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

Election Systems & Software
EVS 5.2.1.0

AutoMARK Voter Assist Terminal, version 1.8.6.0
DS200 Precinct Scanner, v 2.12.1.0
DS850 Central Scanner, v 2.10.1.0
EVS Election Management System, v 5.2.1.0
ExpressVote, Hardware Version, v 1.4.1.0
ExpressVote Activation Printer

Staff Report

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

August 28, 2017

Table of Contents

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

I. INTRODUCTION

1. Scope

This report presents the test results for all phases of the certification test of the Election Systems and Software (ES&S) EVS 5.2.1.0 voting system. The purpose of the testing is to test the compliance of the voting system with California and Federal laws. Testing also uncovers other findings, which do not constitute non-compliance, and those findings are reported to the voting system vendor to address the issues procedurally. The procedures for mitigating any additional findings are made to the documentation, specifically the ES&S Use Procedures.

2. Summary of the Application

Elections Systems and Software Inc. submitted an application for the EVS 5.2.1.0 voting system on September 7, 2016. The system is comprised of the following major components:

- AutoMARK Voter Assist Terminal (VAT) version 1.8.6.0;
- DS200 Precinct Scanner, version 2.12.1.0;
- DS850 Central Scanner, version 2.10.1.0;
- ExpressVote, version 1.4.1.0;
- ExpressVote Activation Printer; and
- EVS Election Management System, version 5.2.1.0.

In addition to these major components, which includes the executable code and the source code, ES&S was required to submit the following: 1) the technical documentation package (TDP); 2) all the hardware components to field two complete working versions of the system, including all peripheral devices, one for the Functional Test Phase and one for the Red Team Penetration Test Phase; 3) all the peripherals that would be in the polling place; and 4) the ES&S Use Procedures.

3. Contracting and Consulting

Upon receipt of a complete application, the Secretary of State released a Request for Quote (RFQ) for assistance with the Security Review, both Source Code and Red Team Penetration testing. The statement of work (SOW) also had an option for the Secretary of State to use the awarded contractor for Functional testing, if it deemed necessary.

Through the formal California contracting process, the Secretary of State awarded a contract to Freeman, Craft, McGregor Group, Inc. (FCMG), who would sub-contract portions of the review to Atsec Information Security, Corp. (@sec) and Coherent Cyber.

II. SUMMARY OF THE SYSTEM

The system consists of seven components:

1. AutoMARK Voter Assist Terminal (VAT), v. 1.8.6.0

The AutoMARK Voter Assist Terminal enables voters who are visually or physically impaired or voters who are more comfortable reading or hearing instructions and choices in an alternative language to privately mark paper ballots.

The AutoMARK supports navigation through touchscreen, physical keypad or Americans with Physical Disabilities Act support peripherals such as a sip and puff device or a two position switch. The touch screen visually guides the voter through the ballot marking process with screen text and symbols. Touch screen controls meet all applicable guidelines for size and readability. Each key is shaped and positioned to provide an intuitive voting session and labeled in both Braille and printed text to indicate function.

A voter using this device simply inserts his or her blank ballot. The AutoMARK then scans the ballot to determine the correct ballot style configuration and displays the ballot through a series of screens on a touch-screen monitor (similar to DRE voting devices). The AutoMARK is capable of being programmed to provide instruction and display the ballot in multiple languages. The AutoMARK supports visually impaired voters through audio instruction and a Braille coded keypad. In this mode, the screen can be blanked to insure voter privacy. This audio mode also supports multiple languages. Finally, physically impaired voters can vote on the AutoMARK using an ATI device or by connecting an included disposable sip-puff device.

If a marked ballot is inserted into the AutoMARK, it will display the marked vote choices on the screen for verification and will also provide that verification through the audio mode.

The AutoMARK does not store, count or tabulate voted ballots. It can only be used to mark optical scan ballots for tabulation by another device or to confirm the vote choices on a voted ballot.

