Los Angeles County VSAP Tally 2.1
Security and Telecommunications Test Report for California Secretary of State

CAF-20003-STR-01

Vendor Name	*Los Angeles County*
Vendor System	*VSAP Tally 2.1*

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
July 26, 2020	1.0	*M. Santos*	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 Compliance is a registered trademark of SLI Compliance, a division of Gaming Laboratories International, LLC.
- All products and company names are used for identification purposes only and may be trademarks of their respective owners.

TABLE OF CONTENTS

Overview

This test report provides results for the security and telecommunications testing on the **County of Los Angeles Voting Solutions for All People (VSAP) Tally 2.1** (**VSAP Tally 2.1**) voting system against the California Voting System Standards (CVSS).

Security and Telecommunications testing examined:

- Top-level system design and architecture
- System documentation and procedures
- Examination and open-ended testing of relevant software and operating system configuration.
- Examination and open-ended testing of system communications, including encryption of data and protocols and procedures for access authorization.
- When applicable, examination and open-ended testing of hardware, including examination of unused hardware ports and the security measures used to lock/seal hardware ports. Physical testing may not be destructive. If a risk is identified that requires destructive testing, it was noted.

Testing was implemented without any prior knowledge of the source code.

The testing was divided into three phases.

- **Phase I – Documentation Review**: A review of all pertinent documents for appropriate processes and procedures for implementing a secure system, including review of the system design and architecture.
- **Phase II – Functional Security Testing**: Testing of relevant software, operating systems, and hardware configurations.
- **Phase III – Telecommunications and Data Transmission Testing**: Testing of all telecommunications aspects of the system.

Phase I – Documentation Review

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

- Top-level system design and architecture
- 2.1.1 Security
- 6.2 Design, Construction, and Maintenance Requirements
- 7.2.2 Access Control Identification
- 7.3.1 Polling Place Security
- 7.3.2 Central Count Location Security

- 7.4.1 Software and Firmware Installation
- 7.4.2 Protection Against Malicious Software
- 7.4.3 Software Distribution and Setup Validation
- 7.4.4 Software Distribution
- 7.4.5 Software Reference Information
- 7.4.6 Software Setup Validation
- 7.8.1 Access Control

See the applicable section below for more information on these requirements.

An issue log of any errors and omissions found in the documentation or anomalies encountered during Phase I testing was maintained.

2.1.1 Security

System security is achieved through a combination of technical capabilities and sound administrative practices. To ensure security, all systems shall:

g. Provide documentation of mandatory administrative procedures for effective system security

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.

7.2.2 Access Control Identification

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 **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.

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

7.3.1 Polling Place Security

For polling place operations, manufacturers **shall** develop and provide detailed documentation of measures to enable poll workers to physically protect and perform orderly shutdown of voting equipment to counteract vandalism, civil disobedience, and similar occurrences.

The measures **shall** allow the immediate detection of tampering with vote casting devices and precinct ballot counters.

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

7.3.2 Central Count Location Security

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.

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

7.4.1 Software and Firmware Installation

The system **shall** meet the following requirements for installation of software, including hardware with embedded firmware.

a. Air Gap Architecture

i. Every voting system **shall** be capable of being deployed in a segregated dual-installation architecture to protect against propagation of viruses. The architecture **shall** allow elections officials to use one or more, permanent server(s) and set of central-office voting devices, known to be running unaltered, certified software and firmware to create memory cards before each election and to use another, physically separate “sacrificial” server and set of voting devices after the election to tabulate results and generate reports. The architecture **shall** allow transfer of the election definition and tally database from the permanent server(s) to the sacrificial server using a write-once medium, such as a CD-R. The

voting system architecture **shall** allow each installation to use its own Ethernet network, port server, and central-office vote-recording units, including any direct-reading electronic (DRE) and optical scan units, permitting the two installations to be segregated and air-gapped to ensure that there are no cross connections. An air gap is established by keeping two installations/networks physically separate and seeing that no device attached to the sacrificial installation/network is connected (directly or indirectly) to the first network, ensuring that data cannot flow from one installation/network to the other.

ii. The Technical Data Package (TDP) for the voting system **shall** provide full procedures and instructions, to be incorporated into the Official Use Procedures for the voting system, to implement the segregated dual-installation architecture.

b. Voting and Tabulating Units

i. If software is resident in the system as firmware, the manufacturer **shall** require and state in the system documentation that every device is to be retested to validate each ROM prior to the start of elections operations.

ii. To prevent alteration of executable code, no software **shall** be permanently installed or resident in the voting system unless the system documentation states that the jurisdiction must provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of the system hardware.

iii. The voting system bootstrap, monitor, and device-controller software may be resident permanently as firmware, provided that this firmware has been shown to be inaccessible to activation or control by any means other than by the authorized initiation and execution of the vote counting program, and its associated exception handlers.

iv. The election-specific programming may be installed and resident as firmware, provided that such firmware is installed on a component (such as a computer chip) other than the component on which the operating system resides.

v. After initiation of Election Day testing, no source code or compilers or assemblers **shall** be resident or accessible.

