FREEMAN, CRAFT, MCGREGOR GROUP

Functional Test Report

County of Los Angeles

VSAP Version 2.0 Voting System

California SOS Contract #18S52064

Prepared for the California Secretary of State December 24, 2019

Table of Contents

Date	Name	Comment	Version
12/7/2019	Kate McGregor and Paul Craft	Initial draft	1.0
12/16/19	Paul Craft	Edit	1.1
12/22/19	Kate McGregor	Edit	1.2
12/22/19	Paul Craft	Review and Format	1.2
12/24/19	Kate McGregor	Revising after client comments	1.3
12/24/19	Paul Craft	Review and Format	1.3

Introduction

This Functional Test Report describes functional testing of the Los Angeles County (the County) Voting System for All People (VSAP) version 2.0 under the California Voting Systems Standards (CVSS) and provides the results of those tests.

Scope of Work and Reporting

Functional Tests are designed to evaluate the system's conformance with Section 2 of the CVSS and hardware functional requirements within Section 4 of the CVSS. Evaluation of conformance to other sections of the CVSS are provided in other reports including the Software Testing Report, Security and Telecommunications Report, Hardware Test Reports Usability, Accessibility, and Privacy Report and Volume Test Report.

This report is in the style of an exception report, describing those instances in which system functionality during testing deviated from that required by the CVSS. We are not attorneys and do not offer legal advice. The tests were conducted to assist the California Secretary of State (SOS) with collection of facts and evidence in order for them to make certification decisions. However, to advise the SOS on the determination of whether the system complies with California's certification requirements would require an interpretation of law. This report does not provide recommendations or offer any opinion as to whether the system can be certified.

Description of System Submitted for Certification

The description of the system and the images in this section were provided by the County.

Brief Description

The system includes software, hardware devices, and peripheral components that allow election professionals to accomplish the following high-level tasks:

Pre-voting tasks:

- Vote by Mail Ballot data creation (VBL)
- Device preparation (FormatOS)
- Device configuration (BMG)

Voting tasks:

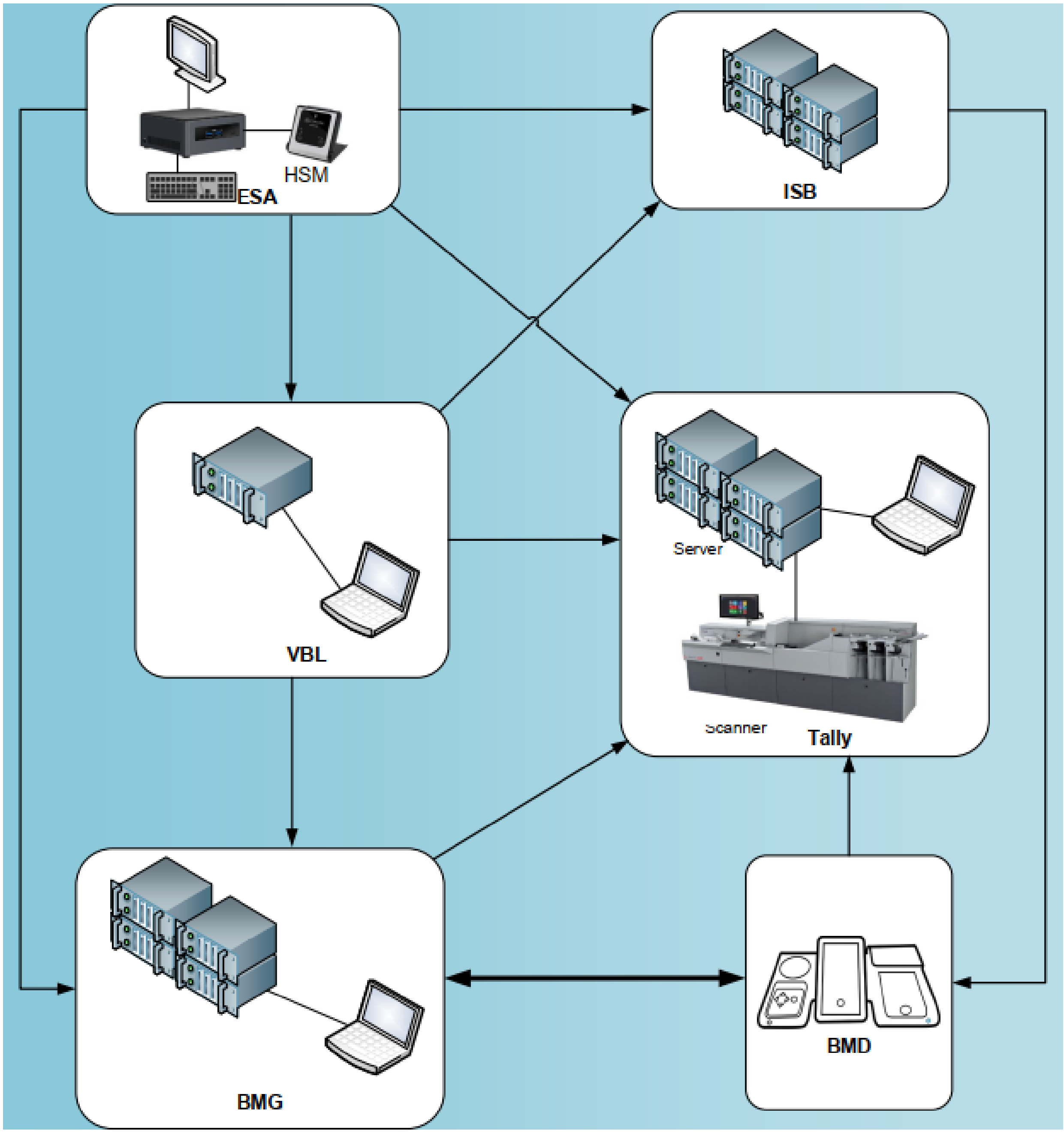
- Polling place voting using the Ballot Marking Device (BMD)

