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

County of Los Angeles'
Voting Solutions for All People (VSAP) Tally 2.0 Voting System

Staff Report

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

December 24, 2019

Table of Contents

I. INTRODUCTION

1. Scope

This report presents the test results for all phases of the certification test of the County of Los Angeles' Voting Solutions for All People (VSAP) Tally 2.0. The purpose of the testing is to test the compliance of the voting system with California and federal laws, including the California Voting System Standards (CVSS). Testing also uncovers other findings, which do not constitute non-compliance, and those findings are reported to the County of Los Angeles to address the issues procedurally. The procedures for mitigating any additional findings are made to the documentation, specifically the County of Los Angeles' VSAP 2.0 Use Procedures.

2. Summary of the Application

The County of Los Angeles submitted an application for the VSAP Tally 2.0 voting system on November 6, 2018. The system is comprised of the following major components:

a. Tally 2.1.3.27

b. Ballot Marking Device (BMD) A0.2

c. FormatOS Version 0.19.0

d. BMD BASI Version 0.19.0

e. BMD BESI Version 0.19.0

f. BMD Manager (BMG) Version 0.19.0

g. VSAP Ballot Layout (VBL) 1.0-8ddf61d

h. Enterprise Signing Authority (ESA)

i. IBML - ImageTrac 6400

In addition to each of the aforementioned components, which includes the executable code and the source code, the County of Los Angeles was required to submit the following: (1) the technical documentation package (TDP); (2) all the hardware and software components, including all peripheral devices needed for all phases of testing; (3) and the VSAP Tally 2.0 Use Procedures.

3. Contracting and Outsourcing

Upon receipt of a complete application, the Secretary of State released a Request for Quote (RFQ) for assistance with testing of the VSAP 2.0 voting system.

Through the formal California contracting process, the Secretary of State awarded a contract to the Freeman Craft McGregor Group (FCMG). Atsec, a sub-contractor of FCMG, performed the Software Testing (Source Code Review), and hardware testing of the ballot marking devices was subcontracted by FCMG to National Technical Systems (NTS) Laboratories.

II. SUMMARY OF THE SYSTEM

The VSAP Tally 2.0 consists of the following components:

- **Tally 2.1.3.27 —**Hardware and software that captures and processes ballot images ensuring that votes on paper ballots are digitally represented and counted, storing the images as Cast Vote Records (CVRs).
- **Ballot Marking Device (BMD), Unit Ver. A0.2—**The central component of the voting system and the main interface for the voter. It includes a touchscreen, an audio-tactile interface, a paper handler, a QR code scanner, a dual-switch input, and an integrated ballot box. The BMD is used by voters to generate, verify, and cast paper ballots.
- **FormatOS Version 0.19.0 –** Application used to wipe new BMD devices.
- **BMD BASI Version 0.19.0 –** Application software for the BMD**.**
- **BMD BESI Version 0.19.0 –** Application for election software for BMD.
- **BMD Manager (BMG) Version 0.19.0 —** Ballot marking device manager application for managing BMDs including software, ballot configurations, and post-election data.
- **VSAP Ballot Layout (VBL) 1.0-8ddf61d—**Defines ballot print formats for BMD, Vote by Mail (VBM), Remote Accessible Vote by Mail (RAVBM) and Uniformed Overseas Citizens Absentee Voting Act (UOCAVA) ballots. VBL also generates data files and packages to configure the BMD, BMG, ISB, and Tally.
- **Enterprise Signing Authority (ESA)—**A cryptographic sub-system (hardware and software) that ensures components of the VSAP conform to security standards and that the data passed to components is secure and authenticated.

- **IBML - ImageTrac 6400** – High speed scanner used in conjunction with Tally tabulation software.

III. TESTING INFORMATION AND RESULTS

1. Background

The Secretary of State staff in conjunction with the FCMG, oversaw all phases of testing of the system, including Functional, Software Testing (Source Code Review), Security and Telecommunications (Red Team Penetration Testing), Volume, and Accessibility, Usability and Privacy Testing, and Hardware Testing.

2. Functional Testing Summary

System Configuration:

The system is self-contained on an air gapped network, per the CVSS requirements. Secretary of State staff witnessed the build of the test environment utilizing the county provided Use Procedures. The build was completed by staff of the FCMG. The artifacts produced, will be kept, and distributed by the Secretary of State. This version is solely for the use of Los Angeles County.

Functional Testing:

The first phase of Functional Testing consisted of following the Use Procedures to import the following four (4) test elections into the environment:

- Presidential Primary (2016 Election) – This election tested the limitations of ballot styles that can be used within the system.
- General Election (Los Angeles County)
- Recall Election (2003 Election) – This election tested the capacity to list 135 candidates.
- Fictional Election – A special election with two congressional districts and one municipality.

Temporary workers hand marked each of the ballots, including some marginal marks to test out stacking functionality. Each election was tabulated using the IBML high speed scanner, and produced the results as expected.

A detailed report of the Functional Testing conducted on the system can be found on our website.