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

7.4.2 Protection Against Malicious Software

Voting systems **shall** deploy commercial-off-the-shelf (COTS) protection against the many forms of threats to which they may be exposed such as file and macro viruses, worms, Trojan horses, and logic bombs.

Manufacturers **shall** develop and document the procedures to be followed to ensure that such protection is maintained in a current status. Virus and malware protection software and updates **shall** be installed using transportable portable media only and **shall not** be installed by download from the Internet.

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

7.4.3 Software Distribution and Setup Validation

Subsections 7.4.4, 7.4.5, and 7.4.6 specify requirements for the distribution of voting system software and the setup validation performed on voting system equipment. These requirements are applicable to voting systems that have completed certification testing.

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

7.4.4 Software Distribution

The manufacturer **shall** document all software including voting system software, third party software (such as operating systems and drivers) to be installed on the certified voting system, and installation programs.

a. The documentation **shall** have a unique identifier (such as a serial number or part number) for the following set of information: documentation, software manufacturer name, product name, version, the certification application number of the voting system, file names and paths or other location information (such as storage addresses) of the software.

b. The documentation **shall** designate all software files as static, semi-static, or dynamic.

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 National Software Reference Library (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 Satisfactorily covered.

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.).

ii. The manufacturer **shall** document the default values of all system storage locations that hold election specific information.

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

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.

Specific activities to be conducted by the State-approved Testing Agency (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.

However, there were a few items in the documentation that may require modification.

1. Tally/VBL server room cameras observed were not 360-degree cameras. Sufficient camera coverage equated to 360-degree coverage but most of the camera's observed were not 360-degree cameras.
2. The documentation references a Password/Credential management server. During the examination it was determined that this product was not being utilized.
3. The BMG/BMD warehouse didn't require all documented guest access practices.
4. The BMG warehouse doesn't currently have all documented security access controls.

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, functional tests were exercised in order to verify and validate the following CVSS requirements:

- 2.1.1 Security
- 5.4.3 In-process Audit Records
- 7.2.1 General Access Control
- 7.2.2 Access Control Identification
- 7.2.3 Access Control Authentication
- 7.2.4 Access Control Authorization
- 7.3 Physical Security Measures
- 7.3.1 Polling Place Security
- 7.3.2 Central Count Location Security
- 7.4.1 Software and Firmware Installation
- 7.4.2 Protection against Malicious Software
- 7.4.3 Software Distribution and Setup Validation
- 7.4.4 Software Distribution
- 7.4.5 Software Reference Information

- 7.4.6 Software Setup Validation
- 7.6 Telecommunications and Data Transmission
- 7.6.1 Maintaining Data Integrity
- 7.6.2 Election Returns
- 7.8.1 Access Control
- 7.8.2 Data Interception and Disruption

See the applicable section below for more information on these requirements.

An issue log of any errors and omissions found in the documentation or anomalies encountered during Phase II testing was maintained.

2.1.1 Security

System security is achieved through a combination of technical capabilities and sound administrative practices. To ensure security, all systems **shall**:

a. Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability.

b. Provide system functions that are executable only in the intended manner and order, and only under the intended conditions.

c. Use the system's control logic to prevent a system function from executing if any preconditions to the function have not been met.

d. Provide safeguards in response to system failure to protect against tampering during system repair or interventions in system operations.

e. Provide security provisions that are compatible with the procedures and administrative tasks involved in equipment preparation, testing, and operation.

f. Incorporate a means of implementing a capability if access to a system function is to be restricted or controlled.

g. Provide documentation of mandatory administrative procedures for effective system security

Testing performed: The overall functionality of the system was assessed based upon these seven functional security requirements:

1. All access control mechanisms were examined to determine if they are adequate to guard against system integrity, availability, confidentiality, and accountability.
2. The system functions were examined to determine that the system functions only in the intended manner.

3. All system control logic was examined to determine if system functions can be executed without preconditions to the functions being met.
4. Examination of the systems safeguards in response to system failures to determine if there is protection against tampering during a system repair or interventions.
5. Confirm that the security provisions are compatible with procedures, administrative tasks during equipment preparation, and election system testing and operation.
6. Determine if system capabilities can be implemented during system functions while the system is restricted or controlled.

Results Applicable to BMD: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to BMG: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to Tally: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to VSAP Ballot Layout (VBL) components: Testing validated that the requirement was Satisfactorily covered.