2. DS200 Precinct Tabulator, v. 2.12.1.0

The DS200 is a digital scan tabulator that scans and stores a full-page image of the ballot. Ballots can be fed in any orientation. During tabulation, the images are processed by proprietary mark recognition software. It is generally used to tabulate ballots in a polling place, but may be used as a central count device in small jurisdictions.

3. DS850 Central Ballot Scanner, v. 2.10.1.0

The DS850 is a high-speed digital scan ballot counter that scans and stores ballot images and is used in central count operations. During tabulation, the images are processed by proprietary mark recognition software. This tabulator can out stack under votes, over votes, blank ballots, write-in ballots and unreadable ballots into separate batches. Ballots may be fed in any orientation.

4. ExpressVote, version 1.4.1.0

The ExpressVote is a touchscreen capture device. It combines paper-based voting and touchscreen technology, which produces an independent, voter-verifiable paper record that is scanned by ES&S tabulators such as the DS200 or DS850.

5. Election Management System (EMS)

The election management system software package composed of the following modules:

a. Electionware, Version 4.7.1.0
b. Event Log Service, Version 1.5.5.0
c. Removable Media Service, Version 1.4.5.0
d. Election Reporting Manager, Version 8.12.1.0
e. Voter Assist Terminal (VAT) Previewer, Version 1.8.6.0
f. ExpressVote Previewer, Version 1.4.1.0
g. ExpressLink, Version 1.3.0.0
h. PaperBallot, Version 4.6.1.0

a. Electionware, Version 4.7.1.0

Electionware is used by a jurisdiction to create the ballot definition for an election. Electionware is then used to program the various media used by the different vote counting components. After the election, Electionware is used to compile and tabulate election returns from throughout the jurisdiction. Finally Electionware contains a series of additional reporting functions.

b. Event Log Service, Version 1.5.5.0

The Event Log Service logs user's actions for the election management applications. It runs in the background, logging system events to the COTS Windows Event Viewer. The log can be used to print audit log reports.

c. Removable Media Service, Version 1.4.5.0

The Removable Media Service supports election media programming.

d. Election Reporting Manager, Version 8.12.1.0

Election Reporting Manager (ERM) is ES&S's election results reporting program. ERM is used to generate paper and electronic reports for poll workers, candidates, and the media. ERM is designed to display updated election totals on a monitor as ballot data is tabulated. Report editing features data to be read from a variety of ballot scanners, report formats to be customized, and accurate election results to be generated.

ERM is designed to support a wide range of ES&S ballot scanning equipment and can produce reports for both central count systems and precinct count systems.

e. Voter Assist Terminal (VAT) Previewer, Version 1.8.6.0

VAT Previewer is the ballot previewer for accessible voting equipment (AutoMARK).

f. ExpressVote Previewer, Version 1.4.1.0

ExpressVote Previewer is the ballot previewer for accessible voting equipment (ExpressVote).

g. ExpressLink, Version 1.3.0.0

ExpressLink is an activation card printing utility for ExpressVote.

h. PaperBallot, Version 4.6.1.0

The PaperBallot module used for designing paper ballots for use with ES&S equipment.

6. ExpressVote Activation Printer

The ExpressVote Activation Printer is a small, thermal, on demand printer used to print the ballot activation code on the ExpressVote activation card.

III. TESTING INFORMATION AND RESULTS

1. Background

ES&S submitted an application to the Secretary of State for certification of the EVS 5.2.1.0 voting system on September 7, 2016. The Election Assistance Commission (EAC) certified this version of the system on December 18, 2015, with the EAC Certification Number: ESSEVS5210.

