ALEX PADILLA | SECRETARY OF STATE | STATE OF CALIFORNIA
OFFICE OF VOTING SYSTEMS TECHNOLOGY ASSESSMENT
1500 11th Street | Sacramento, CA 95814 | **Tel** 916.695.1680 | **Fax** 916.653.4620 | www.sos.ca.gov

County of Los Angeles
Voting Solutions for All People (VSAP) Tally 1.0

Staff Report

Prepared by:
Secretary of State's
Office of Voting Systems Technology Assessment

July 13, 2018

Table of Contents

I. Introduction 1

1. Scope 1
2. Summary of the Application 1
3. Contracting and Outsourcing 1

II. Summary of the System 2

1. VSAP Tally System, v. 1.1.2.2 2
2. IBML ImageTrac Scanner, v. 6400 2

III. Testing Information and Results 2

1. Background 2
2. Functional Testing Summary 3
3. Software (Source Code) Testing Summary 5
4. Security and Telecommunications Testing Summary 5
5. Volume Testing Summary 18

IV. Compliance with State and Federal Laws and Regulations 20

V. Conclusion 26

ALEX PADILLA | SECRETARY OF STATE | STATE OF CALIFORNIA
OFFICE OF VOTING SYSTEMS TECHNOLOGY ASSESSMENT
1500 11th Street | Sacramento, CA 95814 | **Tel** 916.695.1680 | **Fax** 916.653.4620 | www.sos.ca.gov

I. INTRODUCTION

1. Scope

This report presents the test results for all phases of the certification test of the County of Los Angeles' VSAP Tally 1.0. The purpose of the testing is to test the compliance of the voting system with California and Federal laws, including the California Voting System Standards (CVSS). 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. The procedures for mitigating any additional findings are made to the documentation, specifically the County of Los Angeles Use Procedures.

2. Summary of the Application

The County of Los Angeles submitted an application for the VSAP Tally 1.0 central tabulation system on September 19, 2017. The system is comprised of the following major components:

- Voting Solutions for All People (VSAP) Tally software, version 1.1.2.2;
- IBML ImageTrac Scanner, version 6400

In addition to these two components, which includes the executable code and the source code, the County of Los Angeles was required to submit the following: 1) the technical documentation package (TDP); 2) all the hardware components to including all peripheral devices needed for the Functional Test Phase the Security and Telecommunications Test Phase; 3) and the VSAP Tally Blended Use Procedures.

3. Contracting and Consulting

Upon receipt of a complete application, the Secretary of State released a Request for Quote (RFQ) for assistance with the Software Testing (Source Code Review) and Security and Telecommunications testing.

Through the formal California contracting process, the Secretary of State awarded a contract to SLI Compliance (SLI), a division of Gaming Laboratories International, LLC.

II. SUMMARY OF THE SYSTEM

The VSAP Tally 1.0 solution is solely used for scanning and tabulating ballots. The intent of use for this iteration is to process vote by mail (VBM) ballots. The system will be used in a blended environment, with the County of Los Angeles' legacy system Microcomputer Tally System (MTS) version 1.3.1 using InkaVote ballots, which will tabulate precinct ballots.

The system consists of two components:

1. Voting Solutions for All People (VSAP) Tally software, version 1.1.2.2

The VSAP Tally is a central tabulation software solution. The VSAP Tally system as described in the Los Angeles County 2018 Blended Use Procedures is a transition to scanning technology of digital image that then processes the ballot into Cast Vote Records (CVR).

2. IBML ImageTrac Scanner, version 6400

The IBML ImageTrac is a commercial off-the-shelf (COTS) document scanner. The scanner provides the following functionality for the system:

- Scans 10,000 ballots per hour
- Out stacks documents that do not have or are unable to read QR codes and 1d Barcodes.
- Pre-Print ballot id, name the digital image with the ballot id and scan in the same process.