5.4.3 In-process Audit Records

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

Testing performed: As all other requirements are being tested, the Audit Log was reviewed to verify that appropriate records are being recorded for the events occurring.

Results Applicable to BMD: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to BMG: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to Tally: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to VBL components: Testing validated that the requirement was Satisfactorily covered.

7.2.1 General Access Control

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.

Testing performed: Testing was performed on each user role within the voting system to verify that users are allowed to perform all necessary tasks for their role, but are not allowed to perform any tasks not assigned to their role, nor are they able to modify a role to a higher-level role activity.

Testing was performed to verify that all voting system equipment prevents modification of related software/firmware by any means other than the documented procedure for software upgrades. Testing was performed to verify that tampering is not allowed.

Results Applicable to BMD and BMG: Testing validated that the requirement was Partially covered.

The systems lacked full disk encryption allowing for potential circumvention of protections which is considered a vulnerability. This attack could only be performed by an inside threat.

Results Applicable to Tally and VBL components: Testing validated that the requirement was Partially covered.

The systems lacked full disk encryption allowing for potential circumvention of protections which is considered a vulnerability. This attack could only be performed by an inside threat.

Not all physical access controls were consistently implemented.

7.2.2 Access Control Identification

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 **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.

Testing performed: Testing was performed on each user role within the voting system to verify that users are allowed to perform all necessary tasks for their role and are appropriately identified by the system.

Results Applicable to BMD: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to BMG: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to Tally: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to VBL components: Testing validated that the requirement was Satisfactorily covered.

7.2.3 Access Control Authentication

The following authentication requirements apply to all voting system equipment.

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 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 username 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.

Testing performed: Testing was performed to verify that:

- The administrator group or role is able to perform all the functions listed in the requirements above.
- Users are authenticated properly prior to being allowed access
- All private access data is properly secured
- Usernames are not allowed to be part of the password

Results Applicable to BMD: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to BMG: Testing validated that the requirement was Partially covered.

The systems lacked full disk encryption allowing for potential circumvention of protections which is considered a vulnerability. This attack could only be performed by an inside threat.

Results Applicable to Tally and VBL components: Testing validated that the requirement was Partially covered.

The systems lacked full disk encryption allowing for potential circumvention of protections which is considered a vulnerability. This attack could only be performed by an inside threat.

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 on each user role within the voting system to verify that only authorized users, roles, or groups are allowed access to election data, as based on pertinent access control lists or policies.

Results Applicable to BMD and BMG: Testing validated that the requirement was Partially covered.

It was determined that access control authorization procedures were not consistently implemented.

The systems lacked full disk encryption allowing for potential circumvention of protections which is considered a vulnerability. This attack could only be performed by an inside threat.

Results Applicable to Tally and VBL components: Testing validated that the requirement was Partially covered.

It was determined that the systems contains shared secrets that were utilized across multiple systems. The static/shared secrets could be obtained by unauthorized individuals and in turn could allow unauthorized access to system components.

The systems lacked full disk encryption allowing for potential circumvention of protections which is considered a vulnerability. This attack could only be performed by an inside threat.

7.3 Physical Security Measures

a. Any unauthorized physical access **shall** leave physical evidence that an unauthorized event has taken place.

b. Voting systems **shall** only have physical ports and access points that are essential to voting operations and to voting system testing and auditing.

c. An event log entry that identifies the name of the affected device **shall** be generated if a component connected to a piece of voting system equipment is disconnected while polls are open.

d. Ports disabled while polls are open **shall** only be re-enabled by authorized administrators.

e. Access points, such as covers and panels, **shall** be secured by locks or tamper evident seals or tamper resistant countermeasures **shall** be implemented so that system owners can monitor access to voting system components through these points.

f. Ballot boxes **shall** be designed such that any unauthorized physical access results in physical evidence that an unauthorized event has taken place.

Testing performed: Testing was performed to verify:

- That unauthorized physical access leaves physical evidence of the intrusion
- That only ports and access points essential to voting operations, testing, and auditing are present
- That event log entries adequately identify affected devices
- Ports disabled during the open polls period are only able to be re-enabled by an authorized administrator
- That all access points and ballot boxes are secured and provide adequate tamper evidence as well as tamper resistant countermeasures

Results Applicable to BMD and BMG: Testing validated that the requirement was Satisfactorily covered..

Results Applicable to Tally and VBL: Testing validated that the requirement was Satisfactorily covered.

7.3.1 Polling Place Security

For polling place operations, manufacturers **shall** develop and provide detailed documentation of measures to enable poll workers to physically protect and perform orderly shutdown of voting equipment to counteract vandalism, civil disobedience, and similar occurrences.