State examination and functional testing of this system was conducted by Secretary of State staff in conjunction with the State's technical consultant, Freeman, Craft, McGregor Group (FCMG). The configuration of the equipment, using trusted builds from a Voting System Test Laboratory (VSTL), was conducted at the Secretary of State's office in Sacramento, California from March 20 to March 24, 2017. Source Code Review was performed by Atsec Information Security Group from March 20 to June 16, 2017. Functional testing was performed from April 10 to April 14, 2017 (Phase I) and May 8 to May 12, 2017 (Phase II). Red Team testing was performed at Coherent Cyber's office in San Antonio, Texas from May 22 through May 26, 2017. Volume testing was conducted collaboratively by Secretary of State staff and FCMG, with the assistance of fourteen (14) temporary workers at the Solano County Elections office from June 26 through June 27, 2017. Accessibility testing was also a collaborative effort between the Secretary of State staff and FCMG, along with six (6) volunteers from the accessibility community. During each phase of testing, with the exception of Source Code and Red team testing, representatives from ES&S were present to observe and answer any questions that arose during testing.

2. Functional Testing Summary

System Configuration:

Preparation for Functional Testing and all subsequent testing began on March 20, 2017. ES&S provided two server types for certification, one for larger sized jurisdictions (Dell PowerEdge T630) and a smaller server (Dell PowerEdge T430) for smaller jurisdictions. Also provided were four (4) test workstations (Dell 5040) for use as clients to the servers and one as a standalone Election Reporting Manager (ERM) system. ES&S also provided two (2) DS850s, four (4) AutoMARKs, three (3) ExpressVotes, and six (6) DS200 machines.

For approximately one week, test consultants built the test environment utilizing the vendor provided Use Procedures, which included installation of the operating system, commercial-off-the-shelf (COTS) software, voting system trusted build software, and hardening of each system using ES&S's documented process. Firmware updates for the DS850, AutoMARK, ExpressVote, and DS200 machines were also loaded using the vendor provided procedures.

Issues & Observations:

During the configuration build, approximately eleven (11) issues were identified. Nine (9) required mitigation, while two (2) were observations made by the testers.

a. Documentation

Seven (7) issues were related to minor documentation discrepancies, which were given to ES&S for modification. The documentation was subsequently modified and the changes verified by the Secretary of State staff.

b. Server Hardware

One (1) issue was related to the server hardware. The operating system installation failed. An initial investigation determined it was unclear whether the issue was procedural or related to the hardware. The definitive determination was that the hard drives were not properly seated.

c. DS850

The next issue occurred with the DS850 validation. The consultants were unable to complete the hardware validation, as errors were generated when trying to run the comparison routine. It was determined the issue was due to an improperly formatted USB stick.

d. DS200 (Observation)

There was an observation made regarding the DS200 validation routine. The concern was that the validation routine no longer displayed the differences in dynamic files such as the log file. A decision was made to explore the scripts running the validation to see what was being excluded or specifically called. FCMG completed an analysis of the scripts, and determined the process to be complete.

Functional Testing Phase I

The first phase of Functional Testing consisted of following the Use Procedures to configure test elections. The testing included defining six (6) different test election definitions. The election type definitions, jurisdictions, and any anomalies noted are listed in the table below:

Table 2A: Election Definitions

Election Type	Jurisdiction	Anomaly Identified	Resolution
Primary	Sacramento County - June 5, 2012	None	None
General	Contra Costa	Ballot audio files	Jurisdictions should verify

	County – November 6, 2012	would not load. The cause was determined to be empty wave files that were rejected, and thus produced an error.	the wave files have actual sound prior to loading.
Primary – Countywide Vote Center Model	California Statewide Election – October 7, 2003	None	None
Recall Election	California Statewide Election – October 7, 2003	None	None
Recall Election with Recall Question	Fictitious Jurisdiction	The system offers two options for a Recall Election with a question. "Recall Question" or "Question".	The Use Procedures reflect the distinction between the two options. California jurisdictions should select the option to use "Question, followed by a standard contest.
Rank Choice Election	Fictitious Jurisdiction	The system can configure a Rank Choice Vote election; however the system cannot tabulate Rank Choice Vote results.	The system does produce a "Cast Vote Record"; however the data produced must be manually tabulated to follow a Rank Choice Vote algorithm.