III. TESTING INFORMATION AND RESULTS

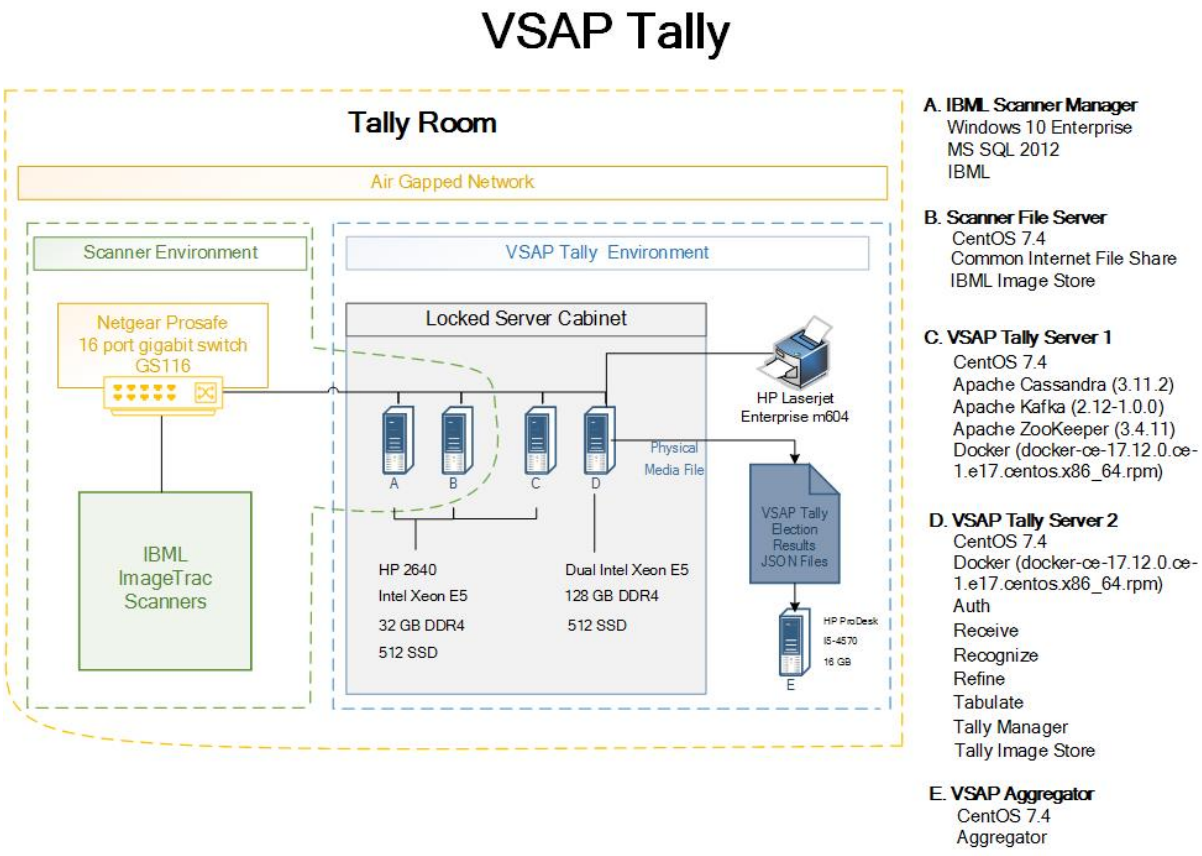
1. Background

Functional and Volume testing of this system was conducted by Secretary of State Staff, in Norwalk, California, from May 23 to May 25, 2018. The configuration of the equipment, including a build from the ground up, was witnessed by Secretary of State Staff on May 23, 2018, using the configuration procedures provided by the County of Los Angeles. Software testing (Source Code Review) was performed by SLI Compliance June 11 to July 12, 2018. Security and Telecommunications testing was performed in Norwalk, California from July 2 to July 3, 2018. Accessibility for this iteration of the VSAP Tally system will be addressed by the County of Los Angeles internal procedures for employee accessibility. This version is solely for the tabulation of vote-by-mail ballots and exclusively for the use of Los Angeles County election employees.

2. Functional Testing Summary

System Configuration:

Preparation for Functional Testing and all subsequent testing began on May 23, 2018. The system is self-contained on an air gapped network, per the CVSS requirements. Secretary of State staff witnessed the build of the test environment utilizing the vendor provided Use Procedures, which included installation of the operating system, commercial-off-the-shelf (COTS) software, tabulation software, and hardening of the system.



Issues & Observations

During the configuration build, each time the system is built it requires installing the latest updates for the operating system.

a. Documentation

The documentation was subsequently modified and the changes verified by the Secretary of State staff.

Phase I - Functional Testing

The first phase of Functional Testing consisted of following the Use Procedures to configure test elections. The testing included defining three (3) different test election definitions.

The election type definitions, jurisdictions, and any anomalies noted are listed in the table below:

Table 2A: Election Definitions

Election Type	Jurisdiction	Anomaly Identified	Resolution
General	Los Angeles County	None	N/A
Primary – Countywide Vote Center Model	Los Angeles County	• Reports – Treasurer Contest count came out 2/4, instead of 4/4. • Ballot Out Stack – Superintendent of Education and Measure I. One ballot had debris that could not be seen with naked eye, but the scanner picked it up a valid count.	Sensitivity settings were adjusted in the configuration file. The ballot was rerun five (5) times, and each time it came out clear after making the adjustment.
Recall Election - Fictional Contest with 72 Candidates and Yes/No Recall Question	Los Angeles County	None	N/A

3. Software Testing (Source Code) Review Summary

The review was conducted at the SLI Compliance offices located in Wheat Ridge, Colorado. SLI evaluated the security and integrity of the voting system, by identifying any security vulnerabilities that could be exploited to:

- Alter vote recording,
- Alter vote results,
- Alter critical data (such as audit logs), or
- Conduct a "denial of service" attack on the voting system.

