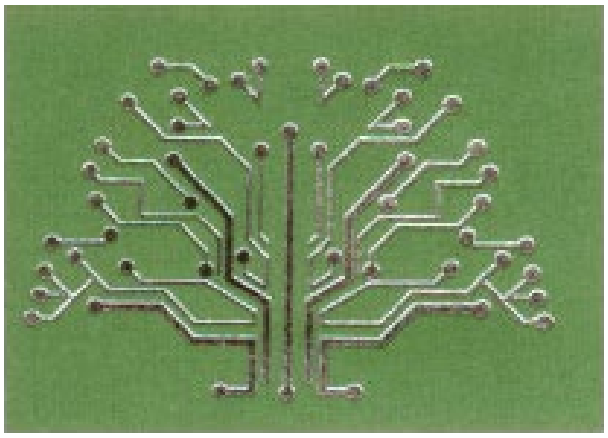


FREEMAN, CRAFT, MCGREGOR GROUP

California Secretary of State
Consultant's Public Report on:

Security and Telecommunications Testing of the LA County VSAP 2.0 Voting System

Prepared for the
California Secretary of State

December 24, 2019

Revision history

Version	Change date	Author(s)	Changes to previous version
1.0	12-02-2019	Weingart	Initial Draft
1.1	12-06-2019	McGregor	Edits
1.1	12-08-2019	Weingart	Edits and updates
1.2	12-09-2019	Weingart	Cleanup
1.3	12-09-2019	Weingart	Cleanup
1.4	12-13-2019	Weingart	Cleanup
1.5	12-24-2019	Weingart	Cleanup

Table of Contents

Introduction

The purpose of the Security and Telecommunications Test is to identify and document vulnerabilities and potential vulnerabilities to physical or logical tampering that could cause:

- Incorrect recording,
- Incorrect tabulation,
- Manipulation of hardware, data, or parameters that might be used to change the outcome of an election, to interfere with voters' ability to cast ballots, or have their votes counted during an election, or to compromise the secrecy of vote.
- Alteration of critical election data such as the election definition or system audit data.

To the extent possible, when a vulnerability is found, the report will indicate whether the vulnerability can be exploited by a:

- Voter: 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 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.
- Warehouse worker: Usually has a limited knowledge of the voting machine design and configuration, although some may have advanced knowledge. May carry out attacks designed by others. They have access to the machines for extended periods while they are being stored and configured prior to delivery to the polls.
- Elections official insider: Wide range of knowledge of the voting machine design and configuration. May have unrestricted access to the machine for long periods of time. Their designated activities include:
    - Set up and pre-election procedures;
    - Election operation;
    - Post-election processing of results; and
    - Archiving and storage operations.
- Vendor insider: With 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.

In addition, this report indicates whether exploiting these vulnerabilities will cause any of the following, or other, compromises to the system:

- Unauthorized changes to system capabilities for:
    - Defining ballot formats
    - Casting and recording votes
    - Calculating vote totals
    - Reporting vote totals
- Alteration of voting system audit trails
- Changing, or preventing the recording of, a vote
- Introducing data for a vote not cast by a registered voter
- Changing calculated vote totals
- Allowing access to vote data including individual votes and vote totals by unauthorized individuals
- Allowing access to voter identification data and data for votes cast by the voter such that an individual can determine the content of specific votes

This public report includes descriptions of the findings and vulnerabilities, an evaluation of the risk associated with each vulnerability, recommendations to mitigate these vulnerabilities and our conclusions. Information that cannot be disclosed publicly under the Non-Disclosure Agreement between the California Secretary of State (SOS) and Los Angeles County (the County) and details of attack methods are not provided in this report in order to make it available to the public.

Scope of Work and Reporting

This report covers the work completed during the Security and Telecommunications Test of the Los Angeles County VSAP 2.0 System (the System). As previously stated, the purpose of this test is to identify and document vulnerabilities and potential vulnerabilities.