3. Software Testing (Source Code) Review Summary

The review was conducted by Atsec. Atsec evaluated the security and integrity of the voting system by identifying any security vulnerabilities that could be exploited to:

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

Atsec's review of the source code, uncovered twenty-six (26) findings, ranging from no severity to low. Of the twenty-six, fourteen (14) of the findings required a mitigation and/or response. The following table **3A: Source Code Findings, details the findings and the responses provided by the county.**

#	Assessment	County Response	Severity
1	Non-compliance with voting system requirements. The CVSS section 2.4.4.1 requires a FIPS 140-2 validated module. The doc.go file and other documentation states that CentOS 7.6.1810 is the Operating System in use. This is not one of the Operating Environments listed in CMVP certificate 1747 for the OpenSSL module.	"The Tally and VBL systems use open SSL as packaged and distributed by CentOS. The Cryptohelper library (written by the same team as Tally) abstracts the use of OpenSSL to make it safer to work with and ensure it is always put in FIPS mode. The version of OpenSSL being used is "openssl-1.0.2k-16.el7_6.1.x86_64.rpm" as found in the installer repo at "rpms/yums/x86_64/7/updates/packages/openssl-1.0.2k-16.el7_6.1.x86_64.rpm" Tally and VBL use the Red Hat FIPS verified OpenSSL package (openssl-1.0.2k-16.el7_6.1.x86_64.rpm as distributed by CentOS. CVSS only requires that the module is verified and not that the cryptographic module is running on a FIPS verified hardware configuration."	Low
2	Non-compliance with voting system requirements. The crypto code documented in VSAP-TDP-005_ System_ Security_ Specification section 9.3 is in historical status for using AES and Triple-DES key wrapping, the OpenSSL module is not documented. Not all of the cryptographic requirements defined in the CVSS document	In reference to section 2.4.4.2 of the CVSS: "This is only a CVSS requirement when tabulating DRE generated ballot images. Note that the requirement for the DRE recording ballots in a randomized order is outlined in section 7.7.3 and note that all of 7.7 is specific to DREs. This section contains requirements for DREs with a Voter Verifiable Paper Audit Trail (VVPAT) component... Due to VSAP being a paper based system Tally is not subject to this requirement." In reference to section 7.6.1 of the CVSS: "CVSS requires detection of transmission errors and, when encryption is used, it must be NIST	Low

#	Assessment	County Response	Severity
	appear to be met.	approved and at least 112 bits ("This should include standard transmission error detection and correction methods such as checksums or message digest hashes"). All messages passed over the network are transmitted over TCP/IP which provides built in integrity checks. Additionally, much of the data transferred is over TLS with its own checksums. All images are further signed on disk when ingested into Tally. Nothing in this section requires encryption or MAC usage in any particular part of the system, just that the cryptography must be strong when used." In reference to section 9.6.7 of the CVSS: "We are working with Smartmatic to provide an updated TDP that aims to clarify and document these questions better. Please let us know if that does not adequately address these questions."	
3	Non-compliance with voting system requirements. The CVSS section 2.4.4.1 requires FIPS 140-2 validated module. The use of BcryptPasswordEncoder and java.security.X509Certificate functions do not appear to be FIPS 140-2 certified. The crypto code is not running in a a FIPS 140-2 approved environment.	"These findings relate to the CMVP listings at NIST for this combination of hardware and software. A discussion with the State is requested."	Low
4	Non-compliance with voting system requirements. The CVSS section 2.4.4.1 requires FIPS 140-2 validated module. The use of Bcrypt functions do not appear to be FIPS 140-2 certified. The crypto code is not running in a a FIPS 140-2 approved environment.	"These findings relate to the CMVP listings at NIST for this combination of hardware and software. A discussion with the State is requested."	Low
5	Use of third-party code is not in and of itself a finding, but great care must be taken to ensure malicious functionality is not introduced into code	All third party code is reviewed before implementation into the system. Will continue to monitor potential threats/risks with third party software. Can provide review results of third party code.	Low (reduced from Medium due to response)

#	Assessment	County Response	Severity
	not under local control. All changes should be reviewed, no code should be included in the system automatically. The volume of third-party code and the variety of sources from which it is obtained is the finding because of the increased possibility for attack. Risk may be considered acceptable provided all new code is reviewed and all imported code is verified at the time of import. Any automatic import of code from a third-party repository (e.g., GitHub) without confirmation that the content is as expected would allow for malicious injection of functionality.		
6	The initial state of the BMG could be unrecoverable or badly formed data could be imported because no errors are generated. MySQL will instead of failing on a bad insert, simply **convert** the data into a format that fits. In other words: INSERT IGNORE can lead to incorrect data imported into the database. Bugs generated from it could be potentially missed, and therefore abused by a malicious attacker. See data should be properly formatted to avoid insertion failures, therefore the use of INSERT IGNORE is inappropriate.	The word 'needed' in this context should be taken as 'used'. Moreover, this script is used only once during deployment, and the results obtained during the tests performed are successful.	Low
7	MySQL allows for adjusting sql_mode, such that group by restrictions aren't maintained, which could lead to "random"	The results obtained with the current BMG version code against these settings are successful. Removing this setting may cause issues.	Low