Post-voting tasks:

- Counting of votes/tabulation (Tally)
- Consolidation and reporting of results and audit logs (Tally and BMG)
- Audits and recounts

System Architecture

Overall system architecture is illustrated in the diagram below.



This diagram illustrates the following components:

VBL – VSAP Ballot Layout

Tally – VSAP Tabulation System

BMG – VSAP Ballot Marking Device Manager

BMD – VSAP Ballot Marking Device/Printer

NOTE: The HAS/ESA (Enterprise Security Authority), the ISB (Interactive Sample Ballot System), and the County Election Management System (not pictured) are out of scope for this report.

Hardware Components

All of the large system components of the VSAP system are multi-computer configurations with several computers processing in parallel and/or several computers handling different parts of the task. VSAP is built on an enterprise data center scale and, as such, is not directly comparable to other current typical voting systems. This will be explained in detail later in this document.

VBL

The VSAP ballot layout program takes the supplied election definition and generates the Vote by Mail (VBM) ballot styles in PDF form for printing. In Los Angeles County the number of styles can exceed 351,000 (4500 precincts, 13 languages, six parties for presidential preference elections).

BMD

The ballot marking device (BMD) is used for voting at the poll. The ballot style can be activated via a blank ballot with a ballot style QR code on it, via a poll pass – generated by the Interactive Sample Ballot system - with a QR code on it, or by the poll worker manually bringing up that style for the voter. All styles are loaded into all BMDs so any style valid for that election may be selected.

FormatOS

FormatOS is used only to initialize and/or rekey the BMDs. The BMD flash hard disk is formatted, and a public private key pair is generated by the BMD. The public key is sent to FormatOS along with the BMD's serial number and stored in a database. The contents of the database are then air-gap transferred to the BMG to facilitate TLS (Transaction Level Security) communication between each BMD and BMG.

BMG

The BMD Manager (BMG), is used to manage the BMDs. Initially, it loads the BMD Administrator Application System Image (BASI) and BMD Election Application System Image (BESI) operating systems then performs diagnostics and captures logs from each of the BMDs (the current system capacity is for approximately 30,000 BMDs). When the BMD checks out as operational, an election may be loaded. After an election is conducted, the logs may be recovered and diagnostics run again on the BMDs. Of course, other elections may be loaded.

Commercial Off-The-Shelf (COTS) Hardware Components

For a detailed listing of the system hardware used in the VSAP system, please refer to *VSAP-TDP-003 System Hardware Specification.pdf*, version 1 draft G in the VSAP Technical Data Package.