Physical security tests, evaluating the effectiveness of tamper evidence detection, and an evaluation of the use of cryptography were conducted in accordance with FIPS 140-2 “Security Requirements for Cryptographic Modules.” To the extent applicable, penetration tests were conducted to be consistent with NIST Special Publication 800-115 “Technical Guide to Information Security Testing Assessment.” The vulnerability

assessments in the work papers (Please see Attachments section below) are based on “Calculating Attack Potential” as defined in section B4 of Vulnerability Assessment (AVA) in Common Methodology for Information Technology Security Evaluation (CEM v3.1R2, September 2007).

These 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.

The work performed and the findings are strictly limited to the specific serial numbered hardware elements and specific software elements as they were configured and examined during the testing. An inventory of those items is included as Attachments A and B and the information in the Attachments section at the end of this report. The results described in this report should be reliable and repeatable for those specific devices.

Manufacturer's Description of System

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:

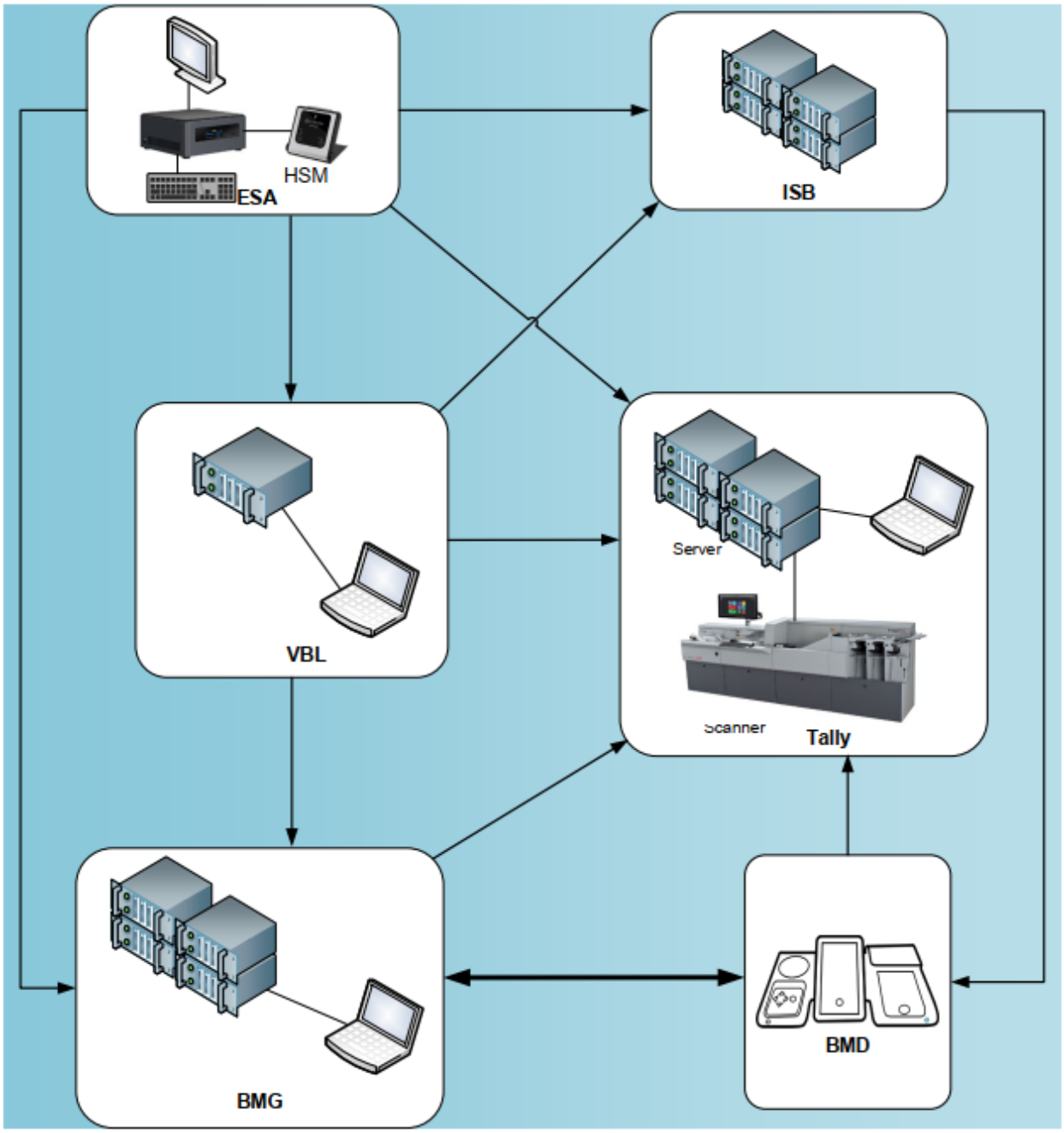
- Polling place voting using the Ballot Marking Device (BMD)