#	Assessment	County Response	Severity
	results being obtained from incorrect queries. This vulnerability applies to versions of MySQL prior to 5.7.5. sql_mode should not be altered, so that non-deterministic queries, and therefore unpredictable values, are not returned to BMG.		
8	The higher potential warnings are included in an accompanying text file to this finding (i.e. same name but with a .txt extension). These should be reviewed by the development team to determine whether they could represent any issue.	"The number of errors that are being reported are partially due to the repos being copied over several times. Based on the feedback there appears to be: ● 3 copies of the Tally source code (2 old and 1 current) ● 4 copies of the Auth source code (2 old and 2 current) ● 5 copies of the Logviewer source code (3 old and 2 current) ● 3 copies of the Ballot Layout source code (2 old and 1 current) This increases the apparent number of errors, since the majority of the issues identified are duplicated across each copy of the repo. With regards to the issues called out, all paths reviewed were inside /vendor. In Go, the vendor path is used for external dependencies (e.g. third party libraries) that were not authored by the Tally/VBL/VSAP teams. All items listed below are stock third party and occur in at least one of the following repositories: **Tally** ● OLD/TDA3.local/OLD/tally-core/tally-core/vendor (appears to not be latest code) ● OLD/TDA3.local/tally-core/tally-core/vendor/ (appears to not be latest code) ● TallySource/tally-core/vendor/ **Auth** ● OLD/TDA3.local/auth-service/auth-service/vendor (appears to not be latest code) ● OLD/TDA3.local/OLD/auth-service/auth-service/vendor (appears to not be latest code) ● TallySource/auth-service/vendor/ ● VBL_source_and_Keys/auth-service/vendor/ Log viewer ● OLD/TDA1.local/logviewer-service/logviewer-service/vendor (appears to not be latest code)	Low (reduced from Medium due to response)

#	Assessment	County Response	Severity
		● OLD/TDA3.local/logviewer-service/logviewer-service/vendor (appears to not be latest code) ● OLD/TDA3.local/OLD/logviewer-service/logviewer-service/vendor (appears to not be latest code) ● TallySource/logviewer-service/vendor/ ● VBL_source_and_Keys/logviewer-service/vendor/ **Ballot Layout** ● OLD/TDA1.local/ballot-layout/ballot-layout/vendor/ ● OLD/TDA1.local/ballot-layout/vendor/ ● VBL_source_and_Keys/ballot-layout/vendor/ These entries are: **Warning: "exported method (or func) * returns unexported type *, which can be annoying to use":** These items are test code: Shopify/sarama/mockresponses.go:29:59: Shopify/sarama/mockresponses.go:61:60: Shopify/sarama/mockresponses.go:105:64: Shopify/sarama/mockresponses.go:164:62: Shopify/sarama/mockresponses.go:240:61: Shopify/sarama/mockresponses.go:324:71: Shopify/sarama/mockresponses.go:373:70: Shopify/sarama/mockresponses.go:420:67: Shopify/sarama/mockresponses.go:477:62: Shopify/sarama/mockresponses.go:530:66: Shopify/sarama/mockresponses.go:550:67: Shopify/sarama/mockresponses.go:569:67: Shopify/sarama/mockresponses.go:588:71: Shopify/sarama/mockresponses.go:607:68: Shopify/sarama/mockresponses.go:630:70: Shopify/sarama/mockresponses.go:656:67: Shopify/sarama/mockresponses.go:677:65: Shopify/sarama/mockresponses.go:695:63: Shopify/sarama/mockresponses.go:717:65: stretchr/testify/mock/mock.go:620:32 testify/mock/mock.go:532:32 Production code written to allow for testing: gocql/gocql/host_source.go:286:30: gocql/gocql/host_source.go:299:28 hashicorp/go-sockaddr/ifaddrs.go:46:49 hashicorp/go-sockaddr/route_info_bsd.go:17:22 hashicorp/go-sockaddr/sockaddrs.go:32:45 modern-go/reflect2/reflect2.go:136:27 k8s.io/apimachinery/pkg/util/strategicpatch/types.go:48:50 k8s.io/apimachinery/pkg/util/strategicpatch/types.go:111:51	

#	Assessment	County Response	Severity
		Although the linter is correct that this can be annoying, this is done intentionally in test code where a mock object is returned that implements the same interface as the real object to allow for better control and injection of test harnesses into unit test code. In production code this pattern allows unit tests to simulate the state the code under test is running in to better check code behavior. **Warning: "a blank import should only be in a main or test package, or have a comment justifying it":** This error only occurs in support packages officially published by the Go team (although it occurs in several copies of the tally-core repo that were scanned: golang.org/x/crypto/openpgp/read.go:10:2 golang.org/x/crypto/openpgp/packet/public_key.go:15:2 golang.org/x/crypto/ssh/common.go:15:2 The same warning**: "a blank import should be only in a main or test package, or have a comment justifying it"** does occur once in a library that the ballot layout team has modified. This code ("bitbucket.org/vsap/pdf/image_obj.go:7:2") occurs three times in the scan results as the results seem to include three copies of the VBL repo. Although this is a library that we had to modify, this file remains unchanged. When updating the library, it was deemed safer to leave imports that we were not impacting alone rather than trying to change things that could have been done stylistically better."	
9	The higher potential warnings are included in an accompanying text file to this finding (i.e. same name but with a .txt extension). These should be reviewed by the development team to determine whether they could represent any issue.	"In this item, like 18, it appears that several repositories are mixed together. We are ignoring the "OLD/BMD_Code/", as that is not our area to respond. We are also ignoring: ● OLD/TDA1.local/ballot-layout/* ● OLD/TDA1.local/logviewer-service/* ● OLD/TDA1.local/vbl_deployment/* ● OLD/TDA3.local/OLD/auth-service/* ● OLD/TDA3.local/OLD/logviewer-service/* ● OLD/TDA3.local/OLD/tally-core/* ● OLD/TDA3.local/auth-service/* ● OLD/TDA3.local/logviewer-service/* ● OLD/TDA3.local/tally-core/* These paths/repos seem to have been superseded by: ● TallySource/auth-service/*	Low (reduced from Medium due to response)