Computing Equipment
All of the computers used in the VSAP systems are COTS. The BMG, VBL, Tally and FormatOS systems run on several HPE ProLiant 380 servers. Each uses a NetApp network file system and network switches manufactured by Cisco and Aruba. The main board in the BMD is COTS.

Computer Workstations
Used as terminals (virtually all user interface is handled via Web Browser or SSH to the local systems), these are installed on specially configured and hardened, computer workstations.

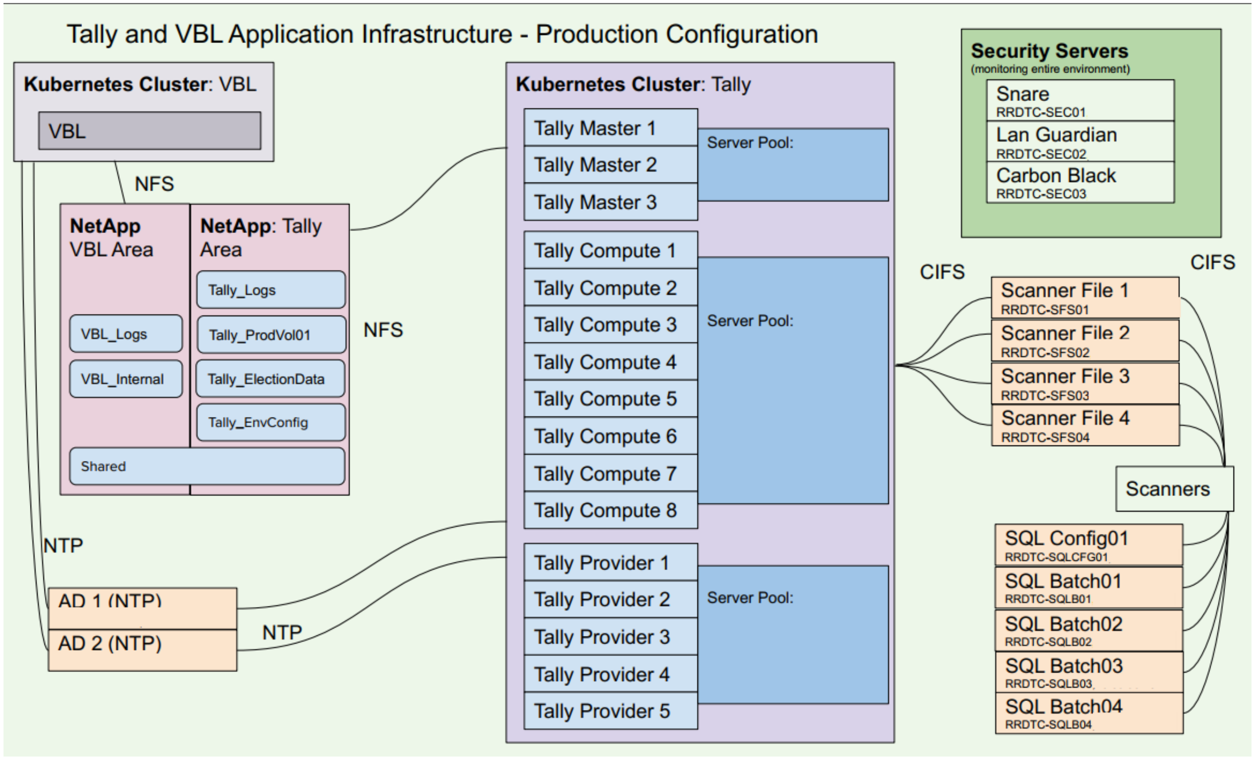
Ballot Scanners
ibml ImageTrac 6000 series scanners in a custom configuration are used by Tally to scan both VBM and BMD ballots.

Report Printers
Several models of Hewlett Packard office laser printers have been tested for use with the system for the purpose of printing reports. These are generic devices supplied by the county and are not specifically identified or inventoried.