Functional Testing Phase II

Phase II of Functional Testing consisted of exercising Logic and Accuracy (L&A) of the voting system. ES&S provided ballots for each type of election defined in **Table 2A**. Each ballot was marked with a test consultant pre-determined marking pattern, to demonstrate the L&A of the DS850 and the DS200 tabulators. There was one issue identified as listed below in **Table 2B**.

Table 2B: Logic and Accuracy

System	Issue Identified	Mitigation
DS200	During the verification of the results, the undervote results in several contests were reported as number of votes lost.	The discrepancy was due to an incorrect setting in Electionware. The issue was resolved and the results tabulated again. The results were audited and matched successfully.

3. Source Code Review Testing Summary

The Source Code Review was conducted by @sec (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.

The review was conducted at the Atsec offices located in Austin, Texas.

Atsec identified a total of thirteen (13) potential vulnerabilities and non conformities with industry programming standards within the system. Ten (10) are classified as medium and three (3) as high. The potential vulnerabilities are outlined below in the following tables, along with the vendor provided mitigations:

Table 3A: Medium Severity		
Issue	**Type**	**Mitigation**
Usage of SHA-1 for signature generation.	Potential vulnerability and non-conformity	While some weaknesses have been found using SHA-1, the algorithm is still viable.
Too small key size for RSA key and signature generation.	Potential vulnerability and non-conformity	The RSA key and signature generation method in EVS 5.2.1.0 meets VVSG standards and provides sufficient security protection when considered with all other security measures around the voting system in addition, it is also important to note that a new key is assigned for each election.
Derive symmetric key from simple hash.	Potential vulnerability	ES&S uses a separate USB stick known as the qualification media as the key transport mechanism. It is recommended that the qualification media be used only by the election central staff and kept in a secure location when not used to initialize machines for an election. The election public key (ESDSA P-384) transported via the qualification media is used to validate all election media content before any

		processing or decryption is attempted.
Usage of the DES algorithm.	Potential vulnerability and non-conformity	This vulnerability is referencing the AutoMARK ballot marking/voter assist device. The AutoMARK is a ballot marking device which validates each election using a SHA-256 hash. This process does not produce any digital output requiring the questionable algorithms referenced.
Usage of RIPEMD-160.	Potential vulnerability and non-conformity	This vulnerability is referencing the AutoMARK ballot marking/voter assist device. The AutoMARK is a ballot marking device which validates each election using a SHA-256 hash. This process does not produce any digital output requiring the questionable algorithms referenced.
Incorrect seeding of DRBG.	Potential vulnerability and non-conformity	DRBG has been determined to provide sufficient levels of security for this application.
Usage of /dev/urandom as TRNG for seeding a DRBG.	Potential vulnerability	On a headless system, /dev/random will block waiting on the entropy pool to be deemed "large enough" before returning. Through testing, the use of /dev/random as the seed was deemed unusable due to this blocking behavior. After thorough research, the use of the /dev/urandom was approved.
Usage of MD2 and MD5.	Vulnerability	The MD2 and MD5 hashes are not being applied to any of the election data consumed or generated by the tabulators or the other components in the system. As a result, this vulnerability is of very minimal concern.
Use of fixed/default IV value for encryption/decryption.	Potential vulnerability	In EVS 5.2.1.0, a different encryption key is generated for each election. Data is encrypted when it is being transferred between voting system components.
Source code vulnerabilities.	Potential vulnerability	EVS 5.2.1.0 was certified by the EAC on December 18, 2015. At that time, all source code was reviewed and approved by an EAC accredited Voting System Testing Laboratory (VSTL) to meet the EAC Voluntary Voting System Guideline (VVSG). These are the guidelines followed by ES&S engineers for all source code.