Post-voting tasks:

- 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 (4,500 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 system 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

Required communication software packages (virtually all user interface is handled via Web Browser or SSH to the local systems) 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.

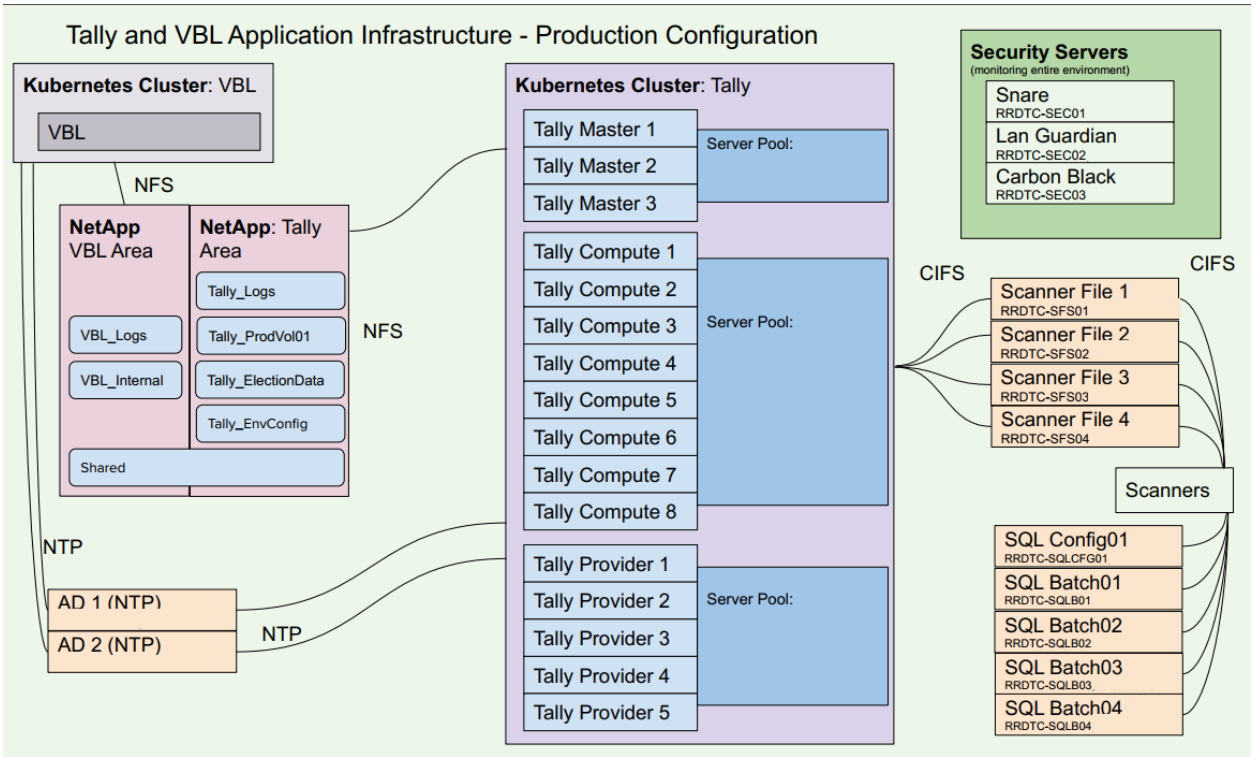
Report Printers

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