#	Assessment	County Response	Severity
		● TallySource/logviewer-service/logviewer/* ● TallySource/tally-core/* ● VBL_source_and_Keys/auth-service/* ● VBL_source_and_Keys/ballot-layout/* ● VBL_source_and_Keys/logviewer-service/* Even here there is a significant amount of duplication, but it brings the total number of findings down to 91. Further review shows that these are actually only 13 distinct issues. Twelve are in Jquery in the file “jquery-3.2.1.min.js” ● 2:lint warning: useless comparison; comparing identical expressions ● 2:lint warning: the else statement could be matched with one of multiple if statements (use curly braces to indicate intent) ● 2:lint warning: the else statement could be matched with one of multiple if statements (use curly braces to indicate intent) ● 3:lint warning: the else statement could be matched with one of multiple if statements (use curly braces to indicate intent) ● 3:lint warning: the else statement could be matched with one of multiple if statements (use curly braces to indicate intent) ● 3:lint warning: the else statement could be matched with one of multiple if statements (use curly braces to indicate intent) ● 3:lint warning: the else statement could be matched with one of multiple if statements (use curly braces to indicate intent) ● 3:lint warning: useless comparison; comparing identical expressions ● 4:lint warning: the else statement could be matched with one of multiple if statements (use curly braces to indicate intent) ● 4:lint warning: the else statement could be matched with one of multiple if statements (use curly braces to indicate intent) ● 4:lint warning: the else statement could be matched with one of multiple if statements (use curly braces to indicate intent) ● 4:lint warning: unknown order of operations for successive plus (e.g. x+++y) or minus (e.g. x---y) signs Jquery is a major project. While we have not analyzed these findings code use cases, there seem to be no CVEs related to them. Additionally,	

#	Assessment	County Response	Severity
		this is checking *minified* code - meaning that it has been post processed to make it as small as possible. It appears that most of these warnings are stylistic to avoid confusion, as such, while valid in code that would be read by humans, are likely not relevant to minified source code as the computer will not treat them as ambiguous or unclear. There was also one identified issue in bootstrap-table.min.js (although it was identified multiple times) that appears to be the same case as the jQuery issues. bootstrap-table.min.js:7:lint warning: the else statement could be matched with one of multiple if statements (use curly braces to indicate intent) Like the jQuery issues above, this is likely due to scanning minified code."	
10	The system is air-gapped—that is, not connected to the internet or connected to any other system that is connected to the internet. Air gap systems include • Ballot Marking Device Manager (BMG) • Ballot Marking Device (BMD) • VSAP Ballot Layout (VBL) • Tally The following security products are used to facilitate the air-gapped environment: • Carbon Black Protection: Provides application control to lock down critical systems in order to prevent unwanted software changes and malicious attacks. • Cylance PROTECT: Threat prevention solution (anti-virus) which utilizes machine-learning, allowing the software to function in isolation from the internet or	CVSS speaks to the possibility that new, unforeseen vulnerabilities in voting systems may emerge during the system lifecycle. In several places (9.6.d and 9.6.3.g as two examples) CVSS requires planning to respond to new threats. The county will fulfill the letter and spirit of these clauses by ensuring that their System Integrator remains responsible for system maintenance.	Low

#	Assessment	County Response	Severity
	cloud connection. • HP Aruba ClearPass: Tracks machine (MAC) addresses of all network cards on the network and can remove unauthorized addresses. • Net Fort LANGuardian: Tracks movement of all software, users, and actions on the network. • Snare System Information and Event Management (SIEM): Records all computer system and network activities, which are available for review in the event of an attack or issue. • Thycotic Secret Server: Manages all administrative privileged network accounts and limits users to standard access, limiting opportunities for software changes. Note: Unused hardware ports (i.e. USB ports) are protected by port locks and/or tamper evident seals with signaling residue to reveal modification and/or removal. The serialized tamper evident seals are manually logged with an operator signature, seal number, location, date and time. This is to prevent removal of authorized connections when the port is in use and to prevent the insertion of unauthorized connections when the port is not in use. This prevents any infected USB flash drive from crossing any air gap.		