There were no discrepancy findings or vulnerabilities identified within the VSAP Tally 1.1.2.2 code base.

4. Security and Telecommunications Testing

Security and Telecommunications testing of the VSAP Tally system was conducted from July 2 to July 3, 2018, by SLI Compliance. The security and telecommunications testing was conducted in four phases as follows:

- Phase I – Security Documentation Review
- Phase II – Functional Security Testing
- Phase III – Telecommunications and Data Transmission Testing
- Phase IV – Onsite Security Testing

Phase I – Security Documentation Review

SLI Compliance reviewed the security documentation supplied by Los Angeles County, and determined there were no vulnerabilities with the documentation. SLI did note that there were some improvements, five (5) minor findings with vague or partially missing documentation.

Table 4A: Security Documentation Review

Test Results	Vendor Mitigation/Response
CVSS 7.4.6 – Documentation is only present to validate VSAP Tally Containers and Trusted Build outputs, and base package installation of COTS software. Detailed documentation for validation of all storage locations associated with election specific information was missing.	The Following locations must exist and be writable by the system: /opt/mounts (mounted into docker) /opt/tally (scripts, configuration) /mount/ballots The following must exist but should not be writeable: /var/lib/docker

Table 4A: Security Documentation Review	
Test Results	**Vendor Mitigation/Response**
	/mount/ballots should also have sufficient room for all the ballot images that will be generated in the election with sufficient safety margin.
CVSS 7.4.5 – Documentation was present for creation of a build environment for the VSAP Tally solution as well as building the environment; however, the documentation has limited references as to how software is distributed and where the certified copy of the software will be stored. There is mention in the documentation that the solution will only be used by LA County.	VSAP Tally System Version 1.1.2.2 is designed for internal use by Los Angeles County only. It will only be installed in the County's secure central count facility and will not be distributed to any other locations. Prior to installation in the central count facility, a copy of the software will be obtained from a software escrow company certified with the California Secretary of State and the security hashes for the download will be validated.
CVSS 7.4.4.b – There is reference to parts of the system being considered static, dynamic or a mix of both, the list of files was not complete or extensive.	A more complete list of files will be compiled and provided.
CVSS 7.4.2 – Documentation was present indicating that due to performance requirements the solution will not actively utilize COTS anti-virus software during operation of the solution. There are, however, supplemental mitigation steps including anti-virus and vulnerability scanning of the environment systems prior to being introduced to an air gapped network.	County will perform malware/anti-virus and vulnerability scanning after system installation in the air-gapped environment. In addition, an offline scan will be performed prior to each batch processing of production ballots for every election.
CVSS 7.4.1 – Documentation was provided that describes the basic overall features requirements and processes for creation and management of an air gapped network. In some cases it is detailed, such has how to update software or firmware on	In the VSAP Tally System Air-Gap Setup document provided, Los Angeles County has documented the procedure to setup an air-gap network and configure all connected devices in the County central facility.

Table 4A: Security Documentation Review	
Test Results	**Vendor Mitigation/Response**
the air gapped systems and software without internet connectivity. No full procedure for a start to finish air gapped network implementation including hardware connectivity is available.	

Phase II – Functional Security Testing

Functional Security Testing includes testing the relevant software and operating system configuration for vulnerabilities, and testing of the hardware, including examination of unused hardware ports and security measures applied to those ports. Functional Security Testing also included verifying the VSAP Tally system meets the applicable requirements of the CVSS.

Table 4B: Functional Security Testing Findings lists the applicable sections of the CVSS, in addition to the findings of the testing conducted by SLI. A response to those findings is also included by the County of Los Angeles.

Table 4B: Functional Security Testing Findings	
Test Results	**Vendor Mitigation/Response**
CVSS 7.4.2 – The actual outcome for this review was a determination that during operations, the systems within the Scanner environment as well as the systems within the VSAP Tally environment do not actively use COTS anti-virus protection. The system instead utilizes initial malware/anti-virus and vulnerability scanning prior to the systems being introduced to the air gapped network. These are mitigation steps that are being relied upon instead of active malicious software protection.	County will perform malware/anti-virus and vulnerability scanning after system installation in the air gapped environment. In addition, an offline scan will be performed prior to each batch processing of production ballots for every election.
CVSS 7.4.6 – • The actual outcome for this review was a determination that there are validation methods to verify the VSAP Tally 1.0 trusted build output as well as a JSON file created with a list of every	VSAP Tally System Version 1.1.2.2 is designed to be installed and operated in an environment with tight physical controls. There is no external network connection to allow processes to access external software. VSAP Tally System Version 1.1.2.2 is not