The measures **shall** allow the immediate detection of tampering with vote casting devices and precinct ballot counters.

Testing performed: Testing was performed to verify that the documented measures provide adequate polling place security.

Results Applicable to BMD: Testing validated that the requirement was Satisfactorily covered.

7.3.2 Central Count Location Security

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.

Testing performed: Testing was performed to verify that the documented measures provide adequate central count location security.

Results Applicable to BMG: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to Tally: Testing validated that the requirement was Satisfactorily covered.

7.4.1 Software and Firmware Installation

The system **shall** meet the following requirements for installation of software, including hardware with embedded firmware.

b. Voting and Tabulating Units

   ii. To prevent alteration of executable code, no software **shall** be permanently installed or resident in the voting system unless the system documentation states that the jurisdiction must provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of the system hardware.

   iii. The voting system bootstrap, monitor, and device-controller software may be resident permanently as firmware, provided that this firmware has been shown to be inaccessible to activation or control by any means other than by the authorized initiation and execution of the vote counting program, and its associated exception handlers.

   iv. The election-specific programming may be installed and resident as firmware, provided that such firmware is installed on a component (such as a computer chip) other than the component on which the operating system resides.

   v. After initiation of Election Day testing, no source code or compilers or assemblers **shall** be resident or accessible.

Testing performed: Testing was performed to verify that if any software or firmware is installed, it is inaccessible to activation or control by anything other than authorized means, unless the documentation states the jurisdiction must provide a secure physical and procedural environment. Testing was performed to verify that no source code, compilers, or assemblers are resident or accessible after Election Day testing.

Results Applicable to BMD: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to BMG: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to Tally: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to VBL components: Testing validated that the requirement was Satisfactorily covered.

7.4.2 Protection against Malicious Software

Voting systems **shall** deploy commercial-off-the-shelf (COTS) protection against the many forms of threats to which they may be exposed such as file and macro viruses, worms, Trojan horses, and logic bombs.

Manufacturers **shall** develop and document the procedures to be followed to ensure that such protection is maintained in a current status. Virus and malware protection software and updates **shall** be installed using transportable portable media only and **shall not** be installed by download from the Internet.

Testing performed: Testing was performed to verify that COTS products are implemented to protect against malicious software, as described in manufacturer documentation.

Results Applicable to BMD: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to BMG: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to Tally: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to VBL components: Testing validated that the requirement was Satisfactorily covered.

7.4.3 Software Distribution and Setup Validation

Subsections 7.4.4, 7.4.5 and 7.4.6 specify requirements for the distribution of voting system software and the setup validation performed on voting system equipment. These requirements are applicable to voting systems that have completed certification testing.

Testing performed: This requirement is met by successful validation of 7.4.4, 7.4.5, and 7.4.6.

Results Applicable to BMD: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to BMG: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to Tally: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to VBL components: Testing validated that the requirement was Satisfactorily covered.

7.4.4 Software Distribution

The manufacturer **shall** document all software including voting system software, third party software (such as operating systems and drivers) to be installed on the certified voting system, and installation programs.

a. The documentation **shall** have a unique identifier (such as a serial number or part number) for the following set of information: documentation, software manufacturer name, product name, version, the certification application number of the voting system, file names and paths or other location information (such as storage addresses) of the software.
b. The documentation **shall** designate all software files as static, semi-static or dynamic.

Results Applicable to BMD: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to BMG: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to Tally: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to VBL components: Testing validated that the requirement was Satisfactorily covered.

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 performed to verify that the software can be verified to match the NSRL reference information.

Results Applicable to BMD: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to BMG: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to Tally: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to VBL components: Testing validated that the requirement was Satisfactorily covered.

7.4.6 Software Setup Validation

a. Setup validation methods **shall** verify that only authorized software is present on the voting equipment. Authorized software is COTS software components needed to run the voting system and voting software components identified by the manufacturer as authorized.

b. The manufacturer **shall** provide a method to comprehensively list all software files that are installed on voting systems.

   i. This method **shall** list version names and numbers for all application software on the voting system.

   ii. This method should list of the date of installation for all application software on the voting system.

