County of Los Angeles VSAP Tally 1.0
Central Tabulation System
Security and Telecommunications Test Report for California

LAC-306-STR-01

Prepared for:

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

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 12th2018	v1.0	*M. Santos, J. Peterson*	Initial Release
July 16th, 2018	V1.1	*M. Santos, J. Peterson*	Updates per CASOS

Disclaimer

The information reported herein must not be used by the client to claim product certification, approval, or endorsement by NVLAP, NIST, or any agency of the Federal Government.

Trademarks

- SLI is a registered trademark of SLI Compliance.
- All products and company names are used for identification purposes only and may be trademarks of their respective owners.

TABLE OF CONTENTS

Introduction

This Test Report outlines the security testing approach SLI Compliance (SLI) followed when performing Security and Telecommunications Testing on the County of Los Angeles VSAP Tally 1.0 (VSAP Tally 1.0) system against the California Voting System Standards (CVSS).

Security and Telecommunications testing examined:

- Top-level system design and architecture
- System documentation and procedures
- 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
- Testing of system communications, including encryption of data, as well as protocols and procedures for access authorization

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

The testing was divided into four phases.

- Phase I included review of all pertinent documents for appropriate processes and procedures for implementing a secure system. This will include review of the system design and architecture.
- Phase II included testing of relevant software, operating systems and hardware configurations.
- Phase III included testing of all telecommunications aspects of the system.
- Phase IV included an onsite inspection of the VSAP Tally environment.

Review Results

Phase I – Documentation Review

The documentation review was conducted to analyze the LA County VSAP Tally 1.0 system for findings against the applicable California Voting System Standards (CVSS):

- Top-level system design and architecture
- Design, construction, and maintenance requirements
- Access control identification
- Central count location security

- Software and firmware installation
- Protection against malicious software
- Software distribution and setup validation
- Software distribution
- Software reference information
- Software setup validation
- Access control

Design, Construction, and Maintenance Requirements

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 6.2 requirement:

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

- The expected outcome for this review was that no issue would be found.
- The actual outcome for this review was a determination that the documentation sufficiently detailed the design, construction, and maintenance requirements for communications related to the VSAP Tally 1.0 solution. The system currently utilizes an air gapped networking infrastructure and public telecommunications are not applicable.

Access Control Identification

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.2.2 requirements:

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

- The expected outcome for this review was that no issue would be found.
- The actual outcome for this review was a determination that the documentation contained sufficient information on users, processes, roles, and specific functions within the documentation. This included VSAP Tally 1.0 application users as well as Backend OS and Scanner access controls.

Central Count Location Security

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.3.2 requirement:

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

- The expected outcome for this review was that no issue would be found.
- The actual outcome for this review was a determination that sufficient documentation was in place detailing the physical, logical, and electronic Central Count security, including video surveillance, building alarms, badge access, and dedicated onsite redundant building power.

Software and Firmware Installation

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.4.1 requirements:

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 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 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

- The expected outcome for this review was that no issue would be found.
- The actual outcome for this review was a determination that, over all, the documentation covered or referenced part of the CVSS requirements. However, while air gap technologies and practices are discussed, no

specific documentation detailing the implementation of these practices was provided.

a. Air Gap Architecture: the documentation described the basic overall features and requirements of the Air Gapped network; however, the documentation does not go into exact specifics of configuration of the setup and deployment of the air gap. The documentation details components of the air gap including who performs the administrative functions and how anti-virus protection is handled. The documentation includes measures to ensure the air gap is maintained including disabling of USB ports, covering media slots use of tamper evident seals, and lock/key combinations.

   However the documentation does not provide exact steps for installation and configuration of the network equipment or the VSAP Tally and Scanner systems in conjunction with maintaining the air gap.

b. i, ii, iii, iv. None of the software of the VSAP Tally 1.0 system is resident as firmware, therefore no documentation is needed for these requirements.

b. v. Confirmed that the build process is documented on a dedicated build environment and that no source code, compilers, or assemblers are present in the production systems.