Table 4B: Functional Security Testing Findings	
Test Results	**Vendor Mitigation/Response**
container generated by the build process and a corresponding hash value. Each of the COTS products contain a hash of the single COTS file installation file(s). This indicates that the software validation is done prior to the installation of the system. • The actual outcome for this review was a determination that there are processes and procedures for creation of SHA512 Hash codes during the trusted build for both the system build outputs and SHA256 hashes of each of the Docker service containers. All COTS Software contains verifiable HASH values to validate that the correct version of the software is installed. • The system has no protections to prevent processes from installing software except for manual processes and procedures and physical security and access controls to prevent unauthorized installation. • The VSAP Tally 1.0 system utilizes processes and procedures and physical security and access controls to prevent previous versions of the system from being installed. • The software update package is not digitally signed. • The Solution doesn't currently utilize an automated process to prevent unwanted installations • The system doesn't have a way to provide a verification method of all system storage locations, only the VSAP Tally 1.0 solution, and the COTS products installers.	designed for distribution and will only be used by Los Angeles County in a tightly-controlled environment. Physical, administrative, and management controls that include strict supervision and monitoring of staff activity while operating the Tally System and the prohibition of wireless phones\devices and unverified removable media in the secure Tally room are some of the mitigation measures that will be implemented to ensure integrity of the air gapped network.

Table 4B: Functional Security Testing Findings	
Test Results	**Vendor Mitigation/Response**
CVSS 7.6.1 – • The actual outcome for this review was a determination that portions of this requirement are not applicable. The system scans already marked ballots which are then processed by the VSAP Tally system. • No checksums or message digests are used to validate scanned ballot images. • Manual recount procedures, California State required one percent manual recount procedures, physical security measures and a tightly controlled air gapped network are all mitigating measures in place.	Ballot security and accountability is critically important for the County. Each ballot has a QR Code with election-specific information encoded, which VSAP Tally reads to ensure the ballot is valid in the current election. Additionally, controls are implemented as part of the Use Procedures to inspect all ballots prior to tabulation and to ensure only valid official ballots are sent to VSAP Tally for processing.
CVSS 7.8.2 - • The actual outcome for this review was a determination that the solution sufficiently protects against data interception and disruption. • The solution currently does not provide end to end transmission security. The VSAP Tally 1.0 solution utilizes encryption of data transmissions between Application containers for image processing and reporting. The connection between the IBML Scanner and the CIFS file share, however, is not transmitted using encryption. • Stringent attention to maintaining the air gapped scanner and Tally environment removes the ability to intercept or modify results as they are being scanned and processed.	Physical, administrative, and management controls that include strict supervision and monitoring of staff activity while operating the Tally System and the prohibition of wireless phones\devices and unverified removable media in the secure Tally room are some of the mitigation measures that will be implemented to ensure integrity of the air gapped network. A major feature of this network is that the network switch being used is configured to only allow one device per port and locks that port to the device's mac address.

Phase III – Telecommunications and Data Transmission Testing

Telecommunications and Data Testing included testing of system communications, including encryption of data, as well as protocols and procedures for access authorization. **Table 4C** list the results of that testing.

Table 4C: Telecommunications and Data Transmission Vulnerabilities		
Issue	**Consultant Assessment**	**Vendor Mitigation/Response**
Cross Site Scripting (DOM-based)	(High Severity) (Tentative confidence) Potentially a false positive as the confidence is set to tentative.	Cross Site Scripting requires having another (malicious) site accessible on the network. This is prevented by strict enforcement of the air gapped network environment and security protocols.
SSL Certificate	(Medium severity) (Certain confidence). Server's certificate is not valid for the server's hostname, and the server certificate is not trusted. This error has little to no impact to the overall security of the solution due to the nature of the air gapped trusted network.	As noted, this issue is mitigated by the strict enforcement of the air gapped network environment and security protocols.
Client-side JSON injection (DOM-based)	(Low Severity) (Firm Confidence). DOM-based JSON injection may happen when a script includes controllable data into a string that is parsed as a JSON data structure and then processed by the application.	Strict enforcement of the air gapped network environment and security protocols should provide sufficient protection against DOM-based attacks.
Transport security	(Low Severity) (Certain confidence). This allows a potential attacker to modify legitimate user network traffic to bypass application use of SSL/TLS encryption.	Strict enforcement of the air gapped network environment and security protocols should provide sufficient protection against these types of attacks.
Informational Vulnerabilities	These vulnerabilities are of an informational nature and include recon information that helps to identify the system, including open ports, OS type and version and services detected. The vulnerabilities explored and	Although as noted these vulnerabilities are believed to be negligible, they are mitigated by the strict enforcement of the air gapped network environment and security protocols.

	detected are believed to be negligible and have little or no impact on the overall security of the system.	