Table 3B: High Severity			
Issue	**Type**	**Consultant Assessment**	**Mitigation**
Audit records do not have sufficient safeguards to prevent alteration by a comprised or malicious administrator.	Potential vulnerability	A separate and distinct owner of the audit table would establish effective principles of least privilege.	Electionware and ERM use EVS Event Logging Service to control user access and store detailed logs of the actions performed on both systems. Both systems would shut down if such an attack was attempted.
Use of SECURITY DEFINER in PLPSQL stored procedures may allow privilege escalation.	Potential vulnerability	The use of this privilege management may need to be more tightly controlled by assigning segregated function owners or reduced in scope to mitigate the attack potential.	The database server is confined within a closed network architecture. Only an authorized Electionware client can connect and execute stored procedures on the server.
Use of weak default password for database administrative user.	Potential vulnerability	If this finding is mitigated by forcing a change of this password then no action is required. If a change is not required and enforced by some other method then corrective measures are needed.	The Manage module of Electionware has a setting, configurable by an administrator to set user password requirements such as password expiration every 90 days.

4. Red Team Testing

Red Team Testing of the EVS 5.2.1.0 voting system was conducted over a three-week period from May 22 to June 9, 2017, by Coherent Cyber, LLC, a subcontractor under the Freeman, Craft, McGregor Group (FCMG). The Red Team Testing consisted of a security audit and a penetration test assessment of the EVS 5.2.1.0 voting system and all of the respective components. The testing took place at the offices of Coherent Cyber, in San Antonio, Texas.

Coherent Cyber identified two physical security vulnerabilities. **Table 4A: Physical Security** lists both physical security vulnerabilities identified, along with the vendor provided mitigations:

Table 4A: Physical Security		
Issue	**Consultant Assessment**	**Vendor Mitigation**
Integrity Seals	Integrity stickers were removed from plastic cases without triggering integrity safeguard	The intent of a seal is to provide evidence of tampering. When properly used, a seal's serial number should be recorded when authorized administrators attach it

		to a machine, remove it, or replace it. In addition, each piece of hardware has designated location to which the seal must be attached. Therefore, if a seal is removed or damaged without proper documentation; this may indicate signs of tampering. In addition, per Use Procedures provided in the certification, E&S equipment should be locked in a secure environment with access granted to authorized personnel only. In addition, physical security should include a tight chain of custody and a pre-and post-election audit which should examine that each seal is properly documented and attached to each respective machine.
DS850 Lock	Every integrity seal, and all but one of the locks (the double-sided locks on the DS850), are vulnerable to straightforward attacks. In addition, the tamper evidence labels can be removed without triggering the tamper safeguards if they are applied to plastic surfaces. Another exploit on the DS850 revealed that a thin, stiff probe can be inserted through a gap in the door hinge, allowing the power switch to be activated or deactivated by unauthorized personnel.	The DS850 is a central tabulator and would therefore be stored in a secured central location under administrative supervision. Thus, this would make an attack on the lock highly unlikely. However, if an attacker did insert a thin probe through a gap and power off the DS850 during the tabulation process, the tabulator will retain the results in temporary storage until the DS850 is rebooted and results can be saved.

Coherent Cyber also identified Information Assurance Compliance vulnerabilities. Using the NIST Security Content Automation Protocol (SCAP), the servers and workstations supplied for testing were scanned for misconfigurations in accordance with US Federal Internal Audit standards. The following tables are incorporated by reference from the Security Audit Report.

Electionware Servers

Table 4B: Missing Operating Systems Patches	
Critical	17
Important	49
Moderate	2
Unrated	8

Table 4C: SCAP Misconfigurations	
Windows 2008 R2 STIG	46
Firewall STIG Configuration	3
.NET Framework 4 STIG Configuration	2
Internet Explorer 9 STIG Configuration	13

Electionware Clients

Table 4D: Missing Operating Systems Patches	
Critical	24
Important	51
Moderate	1
Unrated	9

Table 4E: SCAP Misconfigurations	
Windows 7 STIG	51
Firewall STIG Configuration	3
.NET Framework 4 STIG Configuration	2
Internet Explorer 9 STIG Configuration	3
Windows 7 USGCB Configuration	45
Firewall USGCB Configuration	8

Vendor Mitigation: The patches indicated in Tables 4B to 4E were released after ES&S obtained certification from the EAC. As such the system was hardened, and subsequently not modified with any additional patches or configurations beyond that point. Applying those patches would be a change to the environment, and would require testing for a new certification. Mitigation against attacks the aforementioned patches protect against, are mitigated by containing the client and server machines within a closed network environment.