Description of System Tested

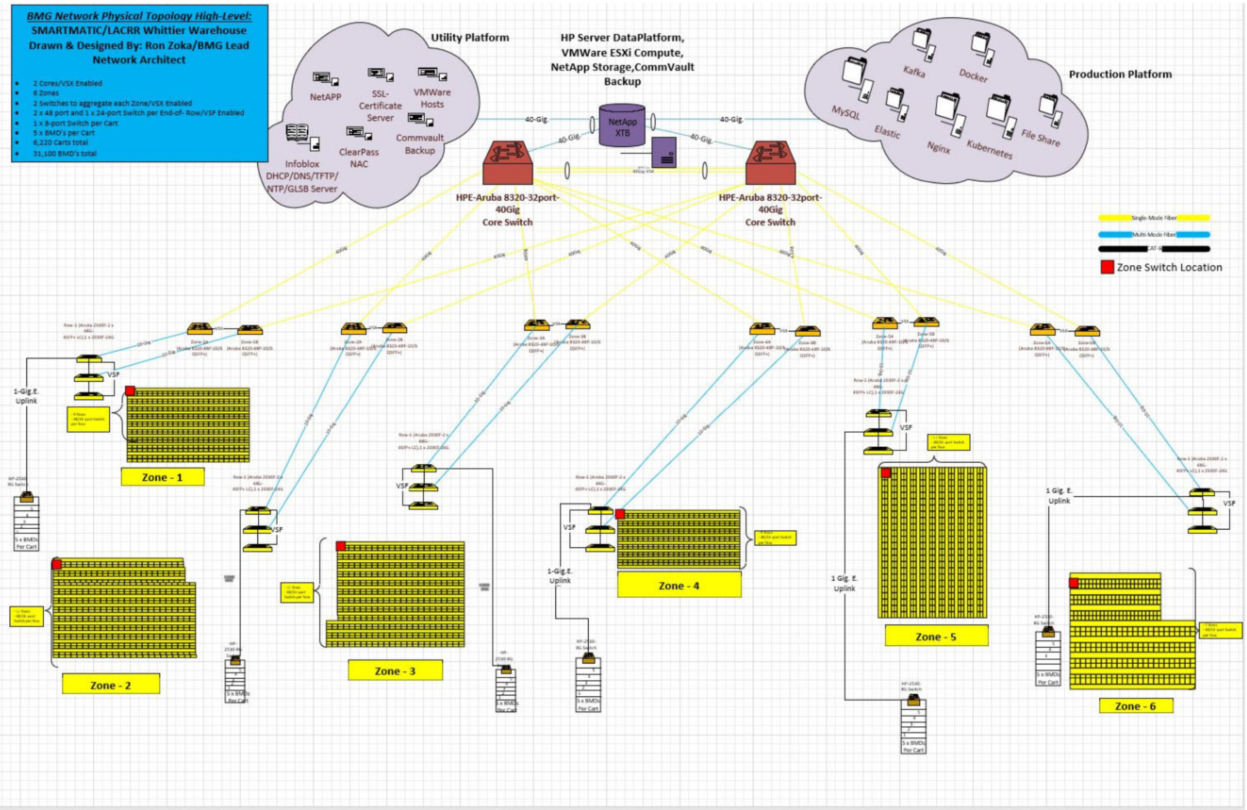
Below are the system diagrams for each of the major VSAP components. Note that several computers are used in each system. For example, in the diagram below illustrating Tally and VBL, Tally uses 16 separate computers, and VBL one. There are five separate SQL servers for the scanner databases. These databases only contain operational parameters for the scanners, no voting data. Four Windows file servers are used for data transfer between the scanners and Tally, and separate servers for Snare logging and Carbon Black security systems. There are also two dedicated network time servers, a NetApp Network File system (which holds all voting data) and a backup system.