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.

d. Voting systems **shall** include a software verification method that either verifies software prior to installation or a method that verifies software using an external interface. Voting systems may include both software verification methods. Voting systems may provide ancillary setup validation methods, including methods for verifying or identifying installed software, other than those described in this section. There are no specific requirements for ancillary setup validation methods. However, any method intended to serve as the voting system software verification method must meet the requirements outlined in this section.

e. Voting systems which implement a software verification method that verifies software prior to installation **shall** meet the following requirements.

i. The voting system **shall** contain no more than one method for installing, updating, or removing software on a system.
   - Voting system equipment **shall** prevent processes from installing software except for the one specific software installation process identified by the manufacturer.
   - The voting system manufacturer **shall** document the procedures for installing, updating, and removing voting system software, configuration files, and data files.
   - Voting system equipment **shall** prevent processes from installing, updating, or removing software while the polls are open.
   - Voting system equipment **shall** prevent the execution of software not installed using the specified software installation process.

ii. The voting system **shall** only allow authenticated administrators to install software on voting equipment. The voting system **shall** present the administrator with a description of the software change being performed, including:
   - A list of all applications and/or file names being updated.
   - The type of action performed on each application and/or file (e.g., new application/file, deletion or overwriting of existing file)

iii. Voting system equipment **shall** store the current version identification of all software installed on the voting system equipment.
   - The current version identification **shall** be included as part of reports created by the voting system equipment.
   - The current version identification **shall** be displayed as part of the voting system equipment start up process.

iv. The process for installing, updating, and removing software **shall** make software changes based on information contained in software update packages. Software update packages **shall** minimally contain the following information:
   - A unique identifier for the software update package.
   - Names of the applications or files modified during the update process.
   - Version numbers of the applications or files modified during the update process.
   - Any software prerequisites or dependencies for the software involved in the update.

- A description of the type of action performed on each application and/or file (e.g., new application/file, deletion or overwriting of existing file).
- The binary data of any new or updated files involved in the update process.

v. The software update package **shall** be formatted in a non-restrictive, publicly-available format. Manufacturers **shall** provide a specification describing how they have implemented the format with respect to the manufacturer's specific voting devices and data, including such items as descriptions of elements, attributes, constraints, extensions, syntax and semantics of the format, and definitions for data fields and schemas.

vi. Software update packages **shall** be digitally signed by using a NIST approved algorithm with a security strength of at least 112 bits.

vii. The software installation process **shall** verify digital signatures, software version identification, software prerequisites and dependencies, and manufacturer specific authorization information associated with the software before the software is installed. The software installation process **shall** not install software with invalid digital signatures, version numbers, or manufacturer specific authorization information, and **shall** not install software on systems that do not meet the update requisites.

viii. The voting system **shall** have the capability to prevent the installation of previous versions of applications or files.

ix. The software installation process **shall** result in information being stored in the voting system equipment's log such that altering or deleting log entries or the log will be detected.

x. The minimum information to be included in the voting system equipment log **shall** be:

- Success or failure of the software installation process;
- Cause of a failed software installation (such as invalid version identification, digital signature, etc.);
- Application or file name(s), and version number(s);
- A description of the type of action performed on each application and/or file (e.g., new application/file, deletion or overwriting of existing file);
- A cryptographic hash of the software update package using FIPS 1402 level 1 or higher validated cryptographic module.

f. If software is verified after being installed on the voting system equipment, the voting system equipment **shall** provide an external interface to the location of the voting system software for software verification purposes.
    i. The external interface:
        - **Shall** be protected using tamper evident techniques,
        - **Shall** have a physical indicator showing when the interface is enabled and disabled
        - **Shall** be disabled during voting
        - Should provide a direct read-only access to the location of the voting system software without the use of installed software ii. The verification process should be able to be performed using COTS software and hardware available from sources other than the voting system manufacturer.
        - If the process uses hashes or digital signatures, then the verification software **shall** use a FIPS 140-2 level 1 or higher validated cryptographic module.
        - The verification process **shall** either (a) use reference information on unalterable storage media received from the repository or (b) verify the digital signature of the reference information on any other media.

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.).
    i. The manufacturer should provide a method to query the voting system to determine the value contained in all system storage locations containing election specific information.

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

Results Applicable to BMD: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to BMG: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to Tally: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to VBL components: Testing 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.

7.6.1 Maintaining Data Integrity

Voting systems that use telecommunications to communicate between system components and locations are subject to the same security requirements governing access to any other system hardware, software, and data function.

a. Voting systems that use electrical or optical transmission of data **shall** ensure the receipt of valid vote records is verified at the receiving station. This should include standard transmission error detection and correction methods such as checksums or message digest hashes. Verification of correct transmission **shall** occur at the voting system application level and ensure that the correct data is recorded on all relevant components consolidated within the polling place prior to the voter completing casting of his or her ballot.

    i. Cryptography used to verify the receipt of vote records **shall** use NIST approved algorithms with security strength of at least 112 bits. Message Authentication Code (MAC) keys **shall** have a security strength of at least 112 bits.

Testing performed: Testing was performed to verify that data is properly encrypted, and that receipt is verified.

Results Applicable to BMG: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to Tally: Testing validated that the requirement was Satisfactorily covered.