Protection against Malicious Software

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.4.2 requirements:

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

- The expected outcome for this review was that no issue would be found.
- The actual outcome for this review was a determination that the VSAP Tally 1.0 system does not actively utilize COTS anti-virus protection on the systems associated with the solution. This includes machines that are designated as part of the scanner solution. The documentations states that all machines/servers be scanned before the election and that after the initial vulnerability assessment / virus scan, all machines will be isolated on the air

gapped network. Documentation also states that during the tabulation process, no anti-virus solution is employed on the closed air gapped network.

Software Distribution and Setup Validation

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.4.3 requirement:

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.

Software Distribution

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.4.4 requirements:

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

- The expected outcome for this review was that no issue would be found.
- The actual outcome for this review was a determination that the manufacturer's documentation contains sufficient references for software utilized in the solution including VSAP Tally 1.0 components, operating system, and COTS products.

  a. The documentation contains sufficient unique identifiers for all requested information including file names (where applicable); versions of documentation; and software manufacturer names, versions, and product names.

b. The documentation indicates that the VSAP Tally 1.0 software is static; bindings such as openssl, zbar and opencv are dynamic; and that Linux production environments, including docker, are a mix of the two (semi-static). However, it did not include a specific listing of all software files.

Software Reference Information

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.4.5 requirements:

a. The manufacturer **shall** provide the 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

- The expected outcome for this review was that no issue would be found.
- The actual outcome for this review was a determination that the instructions for setting up the build environment and building the deployment package are sufficient. However, the documentation did not indicate where the certified copy of the software is obtained (CA SOS or Laboratory that tested the system). There are instructions detailing how to verify if the software distributed is the certified version; however, it does not discuss using unalterable storage media for distribution.

Software Setup Validation

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.4.6 requirements:

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

Results

- The expected outcome for this review was that no issue would be found.
- The actual outcome for this review was a determination that there are validation methods documented to verify the VSAP Tally 1.0 trusted build output as well as a JSON file with a list of every container generated by the build process and a corresponding hash value. Each of the COTS products contains a hash of the single file deployment files. The system, however, does not 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.

Access Control

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.8.1 requirements:

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

- The expected outcome for this review was that no issue would be found.
- The actual outcome for this review was a determination that there is sufficient documentation of access control including: users present, roles of specific users, and documented functionality for all users of the system(s) including scanner users.

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 the security measures applied to those ports

During Phase II testing, functional tests were exercised to verify and validate the following requirements in accordance with the applicable California Voting System Standards (CVSS):

- In-process audit records
- General access control
- Access control identification
- Access control authentication
- Access control authorization
- Physical security measures
- Central count location security
- Software and firmware installation
- Protection against malicious software
- Software distribution and setup validation
- Software reference information
- Software setup validation
- Telecommunications and data transmission
- Maintaining data integrity
- Access control
- Data interception and disruption

In-process Audit Records

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 5.4.3 requirement:

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

Results

- The expected outcome for this review was that no issue would be found.
- 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, and Imagetrac logs.

General Access Control

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.2.1 requirements:

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 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.

Results

- The expected outcome for this review was that no issue would be found.
- 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 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.

Access Control Identification

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.2.2 requirements:

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

- The expected outcome for this review was that no issue would be found.
- 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.

Access Control Authentication

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.2.3 requirements.

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 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.

Results

- The expected outcome for this review was that no issue would be found.
- 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 which sufficiently meets the requirements.

Access Control Authorization

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.2.4 requirements:

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.

Results

- The expected outcome for this review was that no issue would be found.
- The actual outcome for this review was a determination that the system sufficiently ensures that only authorized users/groups/roles have access to

the systems and election data, from the scanning environment through the VSAP Tally 1.0 user interface.

Physical Security Measures

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.3 requirements:

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.

Results

- The expected outcome for this review was that no issue would be found.
- The actual outcome for this review was a determination that the system sufficiently meets the requirement for physical security.

Central Count Location Security

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.3.2 requirement:

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

- The expected outcome for this review was that no issue would be found.

- 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.

Software and Firmware Installation

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.4.1 requirements:

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.