#	Assessment	County Response	Severity
11	Programmatic setting of permissions to highly open configuration, and source files are not deleted after being copied to destinations on cluster machines. Leaving a copy of the CA key in the temp folder of a multi-user operating system is an incorrect configuration of a CA or PKI infrastructure. Industry standard processes dictate that the root CA is created and stored on an air-gapped system, and intermediate CA's used to further certificate generation on destination machines. If this is the root CA in particular, then this is an inappropriate use case. If nothing else, the environment should be cleaned to prevent the CA from falling into the wrong hands.	"In practice, this isn't a significant risk as, although the operating system is multi-user, the machine cluster is single tenant running only the Tally (or VBL) system and only administrators on the Tally system should be authorized on the environment. Mitigation ● The documentation will be updated to instruct the installer user to delete all data from temp once the install is finished. ● A procedure has been added to restrict file system permissions on these files post-install."	Low
12	This configuration could allow someone to systematically try different authentication combinations until a valid one is found, leading to invalid voting data. Unless it's crucial that all users can login from all hosts, then the default template is too liberal in its use and definitions of who can login from where.	"The user must be able to log in from a docker container on one of several (currently about 9) Kubernetes cluster machines. Moving forward, we can look at ways to limit this host list, but at present this would appear to require making some significant assumptions about the details of the production environment (such as IP addresses) that pose a challenge. Moving forward we will look for better options to lock this down. We may be able to implement a manual procedure for more specific grants if this is deemed a high priority issue."	Low
13	While this does not represent an actual vulnerability, it has the potential to cause one in the future. Python 2 will not be supported or updated starting January 1. If any security vulnerabilities are found after that date, not only could they	"We reviewed open CVEs for Python 2.7 (the version used in the BMD) and found none that are scored in the 8, 9, and 10 range. We also note that the VSAP BMD remains under contracted Warranty for two years, and optional Maintenance beyond that timeframe. Python 2 vulnerabilities that might be found by researchers in the future would be dangerous if the product is off support, meaning that no one is available to assess the vulnerability and remediate it if deemed necessary. CVSS speaks to the possibility that	Low

#	Assessment	County Response	Severity
	put the voting system at risk, they would most likely not be fixed. Developers should already be in the process of migrating code to Python 3. Please see https://www.python.org/doc/sunset-python-2/ .	new, unforeseen vulnerabilities in COTS products may emerge during the system lifecycle. In several places (9.6.d and 9.6.3.g as two examples) CVSS requires planning to respond to new threats. At this late time in the Certification campaign, we do not see the ability to move to Python 3 in the BMD software; however, we plan to fulfill the letter and spirit of CVSS and will monitor for new vulnerabilities in Python 2 during the Warranty phase of VSAP lifecycle. Where deemed necessary by Los Angeles County, the system owner and operator, or the Secretary of State new Python 2 vulnerabilities will be remediated under the Warranty contract clauses."	
14	The potential problem with this configuration is simply that the container is running effectively as root. An attacker could use this to reboot the system, delete files, modify passwords, etc. The developer of the voting systems is off the hook for this setting; There is a bug report filed at the following URL, which is attempting to deal with this issue related to Calico: https://github.com/projectcalico/calico/issues/2000 That said, it should be mentioned as a future improvement for the voting system, as this level of access to a machine via container is unnecessary and dangerous.	"We agree that this is not an emergent finding, but a future system version could see this remediated."	Low

A Source Code Review report, including the findings and vendor responses and/or mitigations can be found on our website.

4. Security and Telecommunications Testing (Red Team) Summary

Security and Telecommunications (Red Team Penetration) testing of the VSAP 2.0 system was conducted in November of 2019, by FCMG. The Security and Telecommunications Testing resulted in four (4) findings requiring a response and/or mitigation. Each is described in **Table 4A: Security Findings**:

Table 4A: Security Findings	
Test Results	**County Mitigation/Response**
Locks and Tamper Evident Seals – The seals were removed without damage or evidence of tampering.	The county will address the finding by updating processes and procedures.
Unrestricted Access to Workstation Cases – The stations were not secured with tamper-evident labels or locks.	The county will address the finding by updating processes and procedures.
Ability to Boot from USB – Capability was not disabled on any of the systems tested.	The county will apply port protectors.
Lack of Fill Disk Encryption – No component of the system has full disk encryption.	The county has additional security safeguards in place to mitigate access to the system at large.

A detailed report of the Security and Telecommunications Testing (Red Team Penetration) can be found on or website.

5. Volume Testing Summary

The Volume Test simulates conditions in which the ballot marking devices would be used on Election Day. Approximately fifty (50) BMD units were tested during the volume test, with fourteen (14) temporary workers marking and casting one hundred (100) ballots per device. Two (2) of the units were used to test the capacity of the ballot box attached to the BMD units, by feeding an additional on hundred fifty (150) ballots beyond the initial one hundred (100) ballots. Twenty-nine (29) of the BMD units experienced ballot jams, approximately fifty-two (52), which fell into one of four (4) classifications. Two (2) of the BMD devices encountered and error best described as the screen turning all white and subsequently, unable to recover until the units were restarted.

A detailed Volume Test report, including error logs can be found on our website.