7.6.2 Election Returns

If the voting system provides access to election returns or interactive inquiries, the system **shall**:

a. Allow authorized administrators the ability to disable or restrict access to election returns (for equipment that operates in a central counting environment). This requirement applies as well to polling place equipment that contains a removable memory module or that may be removed in its entirety to a central place for the consolidation of polling place returns

b. Design voting system software and its security environment such that data accessible to interactive queries resides in an external file or database

created and maintained by the elections software under the restrictions applying to any other output report:

i. The output file or database has no provision for write access back to the system

ii. Persons whose only authorized access is to the file or database are denied write access, both to the file or database, and to the system

Testing performed: Testing was performed to determine that if the system provides access to election returns or interactive queries, authorized administrators can disable or restrict access and queries, and that the data resides in an external file or database governed by the voting system.

Results Applicable to BMG: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to Tally: Testing validated that the requirement was Satisfactorily covered.

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 access control procedures work as specified, including against attempts to defeat the implemented access control security on each system component.

Results Applicable to BMG and BMD: Testing validated that the requirement was Partially covered.

Access Control processes that permit high dependency on root access are still an issue with the solution. With many parts of the system requiring elevated access requirements, the ability to protect the root password(s) for the system results in the potential for unauthorized access to the system.

During the examination it was observed that previously implemented passwords were being re-used.

It is recommended that some form of password policy be implemented which includes cycling of previously implemented passwords from previous certification and election activities.

Results Applicable to Tally and VBL components: Testing validated that the requirement was Partially covered:

It was observed that control access in some areas utilized only minimal processes and policies.

During the examination it was observed that user access controls were not consistently implemented.

It is recommended that the documented user access control policies and procedures be fully implemented.

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: Testing was performed to verify appropriate encryption, receipt validation, and data integrity against any attempts to compromise the system.

Results Applicable to BMD: Testing validated that the requirement was Satisfactorily covered.

The BMD device does not store or transmit any cast ballot records. The only thing that is transmitted is the audit logs. All communications between the devices on this network are encrypted.

Results Applicable to BMG: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to Tally and VBL components: Testing validated that the requirement was Satisfactorily covered.

Phase III – Telecommunications and Data Transmission Testing

Telecommunications and Data Transmission Testing will include testing of system communications, including encryption of data, as well as protocols and procedures for access authorization.

During Phase III, functional tests was exercised in order to verify and validate the following CVSS requirements:

- 6.1.2 Data Transmission
- 6.2.1 Confirmation

See the applicable section below for more information on these requirements.

During Phase III testing, an issue log of any errors and omissions found in the documentation or anomalies encountered 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 verify appropriate encryption, receipt validation, and data integrity.

Results Applicable to BMD: Testing validated that the requirement was Satisfactorily met.

Only type of data being transmitted from the BMD device is audit logs, as the BMD is only used to mark and print and store the ballots for tabulation at Tally.

Results Applicable to BMG: Testing validated that the requirement was Partially met.

Telecommunications access control is not consistently implemented.

It is recommended that the documented telecommunications access control policies and procedures be fully implemented.

Results Applicable to VBL components: Testing 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.

Testing performed: Testing was performed to verify appropriate confirmation of data transmission to the user and any actions to be taken.

Results Applicable to BMG: Testing validated that the requirement was Satisfactorily covered.

Results Applicable to Tally: Testing validated that the requirement was Satisfactorily covered.

Open-Ended Vulnerability Testing

Vulnerability testing is an attempt to bypass or break the security of a system or a device. Like functional testing, vulnerability testing can falsify a general assertion

(namely, demonstrate that the system or device is secure) but it cannot verify the security (show that the system or device is secure in all cases). Open-ended vulnerability testing (OEVT) is conducted without the confines of a pre-determined test suite. It instead relies heavily on the experience and expertise of the OEVT Team Members, their knowledge of the system, its component devices and associated vulnerabilities, and their ability to exploit those vulnerabilities.

The goal of OEVT is to discover architecture, design, and implementation flaws in the system that may not be detected using systematic functional, reliability, and security testing and which may be exploited to change the outcome of an election, interfere with voters' ability to cast ballots or have their votes counted during an election, or compromise the secrecy of the vote. The goal of OEVT also includes attempts to discover logic bombs, time bombs, or other Trojan Horses that may have been introduced into the system hardware, firmware, or software for said purposes

Vulnerabilities

Should any vulnerabilities have been discovered, SLI identifies particular standards applicable to each vulnerability.

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

- Voter: Usually has low knowledge of the voting technology software and/or hardware design and configuration. Some may have more advanced knowledge. May carry out attacks designed by others.
- 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: Has a 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: Has great knowledge of the voting machine design and configuration. Has 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.