SLI reported three (3) categorical findings during the Telecommunications and Data Transmission Testing of the VSAP Tally 1.0 system. SLI's determination was that, the overall security posture of the system as a whole is minimal. The findings are listed below in **Table 4D**.

Table 4D: Telecommunications and Data Transmission Categorical		
Issue	**Consultant Assessment**	**Vendor Mitigation/Response**
Six (6) medium severity vulnerabilities	1. SMB signing not required 2. SSL Certificate cannot be trusted 3. SSL Certificate signed using weak hashing algorithm 4. SSL certificate with wrong host name 5. SSL medium strength cipher suites supported 6. SSL Self-signed Certificate	VSAP Tally operates in an air gapped network. Strict access controls and physical security mitigation measures are implemented to ensure the integrity of the air gapped environment.
Two (2) low severity vulnerabilities	1. SSH Server CBC mode ciphers enabled 2. SSL RC4 cipher suites supported.	VSAP Tally operates in an air gapped network. Strict access controls and physical security mitigation measures are implemented to ensure the integrity of the air gapped environment.
Fifty (50) informational severity vulnerabilities.	These vulnerabilities are of an informational nature and include recon information that helps to identify the system, including open ports, OS type and version and services detected. The vulnerabilities explored and detected are believed to be negligible and have little or no impact on the overall security of the system.	Although as noted these vulnerabilities are believed to be negligible, they are mitigated by the strict enforcement of the air gapped network environment and security protocols.

Phase IV – Onsite Security Testing

The Onsite Security Testing consisted of testing for relevant software and operating system configuration for vulnerabilities, testing of hardware, including the examination of unused ports and the security measures applied to the ports, in addition to examination of the physical environment. The applicable portions of CVSS and the results of the Onsite Security Testing are listed in **Table 4E**.

Table 4E: Onsite Security Testing		
CVSS Standard	**Result**	**Vendor Mitigation/Response**
CVSS 5.4.3 - a. Machine generated error and exception messages to demonstrate successful recovery. iv. Notification of system login or access errors, file access errors, and physical violations of security as they occur, and a summary record of these events after processing	The actual outcome for this review was a determination that the system generates and contains sufficient auditing capability. This includes VSAP Tally 1.0 logs, Centos Operating System logs, Windows OS logs, ImageTrac logs.	N/A
CVSS 7.2.1 – 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 Election Management System (EMS) **shall** be capable of identifying and authenticating individuals permitted to perform operations on the EMS. b. Voting system equipment **shall** provide controls that	The actual outcome for this review was a determination that the system sufficiently provides access controls for the VSAP Tally 1.0 solution, as well as the systems that are associated with the solution. The system has processes and procedures in place to prevent modification/tampering with software/firmware, as well as physical security including an air gapped network.	N/A

Table 4E: Onsite Security Testing		
CVSS Standard	**Result**	**Vendor Mitigation/Response**
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.		
CVSS 7.2.2 – 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. b. Voting system equipment that implements role-based access control **shall** support the recommendations for Core RBAC in the ANSI INCITS 359-2004 American National Standard for Information Technology- Role Based Access Control document. c. Voting system equipment	The actual outcome for this review was a determination that the access controls are sufficient for all portions of the VSAP Tally 1.0 environment, including Scanner environment.	N/A

Table 4E: Onsite Security Testing		
CVSS Standard	**Result**	**Vendor Mitigation/Response**
shall allow the administrator group or role to configure the permissions and functionality for each identity, group, or role to include account and group/role creation, modification, and deletion.		
CVSS 7.3 – a. Voting system equipment **shall** authenticate users prior to granting them access to system functions or data. b. When private or secret authentication data is stored in voting system equipment, the data **shall** be protected to ensure that the confidentiality and integrity of the data is not violated. c. Voting system equipment **shall** allow the administrator group or role to set and change passwords, pass phrases, and keys. d. Voting system equipment **shall** allow privileged groups or roles to be disabled and allow new individual privileged groups or roles to be created. e. Voting system equipment **shall** lock out groups, roles, or individuals after a specified number of consecutive failed authentication attempts within a predefined time period. f. Voting systems **shall** allow the administrator group or role to configure the account lock out policy, including the time	The actual outcome for this review was a determination that all username password functionality is maintained by an administrative source. Complex passwords, lockout history, complexity requirements, and expiration of passwords can all be enforced at the operating system level and at the ImageTrac scanning software which sufficiently meets the requirements.	N/A