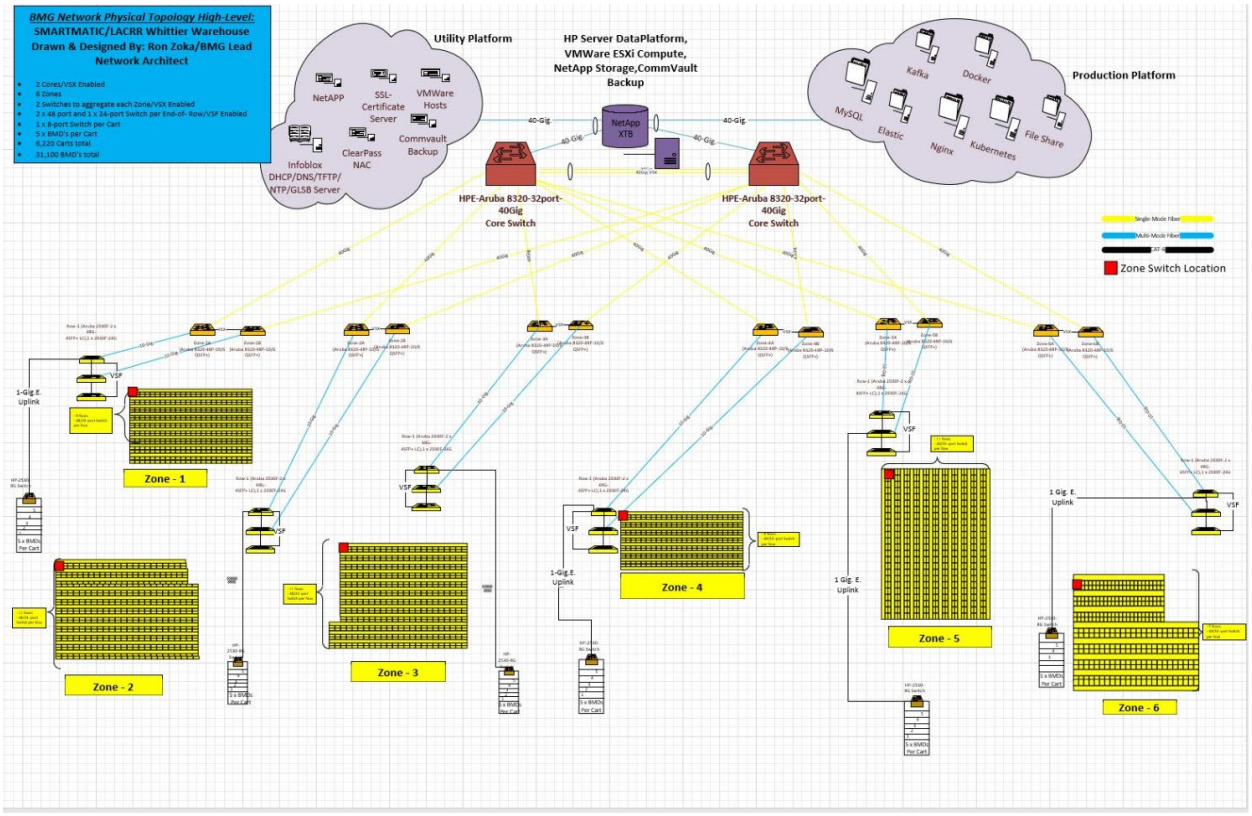
Below are the system diagrams for each of the major VSAP components. Note that several computers are used in each system. For example, in the diagram below illustrating Tally and VBL, Tally uses 16 separate computers, and VBL one. There are five separate SQL servers for the scanner databases. These databases 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 time servers, a NetApp Network File system (which holds all voting data) and a backup system.