VBL and Tally



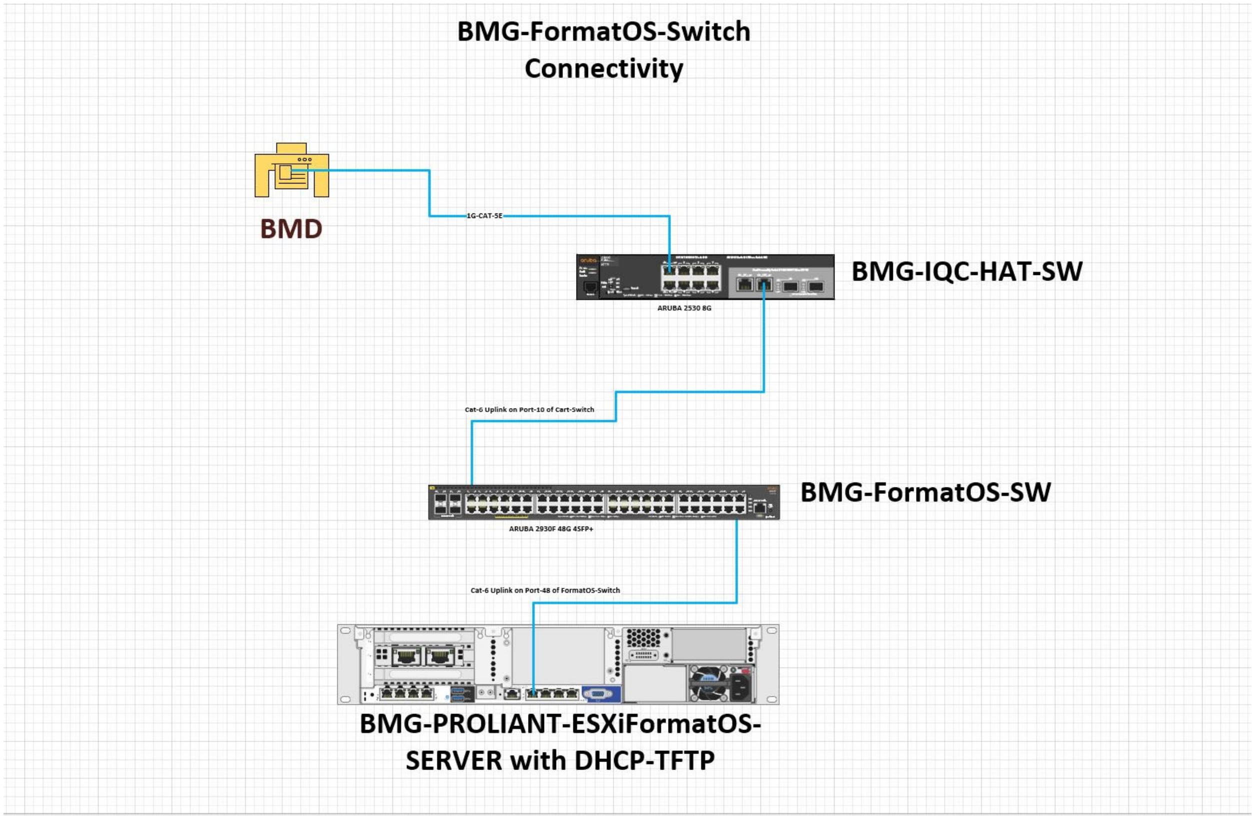
Tally and VBL System Layout

BMG



BMG and BMD Network System Layout

FormatOS


BMG-FormatOS-Switch Connectivity
BMD
1G-CAT-5E
BMG-IQC-HAT-SW
ARUBA 2530 8G
Cat-6 Uplink on Port-10 of Cart-Switch
BMG-FormatOS-SW
ARUBA 2930F 48G 4SFP+
Cat-6 Uplink on Port-48 of FormatOS-Switch
BMG-PROLIANT-ESXiFormatOS-SERVER with DHCP-TFTP

FormatOS System Layout

Federal Certification (If Applicable)

There is no federal certification of this system.

Approach to Testing

Testing is performed following the California Use Procedures for the system. A trusted build of the system is created from the source code and installed on devices that have been wiped clean and have a new installation of the operating systems and required commercial off the shelf (COTS) software. The approach is to run an end-to-end exercise of system functions in four test elections beginning with election definition, voting and tabulating ballots, and producing results reports and logs. The test elections included:

- A primary election defined based on, and using data from, the 2016 Los Angeles County Presidential Preference election. This election is designed to test the ability of all components within the system to handle the data sets generated by a Los Angeles County Primary Election and to test the accuracy of the tabulation.

- A general election based on, and using data from, a Los Angeles County election. This election is designed to simulate the operation of the BMDs in vote centers on Election Day following the California Use Procedures and verify that the procedures and system function are consistent.
- A recall election based on the California 2003 Gubernatorial recall. This election is designed to show that the system can support an election similar to the California Governor's recall election 2003 and to evaluate the consistency of the system's processing of marginal marks on hand marked ballots.
- A special and municipal election that was defined based on two Los Angeles County congressional districts and one municipality. This election is designed to simulate the process of defining and programing a special election conducted in a limited part of the county.