Table 4E: Onsite Security Testing		
CVSS Standard	**Result**	**Vendor Mitigation/Response**
period within which failed attempts must occur, the number of consecutive failed access attempts allowed before lock out, and the length of time the account is locked out. g. If the voting system uses a user name and password authentication method, the voting system **shall** allow the administrator to enforce password strength, histories, and expiration. h. The voting system **shall** allow the administrator group or role to specify password strength for all accounts, including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters. i. The voting system **shall** enforce password histories, and allow the administrator to configure the history length. j. Voting system equipment **shall** ensure that the username is not used in the password. k. Voting systems **shall** provide a means to automatically expire passwords in accordance with the voting jurisdiction's policies. l. Manufacturers **shall** develop and document in detail the measures to be taken in a central counting environment. These measures **shall** include physical and procedural		

Table 4E: Onsite Security Testing		
CVSS Standard	**Result**	**Vendor Mitigation/Response**
controls related to the handling of ballot boxes, preparing of ballots for counting, counting operations and reporting data.		
CVSS 7.3.2 – Manufacturers **shall** develop and document in detail the measures to be taken in a central counting environment. These measures **shall** include physical and procedural controls related to the handling of ballot boxes, preparing of ballots for counting, counting operations and reporting data.	The actual outcome for this review was a determination that the solution fully documents and implements processes and procedures for securing the central count location. These include physical security measures, procedural controls for maintaining the Air Gap network, protection and handling of ballots, and reporting of data. Observation: No specific details pertaining to the security measures to network switching equipment. Security practices for the air gapped network were observed that help to enhance the overall security of the solution but were not documented anywhere in the requirements. Observation: There is reference to maintaining tamper-evident seal numbers multiple times throughout the documentation; however, there is no direct reference to the tamper evident seal log that was in use. Documentation of the procedures for	In the VSAP Tally System Air-Gap Setup document provided, Los Angeles County has documented the procedure to setup an air-gap network and configure all connected devices in the County central facility. In the VSAP Tally System Tamper-Evident Seals Procedures document provided, Los Angeles County has documented how it intends to log the use tamper-evident seals as a security measure.

Table 4E: Onsite Security Testing		
CVSS Standard	**Result**	**Vendor Mitigation/Response**
	maintaining such a log including where it's stored and who has access to the log is needed.	
CVSS 6.1.2 – 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	The actual outcome for this review was a determination that the system sufficiently meets the requirements for data transmission. Testing included Nessus® Vulnerability scans against all connected equipment, as well as physical inspection of the networking equipment connected to the air gapped network.	N/A
CVSS 7.8.1–	The actual outcome for this review was a	N/A

Table 4E: Onsite Security Testing		
CVSS Standard	**Result**	**Vendor Mitigation/Response**
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	determination that the solution successfully meets the requirements for access control.	

Table 4E: Onsite Security Testing		
CVSS Standard	**Result**	**Vendor Mitigation/Response**
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		
CVSS 7.8.2 – 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 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.	The actual outcome for this review was a determination that the solution sufficiently protects against data interception and disruption. The utilization of a physically protected air gapped network helps improve a solution that only employs encryption of data transmissions between application containers for image processing and reporting and not all communications. The connection between the IBML Scanner and the CIFS file share is not currently encrypted. Stringent attention to maintaining the air gapped scanner and Tally environment removes the ability to intercept or modify results as they are being scanned and processed.	Physical, administrative, and management controls that include strict supervision and monitoring of staff activity while operating the Tally System and the prohibition of wireless phones\devices and unverified removable media in the secure Tally room are some of the mitigation measures that will be implemented to ensure integrity of the air gapped network. A major feature of this network is that the network switch being used is configured to only allow one device per port and locks that port to the device's mac address.

SLI determined there were three (3) findings and two (2) observations during the Onsite Security Testing Phase. SLI concluded the impact to the overall security posture of the solution as a whole is minimal.

5. Volume Testing Summary

The Volume Test simulates conditions in which the system components would be used on Election Day. Volume Testing of the VSAP Tally system took place in Los Angeles County, on May 24, 2018. Test ballots from the California 2014 General Election were scanned for over seven (7) hours. The use of this election required an edit of the configuration file within the Tally system.

Table 5A: Machine and Ballot Count

Hardware Component	Number of Machines	Number of Ballots per Machine	Ballot Pages	Total for All Machines
IBML Scanner	1	2,998	Two (2)	5,996

Table 5B: Error Log

Hardware Component	Error Type	Error Occurrence Frequency	Mitigation
IBML Scanner	"Gap Violation" – The scanner is sensitive to the amount of spacing between ballots in the feeder.	Ten (10)	The use procedures and operator cards at the scanner will remind operators of the scanner that adequate spacing between the ballots in the feeder is necessary.
IBML Scanner	"Double Feed Error" – Two ballots were stuck together.	One (1)	IBML suggested adjustments to the scanner to alleviate gap and double

Table 5B: Error Log			
Hardware Component	**Error Type**	**Error Occurrence Frequency**	**Mitigation**
			feed errors. Those suggestions were incorporated into the daily maintenance routine; operators will follow during the tally process. Additionally, operators should utilize a "ballot jogger". Use procedures will address this issue.
IBML Scanner	"Document too long error"	One (1)	Ballot was pulled off of track and delicately hand fed into the scanner.
IBML Scanner	Ballot Out stacked	One (1)	Slight fold in the corner of ballot, covering the registration mark. Use procedures will address this issue.