VBL and Tally



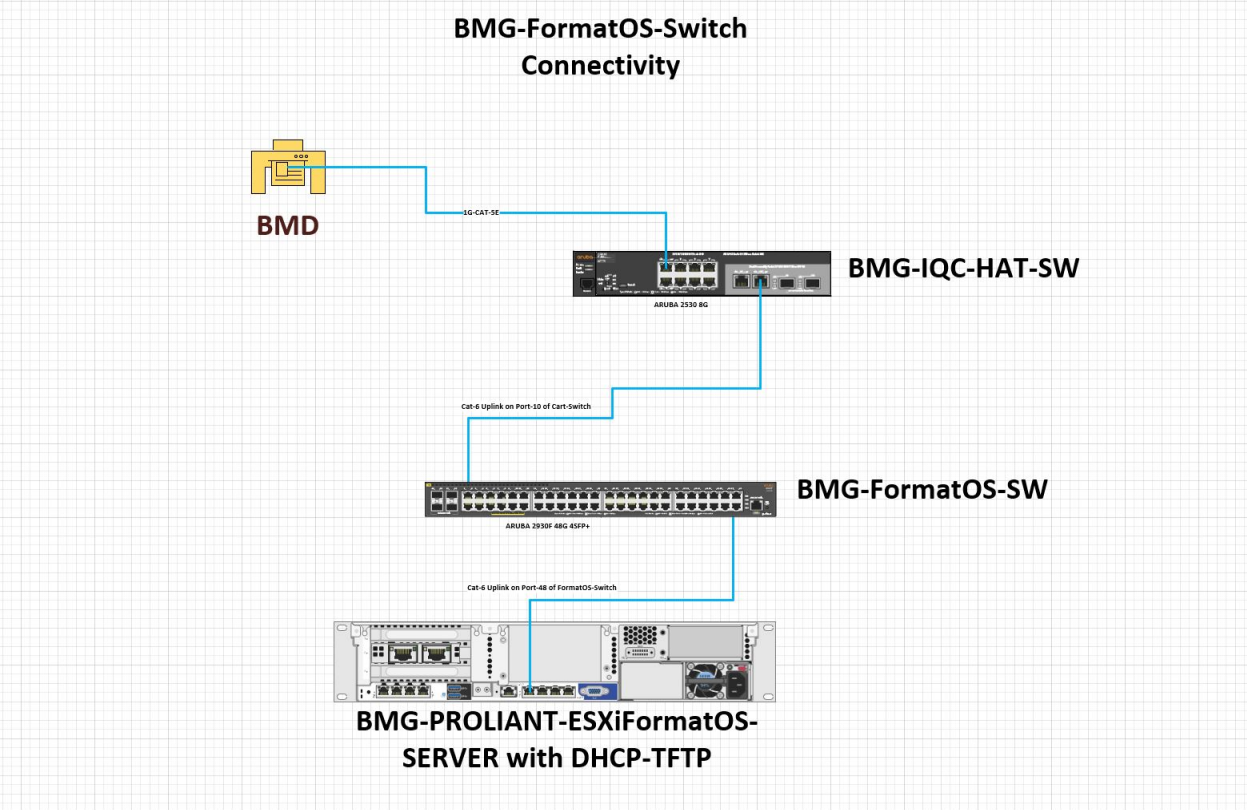
Tally and VBL System Layout

BMG



BMG and BMD Network System Layout

FormatOS



FormatOS System Layout

Assumptions

The components that are used in a central election office were installed on standard COTS PCs as pictured above. Physical security mechanisms, such as locks or tamper-evident labels were applied to these systems, physical security tests were performed. Logical security tests were performed on all of these devices.

The poll devices were supplied with seals and tamper-evident labels and were installed in accordance with the manufacturer's recommendations. As such, a physical security test was performed on all seals and tamper-evident labels. Logical security tests were performed on all devices.

Test procedures assumed that the attacker had an undisturbed place to mount the attacks. It was also assumed that tools and materials, both physical and logical, which are typically used in these attacks, were available.

All tools and methods deployed during this security test are commonly available. The physical tools and devices can be purchased at local consumer outlets or online. Every logical tool can be purchased and/or downloaded online from common locations.