Coherent Cyber identified eight (8) items during the vulnerability assessment. Each is outlined in the following table.

Table 4F: Vulnerability Assessment		
Category	**Component**	**Vendor Mitigation**
Remote Management Default Configuration	EMS	The vulnerabilities found in this section are mitigated through not only the physical security of the Election Management System (EMS), but also the internal setup of the EMS. In terms of physical security, the California Use Procedures for installing both servers specifically states the following: “For maximum security…cover all unused ports, including serial, parallel, USB, Ethernet, etc. using security seal tape whenever possible to prevent

		unauthorized access." With regard to internal security, the EMS is on a closed, local network. In other words, remote systems cannot gain access to this card. In addition, the certified configuration for a server excludes a network cable from being plugged into the iDRAC, thus disabling connectivity. If a network cable were plugged in, a user could potentially reboot/power off the system. However in order to get to this point, an attacker would need to gain credentials to (1) the BIOS, (2) Windows and (3) Electionware. Taking into account the physical security and internal security of the EMS, this vulnerability becomes less of an issue.
Unencrypted File System	ExpressVote, DS200, DS850	This reported vulnerability becomes less of a concern after physical security and election auditing is taken into consideration. ES&S equipment should be locked in a secure environment with access only granted to authorized personnel only. In addition, the equipment should be thoroughly tested during login and accuracy testing, sealed up, and physically secured proper to every election. If these procedures are properly followed, malicious activity would be detected prior to an election.
Unencrypted File System	ExpressVote	The ExpressVote Innodisk is located behind a locked and sealed door on the side of the unit. In order to visually see the Innodisk, an attacker would need a tool to physically remove the metal cover protecting the disk. Once the metal cover is removed, an attacker would need a specialized, non-standard tool to remove the Innodisk from the unit itself. Even if all of this took place, it is important to remember, the ExpressVote is a marking device that does not retain vote results information. Therefore, if there was a malicious attempt to compromise the outcome of any voter session, the selections made by the voter are physically printed prior to being scanned on one of the ES&S tabulators, giving the voter opportunity to ensure their selections are correct following their vote selection session.
Unencrypted File System	DS200	The DS200 compact flash card is located within the DS200 unit, with no outside access other than full disassembly. To gain access, an attacker would need to remove eight screws using a specialized tamper-proof security tool. Not only would the attacker need to remove these specialized security screws, they would also have to penetrate a series of seals. It is also important to remember, in the event of denial of service or evidence of tampering, EVS 5.2.1.0 being a paper-based voting system always offers the opportunity to rescan any suspect ballots.
Unencrypted File	DS850	The compact flash card for the DS850 is located on the

System		back of the machine. In order to gain access to the card, an attacker will need to bypass two locks in addition to wire and tamper evidence security seals placed on the unit. It should be noted that during the red team testing, the DS850 locks were unable to be penetrated and the tamper evidence seals functioned as intended. In addition, it is also worth noting the DS850 is a central tabulator and would not be accessible at any polling site. Rather, it would be located at election headquarters around numerous elections administrators in a secured environment; making an attacked on the DS850 highly unlikely. Again, because this is a paper-based system, should an attack of any kind occur, election officials always have the option of rescanning the ballot should any tampering be suspected.
Java Debugger Service Vulnerability		In order to gain access to the internal components of the DS200, an attacker would have to unscrew a minimum of eight (8) screws with specialized tamper-proof security tool, and remove the upper body of the unit. Again, it is also important to note that because EVS 5.2.1.0 is a paper-based system, election administrators would have the physical paper ballots in the case of exploitation.
Bytecode Decompiled into Human Readable Source		In order for this sort of attack to occur, the attacker must first gain access to the compact flash card. In addition, it should also be noted that the only proof of concept that was able to be tested was the zeroing out of election results. If this were to happen at the close of polls on Election Day, there would be clear evidence of tampering. In this situation, election officials need only go back to the physical paper ballot to determine how many ballots were cast at that particular polling place, and what the results were. It should be noted that DS200 are standalone units. As a result, in order for this sort of attack to have a significant impact, multiple units would need to be manipulated, which would be highly unlikely. If an attacker were able to compromise an election in a manner other than simply zeroing out results, the post-election audit and canvassing process would uncover manipulation of the election.
Unquoted Service Path Vulnerability & Database User Password Hash Dumping		If we take into consideration the physical security of these systems, this vulnerability becomes less of an issue. The EMS should always be in a secure room equipped with a physical chain of custody as to who has access. In addition, the EMS is configured to audit/log all user acts taken on the actual system. As a result, if something like this were to happen, the event themselves