IV. COMPLIANCE WITH STATE AND FEDERAL LAWS AND REGULATIONS

The following are the applicable California Elections Code sections that the Secretary of State tested the County of Los Angeles' VSAP Tally 1.0 central tabulation voting system against. The list is broken down by Elections Code Section, language quoted from the section and how the system complies with the section.

10264 - As soon as the result of the election is declared, the elections official of the governing body shall enter on its records a statement of the result. The statement shall show: (a) The whole number of votes cast in the city. (b) The names of the persons voted for. (c) The measures voted upon. (d) For what office each person was voted for. (e) The number of votes given at each precinct to each person and for and against each measure. (f) The number of votes given in the city to each person and for and against each measure.

The central tabulation voting system has the capability to produce the required report(s).

10550 - As soon as the result of the canvass by the county elections official is declared, the county elections official shall prepare and mail a statement of the result to the secretary of each district participating in the general district election. The statement shall be signed by the county elections official, authenticated by the seal of the county and shall show: (a) The number of ballots cast for elective offices of that district and, when directors of that district are elected by divisions, the number of ballots cast in each division. (b) The name of each candidate for an elective office of that district voted for and the office. (c) The number of votes cast in each precinct for each candidate. (d) When directors are elected by divisions, the number of votes cast in each division for each candidate for the office of director from that division. (e) The number of votes cast in the district for all other elective offices of that district.

The central tabulation voting system has the capability to produce the required report(s).

15101(b) - Any jurisdiction having the necessary computer capability may start to process vote by mail ballots on the seventh business day prior to the election. Processing vote by mail ballots includes opening vote by mail ballot return envelopes, removing ballots, duplicating any damaged ballots, and preparing the ballots to be machine read, or machine reading them, but under no circumstances may a vote count be accessed or released until 8 p.m. on the day of the election. All other jurisdictions shall start to process vote by mail ballots at 5 p.m. on the day before the election.

The central tabulation voting system has the capability to meet this requirement.

15101(c) - Results of any vote by mail ballot tabulation or count shall not be released prior to the close of the polls on the day of the election.

The central tabulation voting system has the capability to scan, but not tabulate or report the results prior to the close of polls on Election Day.

15109 - Except as otherwise provided in this chapter, the counting and canvassing of vote by mail ballots shall be conducted in the same manner and under the same regulations as used for ballots cast in a precinct polling place.

The central tabulation voting system has the capability to meet this requirement.

15110 - Reports to the Secretary of State of the findings of the canvass of vote by mail ballots shall be made by the elections official pursuant to Chapter 3 (commencing with Section 15150) and Chapter 4 (commencing with Section 15300).

The central tabulation voting system has the capability to produce the required report(s).

15150 - For every election, the elections official shall conduct a semifinal official canvass by tabulating vote by mail and precinct ballots and compiling the results. The semifinal official canvass shall commence immediately upon the close of the polls and shall continue without adjournment until all precincts are accounted for.

The central tabulation voting system has the capability to meet this requirement.

15151(a) - The elections official shall transmit the semifinal official results to the Secretary of State in the manner and according to the schedule prescribed by the Secretary of State prior to each election, for the following: (1) All candidates voted for statewide office. (2) All candidates voted for the following offices: (A) State Assembly. (B) State Senate. (C) Member of the United States House of Representatives. (D) Member of the State Board of Equalization. (E) Justice of the Court of Appeals. (3) All persons voted for at the presidential primary or for electors of President and Vice President of the United States. (4) Statewide ballot measures.

The central tabulation voting system has the capability to produce the required report(s).

15152 - Neither the elections official, any member of a precinct board, nor any other person shall count any votes, either for a ballot proposition or candidate, until the close of the polls in that county. After that time, the ballots for all candidates and ballot propositions voted upon solely within the county shall be counted and the results of the balloting made public. However, the results for any candidate or ballot proposition also voted upon in another county or counties shall not be made public until after all the polls in that county and the other county or counties have closed. This paragraph applies regardless of whether the counting is done by manual tabulation or by a vote tabulating device.

The central tabulation voting system has the capability to scan, but not tabulate or report the results prior to the close of polls on Election Day.

15153 - During the semifinal official canvass, write-in votes shall be counted in accordance with Article 3 (commencing with Section 15340) of Chapter 4.