A rank choice voting election was not used because Los Angeles County does not anticipate using rank choice tabulation in the foreseeable future and the system was not designed to use that tabulation methodology.

Ballots used in each election included ballots voted on the BMD and hand marked ballots.

Scope Limitations

Due to the complexity of the system, this functional test was limited to BMD units, VBL, BMG and Tally.

Phases of Testing

The first phase of the test began with wiping all hardware, installing operating systems and required COTS software. A trusted build of the system was created. Working from the system source code in the developer's specified environment, all software modules and installation media was created. This software was then installed on the prepared hardware devices and all configuration steps in the California Use Procedures were carried out.

Election definitions and ballots were produced by LA outside of the test. The system relies upon other LA systems, including voter registration databased and candidate/ contest databases, to create election data for their elections. Although these systems were out of scope for the test, within scope was evaluating the extent to which the elements of the system tested could properly load and use the election definition data.

The second phase of testing was loading the election definition for each test election onto the system, voting test ballots, tabulating results and verification of correct totals.

Functional Findings

With regard to the CVSS, the tests yielded expected results with the exception of the following anomalies:

CVSS 2.1.5: “Because the actual implementation of specific characteristics may vary from system to system, it is the responsibility of the manufacturer to describe each system's characteristics in sufficient detail so that S-ATAs and system users can evaluate the adequacy of the system's audit trail. This description shall be incorporated in the System Operating Manual, which is part of the Technical Data Package.”

> No description of log entries or analysis of the logs were found in the System Operating Manual.

CVSS 2.1.1.a: “Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability.”

> The excessive root access and the ability to boot the system from a USB port give access to the system by unauthorized individuals. Either scenario can result in undetected changes to files and data.

CVSS 2.1.1.b: “Provide system functions that are executable only in the intended manner and order, and only under the intended conditions.”

> The excessive root access and the ability to boot the system from a USB port give access to the system by unauthorized individuals. Both scenarios can allow functions to be executed in non-intended ways.

CVSS 2.1.4.f: “To ensure system integrity, all systems shall: Protect against any attempt at improper data entry or retrieval.”

> The excessive root access and the ability to boot the system from a USB port give access to the system by unauthorized individuals. Either scenario can result in undetected changes to files and data.

CVSS 2.1.5.1.g: “Voting systems shall provide a capability for the status messages to become part of the real-time audit record.”

Ballot jam messages were not recorded in the logs using the same text string as displayed.

CVSS 2.3.3.3.f: “DRE and EBM systems shall notify the voter if he or she has attempted to make more than the allowable number of selections for any contest (e.g., over votes).”

If a voter tries to vote for more than the allowable number of candidates, the BMD cancels the first choice and records the second without informing the voter of the change.

CVSS 2.4.4.1: “Voting systems shall digitally sign electronic reports using NIST approved algorithms with a security strength of at least 112 bits implemented within a FIPS 140-2 level 1 or higher validated cryptographic module operating in FIPS mode.”

All signatures use approved algorithms at these or higher strengths, but with unvalidated cryptographic modules.

CVSS 3.2.2.1: “Notification of Effect of Over voting - If the voter attempts to select more than the allowable number of choices within a contest on a VEBD or PCOS, the voting system shall notify the voter of the effect of this action before the ballot is cast and counted. In the case of manual systems, over votes may be mitigated through appropriately placed instructions.”

When a voter attempts to over vote a race the BMD automatically cancels the first choice and accepts the second without notifying the voter.

CVSS 3.2.4.1. b: “During the voting session, the audio interface of the voting system shall be audible only to the voter.”

The BMD has a second headphone jack that allows a poll worker to listen to the audio ballot for the purpose of assisting a voter using the audio ballot.

CVSS 3.2.4.2.a: “No information shall be kept within an electronic CVR that identifies any alternative language feature(s) used by a voter.”

Tally keeps a graphic image of each ballot scanned as the CVR. Images of mail in alternative language ballots would show the language used on the ballot.

CVSS 3.2.7.a: “No page scrolling - Voting systems shall not require page scrolling by the voter.”