		would be logged. If an attacker tried to stop the audit logs, the EMS will shut down and not be accessible. In addition, hardening of the system restricts normal users from having write access to the path for the services in question. Therefore, in order for this to even take place, an attacker would need to have sysadmin access which would only be granted to one individual. In addition, before an attacker would be able to get to the windows log in, they would have to get through a bios system password in addition to a bios setup password. As a result, it would be highly unlikely to not only insert malicious services, but also run a password hash dump.

5. Volume Testing Summary

The Volume Test simulates conditions in which the system components would be used on Election Day. Volume testing of the EVS 5.2.1.0 voting systems was conducted over two days at the Solano County Elections Office from June 26 to June 28, 2017. Approximately fifteen (15) temporary workers were hired from a third party contractor.

The equipment used in the testing consisted of twenty (20) AutoMarks, twenty (20) DS200 tabulators, and ten (10) ExpressVote units. Both the AutoMark and DS200 are currently certified for use in California, with previous firmware version numbers.

Machine and Ballot Count

Hardware Component	Number of Machines	Number of Ballots per Machine	Ballot Pages	Total for All Machines
DS200	20	418	Two	8,360
AutoMark	40	50	Two	1,000
ExpressVote	10	100	1	1,000

Error Log

Hardware Component	Number of Errors
DS200	19
AutoMark	32
ExpressVote	0

The DS200 experienced approximately nineteen (19) errors, with the vast majority being related to ballot jams. The ballot jams were remedied and instructions to resolve such issues are covered in the Use Procedures, which were also subject to validation and review during the testing process.

The AutoMARK experienced approximately thirty-two (32) errors. Most were printer errors resulting in the ballot not being ejected, restarting the machine to resolve printing issues, and paper jams.

ES&S would like the record to reflect that this volume test did not represent normal usage of the machines. In a real life scenario, the DS200 and the AutoMARK would not have constant ballots being fed into them. During this examination, the constant feeding of ballots within the DS200 did not give it time to drop the ballot into the ballot box before the next ballot was fed. This caused ballots to get bunched together resulting in higher than usual jams.

The ExpressVote did not experience any errors during the Volume Test.

6. Accessibility and Usability Testing Summary

Accessibility testing of the EVS 5.2.1.0 certification took place on June 29 and June 30, 2017, at the California Secretary of State Auditorium. The EVS 5.2.1.0 system has the AutoMark and ExpressVote systems, to meet accessibility requirements in a polling place.

Each system has a touchscreen interface, and auxiliary ports that can be used for such devices such as a sip and puff or a large paddle switch. Both systems are capable of allowing a user to use either an audio ballot or visual presentation the ballot. Both types of functionality can be used exclusively or simultaneously. The systems also have features to allow a voter to verify the selections made, by having the system read the selections back to the voter, or displaying the selections onscreen. Both also support write-ins and warnings for undervotes.

Approximately six (6) testers participated in the Accessibility testing. On June 29, four (4) testers marked ballots using both the AutoMark and the ExpressVote machines. Three voters were visually impaired, and one had mobility and dexterity impairments. On June 30, two (2) testers used the same systems to mark ballots. Each user had mobility impairments; one of the voters also had a dexterity impairment.