Results

- The expected outcome for this review was that no issue would be found.
- The actual outcome for this review was a determination that the VSAP Tally 1.0 solution sufficiently meets the requirements for software and firmware installation. Further testing indicates that the solution is not resident as firmware and that there are processes in place to verify installation media, as well as verification procedures for each of the Docker instances. The systems are protected by extended physical and procedural security measures.

Protection against Malicious Software

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.4.2 requirements:

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

- The expected outcome for this review was that no issue would be found.
- 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 1.0 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.

Software Distribution and Setup Validation

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.4.3 requirement:

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.

Software Setup Validation

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.4.6 requirements:

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.

Results

- The expected outcome for this review was that no issue would be found.
- 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 container generated by the build process and a corresponding hash value. Each of the COTS products contains 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 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 system utilizes processes and procedures to ensure that previous versions of the system are not 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.

Maintaining Data Integrity

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.6.1 requirements:

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.

Results

- The expected outcome for this review was that no issue would be found.
- 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 1.0 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.

Access Control

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.8.1 requirements:

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.

Results

- The expected outcome for this review was that no issue would be found.
- The actual outcome for this review was a determination that the solution successfully meets the requirements for access control.

Data Interception and Disruption

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.8.2 requirements:

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.

Results

- The expected outcome for this review was that no issue would be found.
- 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 that utilizes encryption of data transmissions between application containers for image processing and reporting. The connection between the IBML Scanner and the Common Internet File System (CIFS) file share, however, 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.

BURPSuite Professional results:

Target: https://192.168.7.80:9069 and https://192.168.7.80:9068

- 24 instances of Cross Site Scripting (DOM-based) opportunity in select components of the system. (High Severity) (Tentative confidence) Potentially a false positive as the confidence is set to tentative.
- 1 instance of SSL Certificate opportunity in the system, (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.
- 24 instances of Client-side JSON injection (DOM-based) opportunity in select components of the system. (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.
- 2 Instances of Strict transport security not enforced. (Low Severity) (Certain confidence). This allows a potential attacker to modify legitimate user network traffic to bypass application use of SSL/TLS encryption.
- 50 instances of Information rated vulnerabilities.

Phase III – Telecommunications and Data Transmission Testing

Phase III testing included testing of system communications, including encryption of data, as well as protocols and procedures for access authorization

During Phase III testing, tests were exercised in order to verify and validate the following requirements in accordance with the applicable California Voting System Standards (CVSS):

- Data transmission
- Confirmation

Data Transmission

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 6.1.2 requirements

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.

Results

- The expected outcome for this review was that no issue would be found.
- 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.

Confirmation

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 6.2.1 requirement:

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.

Results

- The expected outcome for this review was that no issue would be found.
- The actual outcome for this review was a determination that official displayed confirmation of successful transmission between the IBML scanner and the Linux CIFS file server is not available. It was determined that if there are bandwidth limitations, mechanical failure, or write errors to the CIFS file server, the scanner user is presented with a halt message,

irrespective of the error or condition experienced. An example of a message is one indicating the max queue length had been exceeded and that scanning would resume after the queue has finished transmitting. Successful and unsuccessful transmission messages between the CIFS file server and the VSAP Tally 1.0 services containers are logged in the Receiver audit logs; however, as each ballot was received, there were no visual messages except for the different Tally Queue number fluctuation.

Phase IV – Onsite Testing

Phase IV consisted of an onsite visit to the Los Angeles County vote center.

Phase IV testing included:

- Testing of relevant software and operating system configuration for pertinent vulnerabilities
- Testing of hardware, including examination of hardware for unused ports and the security measures applied to those ports
- Examination of physical environment

During Phase IV the production environment was examined to verify and validate the following requirements:

- In-process audit records
- General access control
- Access control identification
- Access control authentication
- Physical security measures
- Central count location security
- Telecommunications and data transmission
- Access control

In-process Audit Records

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 5.4.3 requirements:

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

Results

- The expected outcome for this review was that no issue would be found.
- 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.

General Access Control

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.2.1 requirements:

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 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.

Results

- The expected outcome for this review was that no issue would be found.
- 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.

Access Control Identification

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.2.2 requirements:

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

- The expected outcome for this review was that no issue would be found.
- 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.