Approach to Testing

Personnel performing tests included:

Freeman, Craft McGregor Group:

- Kate McGregor
- Lou Losee
- Steve Weingart

The VBL, Tally, BMG and FormatOS systems were set up by the County before the test team arrived. After a brief overview of the system, the team worked with the vendor and subcontractors to perform the trusted build.

Note that the trusted build process was not typical of the three to five standalone systems used in most election systems. VSAP uses an enterprise data center sized system. There are 33 separate computers, plus the NetApp network file system and Commvault backup system that make up the entire Tally/VBL cluster housed in two racks.

The count was similar for the BMG, except that it uses all virtual machines running on the VMWare ESXI hosting system. Therefore, all computers are distributed across the VMWare installation and the NetApp file system. Using automation and scripting to prevent typing and transcription errors throughout the process, the trusted build still took several days to complete. After the systems were built, they were hardened in the same manner, using an installation document and several scripts and processes. The hardening included applying the SCAP ruleset for the appropriate OS version. All final code (much of the code is interpreted, so it is not compiled), was collected and hashed for delivery to the SOS.

The test began in two phases. Since they were accessible, the software specialist immediately started to work on the servers. The hardware specialist started to work on the locks, seals and tamper-evident labels applied to the poll devices.

Once the physical security was bypassed, the entire team focused their attention on the software resident on the servers as well as on the poll devices.

Security identification and vulnerability scanners were employed, as well as direct probing techniques using forensic USB boot disks and attempting to join the local network to detect vulnerabilities. As potential vulnerabilities were discovered, appropriate tools were brought to bear to determine if an exploit was possible. At regular intervals the team discussed the current status and findings to determine if any of the potential vulnerabilities could be used in combination to enable an exploit. This method was repeated and refined as the test continued until the duration of the test period was exhausted.

Note: The VSAP system is air-gapped from the Internet and other networks as required by CVSS. All communication between non-collocated systems is accomplished by using an Iron Key FIPS 140-2 level 3 secured USB devices for key transfer, or via USB drives, in the case of USB drive transfer critical files are signed to ensure integrity.

Scope Limitation

Only the following systems and devices were tested during this examination: VBL, Tally (including the scanners and transfer file and database systems), BMG, and FormatOS.

Any and all other parts of the System, including the Election Management System, were not part of this test process. No comment can be made as to the security of the functions used to create the cryptographic keys employed to secure the System and to generate the election definitions.

No intentional physical damage to the devices was permitted. Some elements were disassembled as part of the testing process, but all items were returned to the pretest state at the end of the test. In the case of the client/server systems, some may have had to be reinstalled to be returned to full service. Great care was taken during testing to avoid causing any physical or permanent damage to the server systems. In some cases, this required one of the testers to know the root passwords of the systems to facilitate controlled shutdowns and restarts. This knowledge was not used to the test team’s advantage in any way.

Findings and Vulnerabilities

Network scanning and test results

Each of the systems (VBL, Tally, BMG and FormatOS) was scanned with network identification and severity vulnerability scanning tools. The results may be seen in attachments (please see the Attachments section below for the list of documents).

The networks were also probed manually and no vulnerabilities were discovered in addition to the findings described below.

Locks and tamper seals are subject to picking and removal

Lock picking was attempted and was successful using standard widely available lock picks and standard techniques.

Tamper-evident adhesive label seals were removed without damage using a solvent and a razor blade. After removal, the label was allowed to dry and was re-applied to the equipment without leaving evidence of any compromise.

Smooth tailed seals were opened successfully and reattached with no visible evidence of compromise.

These attacks could be conducted by a poll worker, elections official insider, warehouse worker or vendor insider. They affect all parts of the system.

Although these are not complete attacks, they do disable the ability to prevent and detect unauthorized access to the equipment and can be the first step enabling more complex attacks.

The easily defeated locks and seals on all of the VSAP devices resulted in the system not conforming to CVSS 2.1.1.a, which provides that all systems shall “Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability.” It also degrades the ability of the system to meet CVSS 7.3.a. which states, “Any unauthorized physical access shall leave physical evidence that an unauthorized event has taken place.”