All testers were given a post test interview to document their experience. The cumulative results are listed below in **Tables 6A and 6B**. Specific comments and opinions regarding each tester's experience, as well as individual responses can be found in Attachment A of the Accessibility Test Report.

Table 6A: ExpressVote Post Test Survey

	Agree Strongly	Agree Somewhat	Disagree Somewhat	Disagree Strongly	N/A or No Opinion
The voting method was private	5	1			
I feel I can use this system to vote independently.	4	1	1		
I am confident	5				1

that my vote was recorded accurately.					
The voting instructions were clear and complete.	3	2			1
The voting method was easy to use.	4		1	1	
I could read the display easily.	3				3
I could understand the speech output.	3		2	1	
The assistive device(s) were easy to reach and use.	4		1	1	
I found the system confusing to use.		2	1	3	
The timeframe it took to vote was what I expected.	2	2	1		1

Table 6B: AutoMark Post Test Survey					
	Agree Strongly	Agree Somewhat	Disagree Somewhat	Disagree Strongly	N/A or No Opinion
The voting method was private	3	3			
I feel I can use this system to vote independently.	5	1			
I am confident that my vote was recorded accurately.	4	1			1
The voting instructions	5		1		

were clear and complete.					
The voting method was easy to use.	4	2			
I could read the display easily.	2	1			3
I could understand the speech output.	2	1			3
The assistive device(s) were easy to reach and use.	3	1	1		1
I found the system confusing to use.			2	4	
The timeframe it took to vote was what I expected.	4		1		1

IV. COMPLIANCE WITH STATE AND FEDERAL LAWS AND REGULATIONS

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.

1) §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.

2) §19101 (b) (2): The system shall preserve the secrecy of the ballot.
   The system presented for testing lacked both a privacy screen and a privacy sleeve for voters using the AutoMARK. With the addition of both, the system should protect the secrecy of the ballot.

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

The system is at least as secure as the previously certified version of this ES&S system. The addition of the DS200 precinct scanner, the DS850 central scanner, and the ExpressVote to the system does not introduce new risks to fraud or manipulation.

4) §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.

5) §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.

   The system meets this requirement. EVS 5.2.1.0 supports English, Spanish, Chinese, Korean, Japanese, and Bengali. 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.

6) §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.

7) §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.

8) §19205 (a): No part of the voting system shall be connected to the internet at any time.

   The system meets this requirement.

9) §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.

10) §19205 (c): No part of the voting system shall receive or transmit wireless communications or wireless data transfers.

The system meets this requirement.

11) §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.

1. **Elections Code Review**

1) §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.

2) §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.

3) §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.

4) §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.

5) §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 complies with these requirements.

6) §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 complies with this requirement.

7) §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 meets this requirement.

8) §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.

9) §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.

10) §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.

11) §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.

12) §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.

13) §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.

14) §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.

2. Review of Federal Statutes or Regulations.

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 fully meets this requirement. The system's paper ballots can be easily printed in these languages, as well as any others. Further, both the AutoMARK and ExpressVote 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.

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.

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

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.

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

3. 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:

1) The paper ballots themselves lend themselves to visual inspection and verification.

2) The AutoMARK and ExpressVote provide its users with a ballot review screen prior to printing the ballot. Further, any voted ballot can be inserted into the ballot for review and verification.
3) The AutoMARK and ExpressVote prevent over-voting a contest.
4) Because all ballots in this system are paper based, there is a fully auditable permanent record of the election.
5) Deployment of the AutoMARK and ExpressVote in a precinct provides accessibility for persons with disabilities at the polling place.

V. CONCLUSION

The EVS 5.2.1.0 voting system, in the configuration tested and documented by the California Installation and ES&S's Use Procedures, meets all applicable California and federal laws. The ES&S EVS 5.2.1.0 voting system is compliant with all California and federal laws.