The central tabulation voting system has the capability to meet this requirement.

5212 - If voting at all precincts within a county is not conducted using the same voting system, the result as to the precincts not subject to this article shall be determined in accordance with other provisions of this code and the result of the vote at precincts subject to this article shall be determined as provided in this article. The statement of the vote in that case shall represent the consolidation of all the results and the results of the canvass of all vote by mail voter ballots.

The central tabulation voting system has the capability to produce the required report(s).

15302(e), (f), (g), (h) - The official canvass shall include, but not be limited to, the following tasks: (e) Processing and counting any valid vote by mail and provisional ballots not included in the semifinal official canvass. (f) Counting any valid write-in votes. (g) Reproducing any damaged ballots, if necessary. (h) Reporting final results to the governing board and the Secretary of State, as required.

The central tabulation voting system has the capability to produce the required report(s).

15342(a) - Any name written upon a ballot for a qualified write-in candidate, including a reasonable facsimile of the spelling of a name, shall be counted for the office, if it is written in the blank space provided and voted as specified below: (a) For voting systems in which write-in spaces appear directly below the list of candidates for that office and provide a voting space, no write-in vote shall be counted unless the voting space next to the write-in space is marked or slotted as directed in the voting instructions, except as provided in subdivision (f). (d) Neither a vote cast for a candidate whose name appears on the ballot nor a vote cast for a write-in candidate shall be counted by a combination of marking and writing, a choice of more names than there are candidates to be nominated or elected to the office. (e) All valid write-in votes shall be tabulated and certified to the elections official on forms provided for this purpose, and the write-in votes shall be added to the results of the count of the ballots at the counting place and be included in the official returns for the precinct.

The central tabulation voting system has the capability to meet this requirement.

15372(a) - The elections official shall prepare a certified statement of the results of the election and submit it to the governing body within 28 days of the election or, in the case of school district, community college district, county board of education, or special district elections conducted on the first Tuesday after the first Monday in November of odd numbered years, no later than the last Monday before the last Friday of that month. (b) The elections official shall post the certified statement of the results of the election on his or her Internet Web site in a downloadable spreadsheet format that may include, but is not limited to, a comma-separated values file or a tab-separated values file and that is compatible with a spreadsheet software application that is widely used at the time

of the posting. The certified statement of the election results shall be posted and maintained on the elections official's Internet Web site for a period of at least 10 years following the election. This subdivision shall apply only to an elections official who uses a computer system that has the capability of producing the election results in a downloadable spreadsheet format without requiring modification of the computer system.

The central tabulation voting system has the capability to produce the required report(s).

15374(a) - The statement of the result shall show all of the following: (1) The total number of ballots cast. (2) The number of votes cast at each precinct for each candidate and for and against each measure. (3) The total number of votes cast for each candidate and for and against each measure. (b) The statement of the result shall also show the number of votes cast in each city, Assembly district, congressional district, senatorial district, State Board of Equalization district, and supervisorial district located in whole or in part in the county, for each candidate for the offices of presidential elector and all statewide offices, depending on the offices to be filled, and on each statewide ballot proposition.

The central tabulation voting system has the capability to produce the required report(s).

19101(b)(1) - The machine or device and its software shall be suitable for the purpose for which it is intended.

The central tabulation voting system meets this requirement.

19101(b)(2) - The system shall preserve the secrecy of the ballot.

The central tabulation voting system meets this requirement.

19101(b) (3) – The system shall be safe from fraud or manipulation.

The central tabulation voting system meets this requirement.

19203 - The Secretary of State shall not certify or conditionally approve a voting system or a part of a voting system that uses paper ballots unless the paper used for the ballots is of sufficient quality that it maintains its integrity and readability throughout the retention period specified in Chapter 4 (commencing with Section 17300) of Division 17.

The ballots used for testing the central tabulation voting system have the capability to meet this requirement.

19204 - The Secretary of State shall not certify or conditionally approve any voting system that includes features that permit a voter to produce, and leave the polling place with, a copy or facsimile of the ballot cast by the voter at that polling place.

The central tabulation voting system has the capability to meet this requirement.

19205 - A voting system shall comply with all of the following: (a) No part of the voting system shall be connected to the Internet at any time. (b) No part of the voting system shall electronically receive or transmit election data through an exterior communication network, including the public telephone system, if the communication originates from or terminates at a polling place, satellite location, or counting center. (c) No part of the voting system shall receive or transmit wireless communications or wireless data transfers.

The central tabulation voting system has the capability to meet this requirement.

V. CONCLUSION

The VSAP Tally 1.0 voting system, in the configuration tested and documented by the California Installation and the County of Los Angeles' Use Procedures, meets all applicable California and federal laws. The County of Los Angeles' VSAP Tally 1.0 voting system is compliant with all applicable California and federal laws.