Access Control Authentication

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.3 requirements.

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 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 controls related to the handling of ballot boxes, preparing of ballots for counting, counting operations and reporting data.

Results

- The expected outcome for this review was that no issue would be found.
- 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.

Physical Security Measures

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.3 requirements:

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.

Results

- The expected outcome for this review was that no issue would be found.
- The actual outcome for this review was a determination that the system sufficiently meets the requirements for physical security.

Central Count Location Security

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.3.2 requirement:

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

- The expected outcome for this review was that no issue would be found.
- 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 maintaining such a log including where it's stored and who has access to the log is needed.

Data Transmission

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 6.1.2 requirements

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.

Results

- The expected outcome for this review was that no issue would be found.
- 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.

Access Control

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.8.1 requirement:

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.

Results

- The expected outcome for this review was that no issue would be found.
- The actual outcome for this review was a determination that the solution successfully meets the requirements for access control.

Data Interception and Disruption

The LA County VSAP Tally 1.0 system was examined for compliance with the following CVSS 7.8.2 requirement:

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.

Results

- The expected outcome for this review was that no issue would be found.
- 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.

Security Findings

This section discusses any Findings from the LA County VSAP Tally 1.0 system review, as well as potential impacts.

Documentation Review Discrepancies

During the security documentation review of the VSAP Tally 1.0 system, it was determined that the documentation addressed, in some way, all of the requirements.

However, in some of the cases it was determined that some of the documentation was vague or warranted additional comment:

- 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.
- 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.
- 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.
- 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.
- 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 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.

Functional Review Discrepancies

During the functional security testing of the VSAP Tally 1.0 system the following findings were discovered:

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.

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 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.

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.

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.

Telecommunications and Data Review Discrepancies

During the telecommunications and data transmission testing of the VSAP Tally 1.0 system, it was determined that the transmission process does not currently encrypt data transmissions end to end and the connections between the IBML scanner and the CIFS file server are not encrypted. Connectivity between the VSAP Tally 1.0 containers and the User interface are all encrypted using OpenSSL.

It was also noted that there are no displayed confirmations of successful transmissions of scanned ballots to the (Common Internet File System) CIFS file server. There are, however, visible messages if an error is encountered notifying the scan operator that there is an issue with the current scan process. An example of messages observed were: (1) the queue limit exceeded message where too many ballots were in the queue waiting to be transferred, and (2) an unsuccessful write message. It should be noted that the VSAP Tally 1.0 system records all of the transmission messages concerning ballot images, (successful, failed, and out-stacked) in the Receiver audit logs.

Another observation is that Server Message Block (SMB) signing is not configured which may allow man-in-the-middle style attacks against CIFS file servers if the opportunity was presented. The impact of this finding is negligible due to the fact

that the environment is protected by a stringent air gapped network configuration and the SMB signing may have been intentionally disabled to prevent performance issues.

Onsite Review Discrepancies

During the onsite security review of the VSAP Tally 1.0 system:

- It was confirmed that during operations, the systems within the Scanner environment as well as the systems within the VSAP Tally 1.0 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.
- The connection between the IBML Scanner and the CIFS file share is not currently encrypted.
- The SMB signing is not configured which may allow man-in-the-middle style attacks against CIFS file servers if the opportunity was presented. The impact of this finding is negligible due to the fact that the environment is protected by a stringent air gapped network configuration and the SMB signing may have been intentionally disabled to prevent performance issues.
    - Observation: No specific details pertaining to the security measures for network switching equipment were provided. Security practices were observed for the air gapped network that help to enhance the overall security of the solution but were not listed anywhere in the documentation.
    - 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 procedures for maintaining such a log including where it's stored and who has access to the log is needed.