Long candidate lists require the voter to scroll on BMDs.

CVSS 3.2.8.b: “When the voter performs an action to record a single vote, the completed system response time of the VEBD shall be no greater than one second in the case of a visual response, and no greater than five seconds in the case of an audio response.”

> Delays in and/or no audio responses observed.

CVSS 3.2.9.a.ii: “Any records, including paper ballots and paper verification records, shall have sufficient information to support auditing by poll workers and others who can read only English.”

> Foreign language ballots only print the yes and no selections for issues in the chosen language.

CVSS 3.3.3.c.ii: “Sanitized headphone or handset - A sanitized headphone or handset shall be made available to each voter. This requirement can be achieved in various ways, including the use of ‘throwaway’ headphones, or of sanitary coverings.”

> The headphones provided are not disposable and no coverings were evident.

CVSS 3.3.3.f: “Mechanically operated controls or keys on an accessible voting station shall be tactilely discernible without activating those controls or keys.”

> The buttons on the key pad of the BMD do not have the variable resistance that allows touch discernible use. The keys depress smoothly and nothing is felt until they bottom out and activate.

CVSS 3.3.5.c: “Labels, displays, controls, keys, audio jacks, and any other part of the accessible voting station necessary for the voter to operate the voting system shall be easily legible and visible to a voter in a wheelchair with normal eyesight (no worse than 20/40, corrected) who is in an appropriate position and orientation with respect to the accessible voting station.”

> The label for the headphone jack is slightly raised plastic in the same color as the body of the machine, it is almost invisible in diffused lighting with 20/20 vision. Another connection is a symbol which is indecipherable.

CVSS 4.1.4.2.d.iii: “Ballot boxes and ballot transfer boxes, which serve as secure containers for the storage and transportation of voted ballots, shall provide specific points where ballots are inserted, with all other points on the box constructed in a manner that prevents ballot insertion.”

> It is possible to insert or remove ballots from both the BMD and ballot transfer boxes without detection.

CVSS 4.1.5.1.f: “All paper-based tabulators and EBMs shall achieve a misfeed rate of no more than 0.002 (1⁄500). (Misfeeds and jams / total ballots processed) as calculated in section 4.1.5.1.g.”

> The misfeed rate for BMDs during the volume test was 0.0096 (1/103.32).

CVSS 4.1.5.2.b: “Ignore, and not record, extraneous perforations, smudges, and folds.”

> Although there are no counters for extraneous items in the system extraneous perforations, smudges and folds will be captured in the graphic cast vote records.

CVSS 4.3.4.a: “All voting systems shall display on each device a separate data plate containing a schedule for and list of operations required to service or to perform preventive maintenance.”

> No data plate containing required information was found on any BMD.

CVSS 5.4.2.c: “The ballot interpretation logic shall test and record the correct installation of ballot formats on voting devices.”

> The interpretation logic residing inside Tally does not test the installation of ballot formats on BMDs.

CVSS 5.4.3.b.iv: “System generated log of all normal process activity and system events that require operator intervention, so that each operator access can be monitored and access sequence can be constructed.”

> No log entries were found that appeared to be data quality monitor messages or by hardware condition monitors.

CVSS 7.2.1.a.i: “The default access control permissions shall implement the minimum permissions needed for each role or group identified by a device.”

> Too many people have access to the root password.

CVSS 7.2.1.c: “The default access control permissions shall implement the minimum permissions needed for each role or group identified by a device.”

> There is excessive root access to the system.

CVSS 7.2.2.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.”

> There is no evidence in the Technical Data Package to indicate that role-based access control, conforming to the recommendations of the Standard is implemented.

CVSS 7.2.4.a: “Voting systems shall ensure that only authorized roles, groups, or individuals have access to election data.”

> Too many functions require access to the root password. Also, a USB boot will give access to the election definition.

CVSS 7.3.a: “Any unauthorized physical access shall leave physical evidence that an unauthorized event has taken place.”

> Seals, locks, labels and sensors can all be bypassed.

CVSS 7.3.b: “Voting systems shall only have physical ports and access points that are essential to voting operations and to voting system testing and auditing.”

> The unrestricted access to, and the ability to boot from, the USB port allows access to voting data.

CVSS 7.3.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."

> Seals, locks, labels and sensors can all be bypassed.