6. Accessibility, Usability and Privacy Testing Summary

The Accessibility, Usability and Privacy testing took place from September to November of 2019. Functional Accessibility took place from October 3 to October 4, 2019, with approximately eighteen (18) volunteer testers participating. The volunteers were from the Los Angeles County accessibility community. The BMD devices used for this test were programmed with the November 8, 2016 General Election. Each volunteer tester was asked to complete a voting session, using the BMD. Upon completion of the session, all volunteer testers were asked to participate in a post-test survey regarding their experience.

Voters consistently reported that they liked the new BMD. Most test voters felt that they could independently vote, without assistance. However, a few voters did note that there was some confusion between the audio ballot, and the text on the screen. The two were not aligned in some instances. Further, some voters reported long periods of silence, with the audio instructions, which led them to believe the voting session was over. Finally, several test voters experienced multiple paper jams and misfeeds.

A detailed Accessibility, Usability and Privacy Test Report, including the survey results, can be found on our website.

7. Hardware Testing Summary

NTS conducted Environmental and Dynamics Testing of the ballot marking devices. The first round of testing, a defective universal power supply (UPS) device caused one of the test results to be Non-Compliant. During a second round of testing, with a replacement UPS unit, the same test was completed successfully. All other hardware tests of the ballot marking devices passed each phase of the hardware testing.

A detailed Hardware Testing report can be found on our website.

IV. COMPLIANCE WITH STATE AND FEDERAL LAWS AND REGULATIONS

1. Elections Code Requirements

Six (6) sections of the California Elections Code, Sections 19101, 19203, 19204, 19204.5, 19205, and 19270, describe in detail the requirements any voting system must meet in order to be approved for use in California elections. These sections are described in detail and analyzed for compliance below.

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

- The system meets this requirement.

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

- The system meets this requirement.

c) §19101 (b) (3): The system shall be safe from fraud or manipulation.

- The system meets this requirement.

d) §19101 (b) (4): The system shall be accessible to voters with disabilities pursuant to section 19242 and applicable federal laws.

- The system meets this requirement.

e) §19101 (b) (5): The system shall be accessible to voters who require assistance in a language other than English if the language is one in which a ballot or ballot materials are required to be made available to voters pursuant to Section 14201 and applicable federal laws.

- VSAP 2.0 supports all 14201 languages. The system is capable of adding additional languages, to produce ballots or ballot materials, and accessible audio files pursuant to Section 14201, utilizing system functionality and outside translation.

f) §19203: The system shall use ballot paper that is of sufficient quality that it maintains its integrity and readability throughout the retention period specified in sections 1700 through 17306.

- The system meets this requirement.

g) §19204: The system shall not include procedures that allow a voter to produce, and leave the polling place with, a copy or facsimile of the ballot cast by that voter at that polling place.

- The system meets this requirement.

h) §19204.5: The Secretary of State shall not certify or conditionally approve a voting system that cannot facilitate the conduct of a ballot level comparison risk-limiting audit.

- The system meets this requirement.

i) **§19205 (a):** No part of the voting system shall be connected to the internet at any time.
   - The system meets this requirement.

j) **§19205 (b):** No part of the voting system shall electronically receive or transmit election data through an exterior communication network, including the public telephone system, if the communication originates from or terminates at a polling place, satellite location, or counting center.
   - The system meets this requirement.

k) **§19205 (c):** No part of the voting system shall receive or transmit wireless communications or wireless data transfers.
   - The system meets this requirement.

l) **§19270 (a):** The Secretary of State shall not certify or conditionally approve a direct recording electronic voting system unless the system includes an accessible voter verified paper audit trail.
   - The system meets this requirement.

2. **Elections Code Review**

1) **§305.5(b):** A paper cast vote record is a ballot only if the paper cast vote record is generated on a voting device or machine that complies with ballot layout requirements and is tabulated by a separate device from the device that created the paper cast vote record.
   - The system meets this requirement.

2) **§13109.7(a):** Notwithstanding Section 13109, for a period of three years commencing with the date that the county elections official for the County of Los Angeles declares that the voting system modernization project underway in 2018 is complete and ready for operation, the county elections official for the County of Los Angeles shall conduct elections using the alternate ballot order described in Section 13109.8.

   (b) The county elections official shall prepare a report regarding the effect of using the alternate ballot order for elections conducted during the time period described in subdivision (a). The report shall include, but not be limited to, the following information:
   (1) Statistics and information on the cost of transitioning to the use of the alternate ballot order.
   (2) The overall turnout of voters in the jurisdiction for each election conducted using the alternate ballot order.
   (3) For different contests listed on the ballot, including, but not limited to, local offices and local ballot measures, state offices and state ballot measures, and federal offices, the following information:
   (A) The turnout of voters for each contest.
   (B) The number of overvotes and undervotes for each contest.
   (C) The dropoff rates for each contest.