Vulnerabilities

Should any vulnerability be discovered, SLI identifies the particular requirement 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 machine design and configuration. May carry out attacks designed by others. They have access to the machine(s) for less than an hour.
- Poll worker: Usually has low knowledge of the voting machine design and configuration. Some may have more advanced knowledge. May carry out attacks designed by others. They have access to the machine(s) for up to one week, but all physical security has been put into place before the machines are received.
- Elections official insider: Usually has a wide range of knowledge of the voting machine design and configuration. May have unrestricted access for long periods of time. Their designated activities include:
  - Set up and pre-election procedures;
  - Election operation;
  - Post-election procedures; and
  - Archiving and storage operations.
- Vendor insider: Usually has great knowledge of the voting machine design and configuration. They have unlimited access to the machine before it is delivered to the purchaser and, thereafter, may have unrestricted access when performing warranty and maintenance service and when providing election administration services.

SLI does not verify or demonstrate exploitability of the vulnerability but the report of the vulnerability will identify factors involved in the exploitation.

Any vulnerability theories developed review team members shall, to the extent possible, be referred to the Secretary of State staff.

Documentation Review Vulnerabilities

During the security documentation review of the VSAP Tally 1.0 system, it was determined that there were no specific vulnerabilities found. The system documentation covers all the CVSS requirements; however, in some cases the documentation could be improved to provide more thorough information.

Functional Review Vulnerabilities

During the functional security testing of the VSAP Tally 1.0 system, it was determined

BURPSuite Professional Results:

Target: https://192.168.7.80:9069 and https://192.168.7.80:9068

- 24 instances of Cross Site Scripting (DOM-based) opportunity in select components of the system. (High Severity) (Tentative confidence) Potentially a false positive as the confidence is set to tentative.
- 1 instance of SSL Certificate opportunity in the system, (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.
- 24 instances of Client-side JSON injection (DOM-based) opportunity in select components of the system. (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.
- 2 Instances of Strict transport security not enforced. (Low Severity) (Certain confidence). This allows a potential attacker to modify legitimate user network traffic to bypass application use of SSL/TLS encryption.
- 50 instances of Information rated vulnerabilities.

Telecommunications and Data Review Vulnerabilities

During the telecommunications and data transmission testing of the VSAP Tally 1.0 system, it was determined Nessus® Vulnerability scans indicated the following results:

- 10% Medium vulnerabilities
- 3% Low vulnerabilities
- 86% Informational vulnerabilities

Medium Vulnerabilities:

Five SSL vulnerabilities that relate to the use of self-signed SSL certificates. In the proposed/tested environment, the impact of these vulnerabilities is negligible and does not negatively impact the overall security of the solution's networked environments.

Three SMB Signing not required that could allow an unauthenticated remote attacker to conduct man-in-the-middle attacks against the SMB server shared. It should be noted that SMB signing could negatively impact performance on the SMB server due to having to sign and verify each packet. In the proposed/tested environment, the impact of this vulnerability is negligible and does not negatively impact the overall security of the solution's networked environments.

Low vulnerabilities:

Three SSH Server CBC mode ciphers enabled may allow attackers to recover plaintext from cipher text when using SSH for server connections. In the proposed/tested environment, the impact of this vulnerability is negligible and does not negatively impact the overall security of the solution's networked environments.

SSL RC4 cipher suite supported. This indicates that the RC4 cipher that was compromised may allow an attacker to recover plaintext from cipher text if the cipher is used. In the proposed/tested environment, the impact of this vulnerability is negligible and does not negatively impact the overall security of the solution's networked environments.

Informational Vulnerabilities:

The rest of the vulnerabilities are informational and cover informational details about each system scanned. These vulnerabilities are of informational use only and in most cases are only used as reconnaissance information about the target system.

Onsite Review Vulnerabilities

During the onsite Security review of the VSAP Tally 1.0 system, it was determined Nessus® Vulnerability scans of the entire networked solution indicated the following results:

- 10% Medium vulnerabilities
- 3% Low vulnerabilities
- 86% Informational vulnerabilities

Medium Vulnerabilities:

Five SSL vulnerabilities that relate to the use of self-signed SSL certificates, in the proposed/tested environment, the impact of these vulnerabilities is negligible and does not negatively impact the overall security of the solution's networked environments.

