the architecture and code is amenable to an external review
  - o Whether code analysis tools can be usefully applied
  - o Whether the code complexity is at a level that obfuscates its logic

Security considerations reviewed against the code base included:

- Search for exposures to commonly exploited vulnerabilities
- Evaluate the use and correct implementation of cryptography and key management
- Analyze error and exception handling

- Evaluate the likelihood of security failures being detected including:
  - o Evaluate whether audit mechanisms are reliable and tamper resistant
  - o Evaluate whether 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
- Evaluate the design and implementation to ensure that sound, generally accepted engineering practices are followed, checking to verify that code is defensively written against:
  - o Bad data
  - o Errors in other modules
  - o Changes in environment
  - o User errors
  - o Other adverse conditions
- Evaluate for embedded, exploitable code (such as "Easter eggs") that can be triggered to affect the system
- Evaluate 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.
- 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.

Coding languages involved in the VSAP Tally 1.0 application are shown in Table 1.

Table 1 – County of Los Angeles VSAP Tally 1.0 System Components

Language	Lines of Code	Tally 1.0 Code Version	Standard
GO	100,000	1.1.2.2	1. California Voting System Standards 2. The Go Programming Language Specification (golang.org/ref/spec) 3. Effective Go(golang.org/doc/effective_go.html)

Source Code Review Tools utilized by SLI included:

- Module Finder: an SLI proprietary application used to parse module names from C/C++ and VB code and populate the identified module names into the review documents
- Understand: a commercial application used to review code to stated requirements

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 Tally 1.0 Source Code Review

No source code requirements were found to be at issue within the VSAP Tally 1.0 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 Tally 1.0 source code vulnerability review

No vulnerabilities were identified within the VSAP Tally 1.0 code base.

Final Report

No discrepancy findings were determined for the VSAP Tally 1.0 code base.

No vulnerabilities were identified within the VSAP Tally 1.0 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.

<div align="center">

End of VSAP Tally 1.0 Software Test Report

</div>