Unrestricted access to workstation cases

The cases of the Command and Control workstations (generic standard PCs used for accessing and interacting with the system via a web browser) were not secured with tamper-evident labels or locks. The cases were opened in seconds without

using any tools. Once access was gained, any BIOS password could have been removed. This makes it possible to boot the machine using an outside operating system on a USB drive. In addition, there is no disk encryption so the hard disks could be directly accessed and all data files were accessible and alterable. Carbon Black security prevents changing executable files, but the terminal systems were not fully included in the hardening.

This attack could be conducted by an elections official insider or a vendor insider. It affects all system configurations that include a workstation. The workstations are vulnerable to physical attacks that facilitate the software attacks described in findings outlined later in this report.

The configuration of the system workstations presented to the test team did not conform to CVSS 2.1.1.a, which provides that all systems shall “Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability.” Failure to secure the workstation cases results in a nonconformance with CVSS 7.2.1 which states, “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.” and CVSS 7.3.a, b, and e which state:

> “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.”
>
> “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.”

Ability to Boot from USB

Booting from a USB drive was not disabled on any of the systems. As such, gaining physical access to the machines allowed access to both the operating and application files for VBL, Tally and FormatOS. This was performed by booting an external USB disk with forensic applications. This was not applicable to BMG as it

uses all virtual machines and no local disks, only NetApp. The authentication requirements enforced by NetApp protect BMG in this instance.

Because booting from a USB drive doesn't use the operating system on the targeted computer, that computer is offline from the System's perspective. As such, this approach defeats the ability of Carbon Black to prevent running unregistered executables. For the same reason, Snare, the logging system, will not receive any information while running from the USB drive.

Access to the application binaries permits recovering and decompiling and/ or examining system source code. The cryptographic key material used to protect the integrity of elections was not encrypted. All cryptographic keys present were accessible in plaintext. Configuration files may also be modified to change the behavior of the system. This allowed secrets used to ensure election integrity to be recovered with only physical access to the system's storage device.

This attack could be conducted by an elections official insider or a vendor insider. A voter would not have sufficient access to the system to successfully complete the prerequisite defeat of physical security without leaving evidence of the attack.

This vulnerability, combined with the unrestricted access to system racks, results in the system not conforming with CVSS 2.1.4.f, which provides that all systems shall "Protect against any attempt at improper data entry or retrieval."

CVSS 7.2.1.b states, "Voting system equipment shall provide controls that permit or deny access to the device's software and files." Booting from a USB drive gives access to all files not on NetApp, so this is also a non-conformance.

The System also does not conform to CVSS 7.3.b, which states "Voting systems shall only have physical ports and access points that are essential to voting operations and to voting system testing and auditing." Permitting the System to start from an external USB drive is not needed at any time to implement voting operations.

Shared/Static Secrets

The system has shared static secrets that are used to ensure election integrity. During the course of this test, multiple secrets were shared throughout the system. Recovering these secrets from one component in the system allowed other portions of the system to be attacked. This resulted in the ability to sign election files to be modified and signed for use farther down the system hierarchy.

This attack could be conducted by an elections official insider or vendor insider. It affects all elements and configurations of the system.

Although CVSS has no prohibitions on static or shared secrets, the attacker's ability to recover these secrets allows unauthorized administrative access to all system components. As a result, it does not conform with CVSS 7.2.4.a which states, "Voting systems shall ensure that only authorized roles, groups, or individuals have access to election data."

High Dependency on Root Access

Root access is required for many regular operations in the VSAP system. These include, but are not limited to, updating cryptographic keys used to protect and verify the integrity of elections and voting information and performing regular system maintenance, including regular system shutdown and startup. This situation invariably leads to poor control of access to the root password which enables subsequent unauthorized access.

Access to the application binaries permits recovering and decompiling and/or examining system source code. The cryptographic key material used to protect the integrity of elections was not encrypted. All cryptographic keys present were accessible in plaintext. This allowed secrets used to ensure election integrity to be recovered with only physical access to the system's storage device. Configuration files could also be modified to change the behavior of the system.

This attack could be conducted by an elections official insider or a vendor insider.