Three SMB Signing not required that could allow an unauthenticated remote attacker to conduct man-in-the-middle attacks against the SMB shared server. It should be noted that SMB signing could negatively impact performance on the SMB server due to having to sign and verify each packet. In the proposed / tested environment, the impact of this vulnerability is negligible and does not negatively impact the overall security of the solution's networked environments.

Low vulnerabilities:

Three SSH Server CBC mode ciphers enabled may allow attackers to recover plaintext from cipher text when using SSH for server connections. In the proposed/tested environment, the impact of this vulnerability is negligible and does not negatively impact the overall security of the solution's networked environments.

SSL RC4 cipher suite supported. This indicates that the RC4 cipher that was compromised may allow an attacker to recover plaintext from cipher text if the cipher is used. In the proposed / tested environment, the impact of this vulnerability is negligible and does not negatively impact the overall security of the solution's networked environments.

Informational Vulnerabilities:

The rest of the vulnerabilities are informational and cover informational details about each system scanned. These vulnerabilities are of informational use only and in most cases are only used as reconnaissance information about the target system.

Conclusion

Five minor findings were located within the security documentation review portion of the LA County VSAP Tally 1.0 system documentation review related to vague or partially missing documentation. Overall, each of the requirements is addressed in the documentation though in some cases more documentation may be required to sufficiently detail system capabilities to meet the requirements.

No Vulnerabilities were located within the security documentation review portion of the LA County VSAP Tally 1.0 system.

Three findings were written during the telecommunications and data transmission testing portion of the LA County VSAP Tally 1.0 system. However, the impact to the overall security posture of the solution as a whole is minimal. Partial transmission encryption, no SMB signing on CIFS file shares, and no visual transmission successful messages.

In total there were fifty eight distinct vulnerabilities located within the telecommunications and data transmission testing portion of the LA County VSAP Tally 1.0 system.

Six 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

Two low severity vulnerabilities:

1. SSH Server CBC mode ciphers enabled
2. SSL RC4 cipher suites supported.

Fifty 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.

Four findings were located within the functional security testing portion of the LA County VSAP Tally 1.0 system:

CVSS 7.4.2 requires that malicious software protection software be in use on the current voting system, in the case of the VSAP Tally 1.0 solution, a choice to forgo anti-virus and malicious software protection was made to maintain performance requirements. The mitigation steps include scanning for both vulnerabilities and malicious software prior to being introduced to the solution network environment. Includes stringent air gap network management and monitoring including physical security measures such as lock/key for server rack access and all accessible USB ports are disabled or have security seals.

CVSS 7.4.6 requires extensive software validation for installation and verification of voting software solutions onto equipment. The outcome of the review is that the system provides verification of VSAP Tally 1.0 installation files, and Docker container for every instance of a Docker container created. The process also includes verification of all COTS software installation files prior to being deployed.

- 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 system utilizes processes and procedures and physical security and access controls to prevent previous versions of the system are not 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.

CVSS 7.6.1 requires that voting systems that utilize telecommunications to communicate between system components have the same security requirements as other system hardware and software and data function.

- The system scans already marked ballots which are then processed by the VSAP Tally 1.0 system.
  - No checksums or message digests are used to validate scanned ballot images.
  - No standard error detection or correction methods were observed.

CVSS 7.8.2

- 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.
  - 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.

Vulnerabilities were located within the functional security testing portion of the LA County VSAP Tally 1.0 system that were determined to have a low impact to the overall security of the system due to the extended measures taken to provide an air gapped central count network. All of the vulnerabilities found require that unauthorized devices or equipment be in place to intercept and or attack the systems on a closed isolated network.

Three Findings and two observations were located within the Onsite security testing portion of the LA County VSAP Tally 1.0 system. The impact to the overall security posture of the solution as a whole is minimal.

In total there were fifty eight distinctive vulnerabilities located within the telecommunications and data transmission testing portion of the LA County VSAP Tally 1.0 system.

Six distinctive 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

Two low severity vulnerabilities:

1. SSH Server CBC mode ciphers enabled
2. SSL RC4 cipher suites supported.

Fifty 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.

Final Report

Some issues are of note, as listed in the “Conclusion” section above, though none that are not able to be mitigated.

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

End of Security and Telecommunications Test Report