7.5.1 OEVT Scope and Priorities

a. Scope of open-ended vulnerability testing – The scope of open-ended vulnerability testing **shall** include the voting system security during all phases of the voting process and **shall** include all manufacturer supplied voting system use procedures. The scope of OEVT includes, but is not limited to, the following:
   i. Voting system security
   ii. Voting system physical security while voting devices are:
      - In storage
      - Being configured
      - Being transported
      - Being used
   iii. Voting system use procedures

b. Focus of open-ended vulnerability testing – OEVT Team members **shall** seek out vulnerabilities in the voting system that might be used to change the outcome of an election, to interfere with voters' ability to cast ballots or have their votes counted during an election or to compromise the secrecy of vote.

c. OEVT General Priorities – The OEVT team **shall** prioritize testing efforts based on:
   i. Threat scenarios for the voting system under investigation;
   ii. The availability of time and resources;
   iii. The OEVT team's determination of easily exploitable vulnerabilities; and
   iv. The OEVT team's determination of which exploitation scenarios are more likely to impact the outcome of an election, interfere with voters' ability to cast ballots or have their votes counted during an election or compromise the secrecy of the vote.
   v. All threat scenarios must be plausible in that they should not be in conflict with the anticipated implementation, associated use procedures, the workmanship requirements (assuming those requirements were all

met) or the development environment specification as supplied by the manufacturer in the TDP;

vi. Open-ended vulnerability testing should not exclude those threat scenarios involving collusion between multiple parties including manufacturer insiders. It is acknowledged that threat scenarios become less plausible as the number of conspirators increases;

vii. It is assumed that attackers may be well resourced and may have access to the system while under development;

viii. Threats that can be exploited to change the outcome of an election and flaws that can provide erroneous results for an election should have the highest priority;

ix. Threats that can cause a denial of service during the election should be considered of very high priority;

x. Threats that can compromise the secrecy of the vote should be considered of high priority;

xi. A threat to disclosure or modification of metadata (e.g., security audit log) that does not change the outcome of the election, does not cause denial of service during the election, or does not compromise the secrecy of ballot should be considered of lower priority;

xii. If the voting device uses COTS products, then the OEVT team should also investigate publicly known vulnerabilities; and

xiii. The OEVT team should not consider the voting device vulnerabilities that require Internet connectivity for exploitation if the voting device is not connected to the Internet during the election and otherwise. However, if the voting device is connected to another device which in turn may have been connected to the Internet (as may be the case of epollbooks), Internet based attacks may be plausible and should be investigated.

7.5.2 OEVT Resources and Level of Effort

a. OEVT team resources – The OEVT team **shall** use the manufacturer supplied Technical Data Package (TDP) and User documentation, have access to voting devices configured similar to how they are to be used in an election, and have access to all other material and tools necessary to conduct a thorough investigation. Materials supplied to the OEVT team **shall** include but not be limited to the following:

i. Threat analysis describing threats mitigated by the voting system;

ii. Security architecture describing how threats to the voting system are mitigated;

iii. High level design of the system;

iv. Any other documentation provided to an EAC voting system testing laboratory or S-ATA, if applicable;

v. Source code;

vi. Operational voting system configured for election, but with the ability for the OEVT team to reconfigure it;

vii. Testing reports from the developer and from the testing laboratory including previous OEVT results;

viii. Tools sufficient to conduct a test lab build; and

ix. Procedures specified by the manufacturer as necessary for implementation and secure use.

b. Open-ended vulnerability team establishment – The test lab **shall** establish an OEVT team of at least three security experts and at least one election management expert to conduct the open-ended vulnerability testing.

c. OEVT Team Composition: Security Experts – The OEVT team **shall** have at least one member with six or more years of experience in the area of software engineering, at least one member with six or more years of experience in the area of information security, at least one member with six or more years of experience in the area of penetration testing and at least one member with six or more years of experience in the area of voting system security.

d. OEVT Team Composition: Election Management Expert – The OEVT team **shall** have at least one member with at least eight years of experience in the area of election management. The OEVT team **shall** consult with an elections expert, designated by the Secretary of State, who is familiar with election procedures, how the voting systems are installed and used, and how votes are counted.

e. OEVT team knowledge – The OEVT team knowledge **shall** include but not be limited to the following:

i. Complete knowledge of work done to date on voting system design, research and analysis conducted on voting system security, and known and suspected flaws in voting systems;

ii. Complete knowledge of threats to voting systems;

iii. Knowledge equivalent to a bachelor's degree in computer science or related field;

iv. Experience in design, implementation, security analysis, or testing of technologies or products involved in voting system; and

v. Experience in the conduct and management of elections.

f. OEVT level of effort: test plan – In determining the level of effort to apply to open-ended vulnerability testing, the test lab **shall** take into consideration the size and complexity of the voting system; any available results from the "close ended" functional, security, and usability testing activities and laboratory analysis and testing activities; the number of vulnerabilities found in previous security analyses; and testing of the voting system and its prior versions.

g. OEVT level of effort: commitment of resources – The OEVT team **shall** examine the system for a minimum of 12 staff weeks.