(4) Legislative recommendations.
(c) The report described in subdivision (b) shall, whenever possible, compare an election conducted pursuant to this section and using the alternate ballot order described in Section 13109.8 to similar elections conducted using the ballot order described in Section 13109 in the same jurisdiction or in a comparable jurisdiction.
(d) Three years after the declaration date described in subdivision (a), the county elections official shall submit the report described in subdivision (b) to the Secretary of State and to the Legislature in accordance with Section 9795 of the Government Code. The county elections official shall also post a publicly accessible copy of the report on the Internet Web site of the county elections official.
(e) Notwithstanding any other law, the county elections official may adjust ballot instructions to the extent necessary to comply with this section.
(f) Immediately after making the declaration described in subdivision (a), the county elections official shall post the declaration on his or her Internet Web site and send the declaration to the Secretary of State, the Secretary of the Senate, the Chief Clerk of the Assembly, and the Legislative Counsel.
(g) This section shall remain in effect only until the first January 1 that occurs at least four years after the declaration date described in subdivision (a), and as of that date is repealed.

- The system meets this requirement.

3) **§15360:** During the official canvass of every election in which a voting system is used, the official conducting the election shall conduct a public manual tally of the ballots tabulated by those devices cast in one percent of the precincts chosen at random by the elections official. If one percent of the precincts should be less than one whole precinct, the tally shall be conducted in one precinct chosen at random by the elections official.

   In addition to the one percent count, the elections official shall, for each race not included in the initial group of precincts, count one additional precinct. The manual tally shall apply only to the race not previously counted.

   – The system fully supports this requirement.

4) **§19300:** A voting machine shall, except at a direct primary election or any election at which a candidate for voter-nominated office is to appear on the ballot, permit the voter to vote for all the candidates of one party or in part for the candidates of one party and in part for the candidates of one or more other parties.

   – The system meets this requirement.

5) **§19301:** A voting machine shall provide in the general election for grouping under the name of the office to be voted on, all the candidates

for the office with the designation of the parties, if any, by which they were respectively nominated.

The designation may be by usual or reasonable abbreviation of party names.

- The system meets this requirement.

6) **§19302:** The labels on voting machines and the way in which candidates' names are grouped shall conform as nearly as possible to the form of ballot provided for in elections where voting machines are not used.
   - The system meets this requirement.

7) **§19303:** If the voting machine is so constructed that a voter can cast a vote in part for presidential electors of one party and in part for those of one or more other parties or those not nominated by any party, it may also be provided with: (a) one device for each party for voting for all the presidential electors of that party by one operation, (b) a ballot label therefore containing only the words "presidential electors" preceded by the name of the party and followed by the names of its candidates for the offices of President and Vice President, and (c) a registering device therefore which shall register the vote cast for the electors when thus voted collectively.

   If a voting machine is so constructed that a voter can cast a vote in part for delegates to a national party convention of one party and in part for those of one or more other parties or those not nominated by any party, it may be provided with one device for each party for voting by one operation for each group of candidates to national conventions that may be voted for as a group according to the law governing presidential primaries.

   No straight party voting device shall be used except for delegates to a national convention or for presidential electors.
   - The system meets this requirement.

8) **§19304:** A write-in ballot shall be cast in its appropriate place on the machine, or it shall be void and not counted.
   - The system supports this requirement.

9) **§19320:** Before preparing a voting machine for any general election, the elections official shall mail written notice to the chairperson of the county central committee of at least two of the principal political parties, stating the time and place where machines will be prepared. At the specified time, one representative of each of the political parties shall be afforded an opportunity to see that the machines are in proper condition for use in the election.

   The party representatives shall be sworn to perform faithfully their duties but shall not interfere with the officials or assume any of their duties. When a machine has been so examined by the representatives, it shall be sealed with a numbered metal seal. The representatives shall certify to the

number of the machines, whether all of the counters are set at zero (000), and the number registered on the protective counter and on the seal.

- The system supports this requirement.

10) **§19321:** The elections official shall affix ballot labels to the machines to correspond with the sample ballot for the election. He or she shall employ competent persons to assist him or her in affixing the labels and in putting the machines in order. Each machine shall be tested to ascertain whether it is operating properly.

- The system supports this requirement.

11) **§19322:** When a voting machine has been properly prepared for an election, it shall be locked against voting and sealed. After that initial preparation, a member of the precinct board or some duly authorized person, other than the one preparing the machines, shall inspect each machine and submit a written report. The report shall note the following: (1) Whether all of the registering counters are set at zero (000), (2) whether the machine is arranged in all respects in good order for the election, (3) whether the machine is locked, (4) the number on the protective counter, (5) the number on the seal. The keys shall be delivered to the election board together with a copy of the written report, made on the proper blanks, stating that the machine is in every way properly prepared for the election.

- The system supports this requirement.

12) **§19340:** Any member of a precinct board who has not previously attended a training class in the use of the voting machines and the duties of a board member shall be required to do so, unless appointed to fill an emergency vacancy.

- The system does not adversely impact this requirement.

13) **§19341:** The precinct board shall consist of one inspector and two judges who shall be appointed and compensated pursuant to the general election laws. One additional inspector or judge shall be appointed for each additional voting machine used in the polling place.

- The system does not adversely impact this requirement.

14) **§19360:** Before unsealing the envelope containing the keys and opening the doors concealing the counters the precinct board shall determine that the number on the seal on the machine and the number registered on the protective counter correspond to the numbers on the envelope.