This vulnerability, combined with the easy access to system racks, results in the system not conforming with CVSS 2.1.4.f, which provides that all systems shall "Protect against any attempt at improper data entry or retrieval" and CVSS 7.2.1.b which states, "Voting system equipment shall provide controls that permit or deny access to the device's software and files." The ability to recover secrets allows unauthorized administrative access to all system components and does not comply with CVSS 7.2.4.a which states, "Voting systems shall ensure that only authorized roles, groups, or individuals have access to election data."

Lack of Full Disk Encryption

No component of the system has full disk encryption. Gaining physical access to the machines allowed access to both the operating and application files. This was

performed by booting an external USB disk containing forensic applications. Another approach to this attack involves removing the disks from the computer and inserting them into another system. Since these systems were set up with RAID (Redundant Array of Independent Disks), another computer set up with a similarly configured RAID controller would allow not only recovery of all data and secrets, it will also allow the entire system to be cloned. This approach can also be used to defeat the ability of Carbon Black to prevent running of unregistered executables. When booted from a source other than the original operating system, that computer is offline with respect to the System. Also, the Snare logging function will not receive any log information and the event will not be recorded.

Access to the application binaries permits recovering, decompiling and or examining system source code. The cryptographic key material used to protect the integrity of elections was not encrypted at rest, all cryptographic keys present were accessible in plaintext. This allowed secrets used to ensure election integrity to be recovered with only physical access to the system's storage device.

This attack could be conducted by an elections official insider or a vendor insider. A voter would not have sufficient access to the system to successfully complete the prerequisite defeat of physical security without leaving evidence of the attack.

This vulnerability, combined with the unrestricted access to system racks, results in the system not complying with CVSS 2.1.4.f, which provides that all systems shall "Protect against any attempt at improper data entry or retrieval" and CVSS 7.2.1.b which states, "Voting system equipment shall provide controls that permit or deny access to the device's software and files."

Lack of Validated FIPS140-2 Cryptographic Modules

The systems (VBL/Tally, BMG, and FormatOS) utilize the Linux operating system as the base platform. The cryptographic modules employed for cryptographic processing in FormatOS, BMG, Tally and VBL are not FIPS 140-2 validated.

This is not compliant with CVSS 7.5.4.iii which states, "Use of a cryptographic module that has not been validated against FIPS140-2," as a violation of the OEVT requirements as stated in CVSS 7.5.4.a. The Red Hat validated module for RHEL stated in section 9.3 of the *VSAP-TDP-005_System_Security_Specification.pdf* is not validated on CentOS (Tally, VBL, BMG) or Ubuntu (FormatOS), neither the employed OS versions nor platforms used are validated. The cryptographic functions used by the Java implementation also appear not to be FIPS 140-2 validated.

Attachments and Inventories of Items Tested

For the inventory of the BMG components, please see:

A) BMG-Device-SerialNum-11-08-2019.xlsx

For the inventory of the Tally and VBL components, please see:

B) VSAP Tally-VBL environment details_v2.pdf

Scan Reports:

C) BMG-OpenVas_Scan_hosts_10_0_9_0-254.pdf
D) BMG-nmap_Scan_hosts_10_0_9_0-254.pdf
E) FormatOS-OpenVAS_Scan-2019-11-20.pdf
F) VBL-Tally-nmap-11-18-2019.txt

The scanners used were:

Scanner 8, S/N 88555-1, ibml serial number A1081519000014
Scanner 18, S/N 88556-5, ibml serial number A1081519000012

The FormatOS components were:

Computer: HPE ProLiant DL380 Server SN: 2M291400M8
Network switch: Aruba 2930F SN: TW93HKT0D7 JL253-6001

Work Papers:

G) 001-Red Team Work Paper - BMD Ballot Box – V2.docx
H) 002-Red Team Work Paper - Locks, Seals and Labels-v2.docx
I) 003-Red Team Work Paper - Root Access.docx
J) 004-Red Team Work Paper - USB Boot.docx
K) 005-Red Team Work Paper - Root Access and USB Boot Vulnerabilities.docx