7.5.3 Context of OEVT Testing

a. Context of testing – Open ended vulnerability testing shall be conducted within the context of a process model describing a specific implementation of the voting system and a corresponding model of plausible threats

b. Adequate system model – The OEVT team shall verify that the manufacturer provided system model sufficiently describes the intended implementation of the voting system.

c. Adequate threat model – The OEVT team shall verify that the threat model sufficiently addresses significant threats to the voting system. Significant threats are those that could:

   i. Change the outcome of an election;

   ii. Interfere with voters' ability to cast ballots or have their votes counted during an election; or

   iii. Compromise the secrecy of vote

Results Applicable to BMD: Testing validated that the requirement was Successfully covered.

Results Applicable to BMG: Testing validated that the requirement was Partially covered.

Programmatic access control is not consistently implemented.

A Nessus scan reported two High risk factor issues, fourteen Medium risk factor issues, and five Low risk factor issues.

To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic.

This vulnerability can be accessed by an election official insider.

Results Applicable to Tally and VBL components: Testing validated that the requirement was Partially covered.

A Nessus scan reported two Critical risk factor issues, two High risk factor issues, six Medium risk factor issues, and three Low risk factor issues.

Observations about potential vulnerabilities observed with regard to BMG, Tally and VBL:

1. There were a number of networking reported vulnerabilities. Due to the solution being on an air-gapped network, the risk of these vulnerabilities being exploited is virtually non-existent. They are being reported as they are still considered vulnerabilities and there are mitigations that can be completed to close the vulnerability.
   During the examination it was determined that the solution doesn't consistently implement cryptographic modules in the system components.
2. Access control authorizations not consistently implemented.
3. Telecommunications data protection mechanisms not consistently implemented.

These vulnerabilities can be accessed by an election official insider.

Tools

Tools used include:

- Nessus Professional
- Metasploit framework V5.0.23-dev
- Wireshark V2.6.8
- Kali Linux V 2019.2
- HAK5 USB Rubber Ducky
- HAK5 Bash Bunny
- USB3 Test Plug
- Lock Picks
- Burp Suite Professional

VSAP Tally 2.0 Issues

During the CVSS requirements examination and the Open-Ended Vulnerability Testing (OEVT) portion of this testing, issues from the previous VSAP Tally 2.0 examination conducted in 2019, were examined in this release, VSAP Tally 2.1, to determine if the issues had been resolved. In some cases, issues found during VSAP Tally 2.0 were successfully mitigated.

These include:

1. Ability to boot from USB on systems. This includes disabling USB access, or physically restricting access to USB ports.
2. Unrestricted access to workstation cases.
3. Unrestricted access to server racks.

These vulnerabilities have been successfully mitigated.

The following issues discovered in VSAP Tally 2.0 were not successfully addressed in this current certification effort:

1. **FIPS 140-2 compliant cryptographic module utilization**: While there is utilization of FIPS validated modules through different portions of the systems. Initial examination does not have the FIPS modules deployed and enabled. Through discussions it was determined that this is set to be incorporated into the next certification effort.
2. **Full Disk encryption**: Currently, full disk encryption is not being utilized on systems within the solution. This is also another enhancement that is being slated for the next certification effort.
3. **Dependency on root access**: The same amount of dependency on elevated (root) access was observed during the examination, including utilization of functions like cryptographic keys, system maintenance, system shutdown/startup, and other system functions. It should be noted that attempts to provide segregation of password knowledge between County and Vendor resources was observed.
4. **Shared/static secrets**: Hard coded passwords, and ".yml" configuration files that contain system passwords were observed throughout the solution.

These previously discovered vulnerabilities constitute a risk and potential attack vector for the system.

Final Report

The documentation review found all aspects of the documentation to be satisfactorily covered.

The functional security review found some issues concerning full disk encryption not being fully implemented, as well as access control authorization procedures not consistently implemented.

A number of critical, high, medium, and low vulnerabilities were found during vulnerability scans of the entire VSAP Tally 2.1 solution environment. With the physical and air-gap mitigations, the chance of these vulnerabilities being exploited is considered to be low to medium. These vulnerabilities, however, are still present

and constitute a potential attack vector should any of the physical or air-gap protections become circumvented.

Review of the VSAP Tally 2.0 issues showed that three items have been resolved, and four items remain unresolved.

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

End of VSAP Tally 2.1 Security and Telecommunications Test Report