CVSS 7.3.f: “Ballot boxes shall be designed such that any unauthorized physical access results in physical evidence that an unauthorized event has taken place.”

> The printer cover allows access to the ballot box and can be opened without detection.

CVSS 7.4.4.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.”

> There is no documentation for the version numbers of hundreds of RPM support packages.

CVSS 7.4.6. e.viii: “The minimum information to be included in the voting system equipment log shall be a cryptographic hash of the software update package using FIPS 1402 level 1 or higher validated cryptographic module”.

> The system does not use FIPS 140-2 validated cryptographic modules.

CVSS 7.4.6.f.i: “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 system does not use FIPS 140-2 validated cryptographic modules.

CVSS 7.5.4.a.i: “Evidence that any single person can cause a violation of a voting system security goal (e.g., integrity of election results, privacy of the voter, availability of the voting system), assuming that all other parties follow procedures appropriate for their roles as specified in the manufacturer’s documentation.”

> The excessive access to the root password and the ability to boot from a USB port allow too many individuals access to the election definition and ballot data.

CVSS 7.5.4.a.iii: “OEVT fail criteria: violation of requirements - The voting device shall fail open ended vulnerability testing if the OEVT team finds vulnerabilities or errors in the voting device that violate requirements in the Standards. While the OEVT is directed at issues of device and system security, a violation of any requirement can lead to failure. The S-ATA shall report an OEVT failure if any of the following are found: Use of a cryptographic module that has not been validated against FIPS 140-2.”

> CentOS and Ubuntu are not FIPS validated.

CVSS 7.5.4.a.iv: “OEVT fail criteria: violation of requirements - The voting device shall fail open ended vulnerability testing if the OEVT team finds vulnerabilities or errors in the voting device that violate requirements in the Standards. While the OEVT is directed at issues of device and system security, a violation of any requirement can lead to failure. The S-ATA shall report an OEVT failure if any of the following are found: Ability to modify electronic event logs without detection.”

> The testers were able to gain access to the electronic event logs.

CVSS 7.5.4.a.vii: “OEVT fail criteria: violation of requirements - The voting device shall fail open ended vulnerability testing if the OEVT team finds vulnerabilities or errors in the voting device that violate requirements in the Standards. While the OEVT is directed at issues of device and system security, a violation of any requirement can lead to failure. The S-ATA shall report an

OEVT failure if any of the following are found: Access to configuration file without authentication."

> Access to the configuration files for BMD and BMG was prohibited, but could be obtained for everything else.

CVSS 7.5.4.a.xii: "OEVT fail criteria: violation of requirements - The voting device shall fail open ended vulnerability testing if the OEVT team finds vulnerabilities or errors in the voting device that violate requirements in the Standards. While the OEVT is directed at issues of device and system security, a violation of any requirement can lead to failure. The S-ATA shall report an OEVT failure if any of the following are found: Ballot boxes without appropriate tamper evidence countermeasures."

> Seals, locks, labels and sensors can all be bypassed.

CVSS 7.5.4.b: "Threat model: failure - Voting systems shall fail open ended vulnerability testing if the manufacturer's model of the system along with associated use procedures and security controls does not adequately mitigate all significant threats as described in the threat model. The OEVT team may use a threat model that has been amended based on their findings in accordance with 7.5.4.3.c."

> The testers were able to gain access to the system regardless of mitigations.

CVSS 7.5.4.c.i: "OEVT fail criteria: critical flaws - The voting device shall fail open ended vulnerability testing if the OEVT team provides a plausible description of how vulnerabilities or errors found in a voting device or the implementation of its security features could be used to: Change the outcome of an election."

> The ability to boot from the USB port allows election data to be modified.

CVSS 7.5.4.c.ii: "OEVT fail criteria: critical flaws - The voting device shall fail open ended vulnerability testing if the OEVT team provides a plausible description of how vulnerabilities or errors found in a voting device or the implementation of its security features could be used to: Interfere with voters' ability to cast ballots or have their votes counted during an election."

> The ability to boot from the USB port allows election data to be modified.

CVSS 7.5.4.c.iii: "Compromise the secrecy of vote without having to demonstrate a successful exploitation of said vulnerabilities or errors."

> A jam in the ballot box requires the box to be opened and displays the voter selections on the ballot.