Each member of the precinct board shall then carefully examine the counters to see that each registers zero (000). If the machine is provided with embossing, printing, or photography devices that record the readings of the counters the board shall, instead of opening the counter compartment, cause a “before election proof sheet” to be produced and determined by it that all counters register zero (000).

If any discrepancy is found in the numbers registered on the counters or the “before election proof sheet” the precinct board shall make, sign, and post a written statement attesting to this fact. In filling out the statement of return of votes cast, the precinct board shall subtract any number shown on the counter from the number shown on the counter at the close of the polls.

- The system supports this requirement.

15) **§19361:** The keys to the voting machines shall be delivered to the precinct board no later than twelve hours before the opening of the polls. They shall be in an envelope upon which is written the designation and location of the election precinct, the number of the voting machine, the number on the seal, and the number registered on the protective counter. The precinct board member receiving the key shall sign a receipt.

    The envelope shall not be opened until at least two members of the precinct board are present to determine that the envelope has not been opened.

    At the close of the polls the keys shall be placed in the envelope supplied by the official and the number of the machine, the number written on the envelope.

    - The system supports this requirement.

16) **§19362:** The exterior of the voting machine and every part of the polling place shall be in plain view of the election precinct board and the poll watchers.
    Each machine shall be at least four feet from the poll clerk’s table.

    - The system supports this requirement.

3. **Review of Federal Statutes or Regulations.**

a) The Voting Rights Act (VRA) of 1965, as amended (42 U.S.C. 1973), requires all elections in certain covered jurisdictions to provide registration and voting materials and oral assistance in the language of a qualified language minority group in addition to English. Currently in California, there are ten VRA languages (English, Spanish, Chinese, Hindi, Japanese, Khmer, Korean, Tagalog, Thai, and Vietnamese) as prescribed under the law.

- The system meets this requirement. The system’s paper ballots can be easily printed in these languages, as well as any others. Further, BMD can be programmed to display the ballot in any of these languages on the touch screen interface and to provide audio instruction in any of these languages.

b) The National Voter Registration Act of 1993 (42 U.S.C. 1973gg and 11 CFR 8) allows for the casting of provisional ballots through Fail-Safe Voting procedures.

- The system meets this requirement. Provisional ballots can easily be cast with this system. The BMD only marks ballots (or verifies the marking of a ballot), it has no impact on provisional voting.

c) The Voting Accessibility for the Elderly and Handicapped Act of 1984 (42 U.S.C. 1973ee through 1973ee-6) requires each political subdivision conducting elections within each state to assure that all polling places for federal elections are accessible to elderly and handicapped voters, except in the case of an emergency as determined by the state's chief election officer or unless the state's chief election officer: (1) determines, by surveying all potential polling places, that no such place in the area is accessible or can be made temporarily accessible, and (2) assures that any handicapped voter assigned to an inaccessible polling place will, upon advance request under established state procedures, either be assigned to an accessible polling place or be provided an alternative means of casting a ballot on election day.

- This system supports this requirement.

d) The Retention of Voting Documentation (42 U.S.C. 1974 through 1974e) statute applies in all jurisdictions and to all elections in which a federal candidate is on a ballot. It requires elections officials to preserve for twenty two months all records and papers which came into their possession relating to an application, registration, payment of a poll tax, or other act requisite to voting. Note: The US Department of Justice considers this law to cover all voter registration records, all poll lists and similar documents reflecting the identity of voters casting ballots at the polls, all applications for absentee ballots, all envelopes in which absentee ballots are returned for tabulation, all documents containing oaths of voters, all documents relating to challenges to voters or absentee ballots, all tally sheets and canvass reports, all records reflecting the appointment of persons entitled to act as poll officials or poll watchers, and all computer programs used to tabulate votes electronically. In addition, it is the Department of Justice's view that the phrase "other act requisite to voting" requires the retention of the ballots themselves, at least in those jurisdictions where a voter's electoral preference is manifested by marking a piece of paper or by punching holes in a computer card.

- The system meets this requirement. All votes in this system are recorded on paper ballots that can be easily retained.

4. **Help America Vote Act (HAVA) Requirements**

The Help America Vote Act (HAVA) §301(a) mandates several requirements for voting systems, including:

1) The ability to verify the vote choices on the ballot before that ballot is cast and counted,
2) Notification to the voter of over-votes on a ballot,
3) Auditability with a permanent paper record of votes cast,
4) Accessibility for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence)

   – This system supports these requirements in the following manner:

      a) The paper ballots themselves lend themselves to visual inspection and verification.
      b) The BMD provides its users with a ballot review screen prior to printing the ballot. Further, any voted ballot can be inserted into the unit for review and verification.
      c) The BMD prevents over-voting a contest.
      d) Because all ballots in this system are paper based, there is a fully auditable and permanent record of the election.
      e) Deployment of the BMD in a precinct provides accessibility for persons with disabilities at the polling place.

V. CONCLUSION

The VSAP Tally 2.0 voting system, in the configuration tested and documented by the County of Los Angeles' Use Procedures, meets all applicable California and federal laws. The County of Los Angeles' VSAP Tally 2.0 voting system is compliant with all applicable California and federal laws.