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

HART INTERCIVIC INC.
VERITY VOTING 3.0.1

Components
Verity Scan: Software version 3.0.1
Verity Touch Writer: Software version 3.0.1
Verity Reader: Software version 3.0.1
Verity Print: Software version 3.0.1
Verity Device Microcontroller: Software version 17
Verity Data: Software version 3.0.1
Verity Build: Software version 3.0.1
Verity Central: Software version 3.0.1
Verity Count: Software version 3.0.1
Verity Election Management: Software version 3.0.1
Verity Desktop: Software version 3.0.1
Verity User Manager: Software version 3.0.1

Staff Report

Prepared by:
Secretary of State's Office of
Voting Systems Technology Assessment
September 5, 2018

Table of Contents

I. INTRODUCTION

1. Scope

This report presents the test results for the certification testing of the Hart InterCivic Inc. (Hart) Verity Voting (Verity) 3.0.1 voting system. The purpose of testing is to evaluate the compliance of the voting system with California Voting Systems Standards, and State & 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 California Use Procedures.

2. Summary of the Application

Hart submitted an application for the Verity Voting 3.0 voting system on September 14, 2017. In addition to the software, which includes the executable code and the source code, Hart was required to submit the following:

- The Technical Documentation Package (TDP);
- 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 Security Test Phase;
- 20 Verity Touch Writer ballot marking machines, and all the peripherals that would be in the polling place;
- 50 Verity Scan precinct scanners, and all the peripherals that would be in the polling place; and
- The California Use Procedures.

During the Security and Telecommunications Testing and Software Testing of the Hart InterCivic Verity Voting 3.0 voting system, potential vulnerabilities were discovered in the system that required mitigating changes to the voting system. Hart's changes were sufficient to require a new version number. The new version number is 3.0.1. Hart provided an updated Application, Technical Documentation Package (TDP), California Use Procedures, Change Log, and Source Code for the modified Verity Voting 3.0.1 voting system on August 20, 2018. Regression Testing was performed to verify the effectiveness of the changes and ensure that the changes did not degrade the system's functionality, efficiency, or accuracy.

The voting system is comprised of the following major software components:

- Verity Scan: Software version 3.0.1;
- Verity Touch Writer: Software version 3.0.1;
- Verity Reader: Software version 3.0.1;
- Verity Print: Software version 3.0.1;
- Verity Device Microcontroller: Software version 17;
- Verity Data: Software version 3.0.1;

- Verity Build: Software version 3.0.1;
- Verity Central: Software version 3.0.1;
- Verity Count: Software version 3.0.1;
- Verity Election Management: Software version 3.0.1;
- Verity Desktop: Software version 3.0.1; and
- Verity User Manager: Software version 3.0.1.

3. Contracting

Upon receipt of a complete application, the Secretary of State released a Request for Proposal (RFP) for assistance with the Security Review, which is comprised of Security/Telecommunications and Source Code (Software Review) Testing.

Through the formal California contracting process, the Secretary of State awarded a contract to Freeman, Craft, McGregor Group (FCMG) of Tallahassee Florida.

II. SUMMARY OF THE SYSTEM

The Verity Voting 3.0.1 system is a paper-based voting system consisting of the following major components: Verity Election Management System (EMS), Verity Data (Data), Verity Build (Build), Verity Central (Central), Verity Count (Count), Verity Scan (Scan), Verity Touch Writer (Verity Touch Writer), Verity Print (Print), and Verity Reader (Reader).

1. Election Management System

The Verity Election Management System set of applications are responsible for all pre-voting and post-voting groups of activities in the process of defining and managing elections.

The complete EMS software platform consists of client (end-user) and server (back-end) applications as follows:

- Verity Data: Data is used by election officials to enter election data for contests, candidates, proposition text, translations, and audio. Data also provides the user with controls for proofing of data, layout, and performs validation prior to locking the data to ensure its readiness for use in Verity Build, the election definition software.

- Verity Build: An election definition and device settings component. Build is a required component of the Verity Voting system, used by officials to complete pre-voting tasks for creating and generating an election definition and ballots. Build provides a ballot layout proofing process. The process establishes relationships between election data, jurisdiction, and polling place data for the shared election definition. Build will create the portable media, called vDrives, to provide a method of transferring the shared election definition to Verity Voting

machines and other Verity components. vDrive uses an “air-gap,” or non-networked transfer method, to provide more secure exchange of election data.

- Verity Central: A central ballot scanning and adjudication component used by officials for paper ballot scanning, contest resolution, and conversion of voter selection marks to electronic Cast Vote Records (CVRs). Once the CVRs are written to vDrive(s) they can be transferred into Verity Count for vote tabulation and reporting of election results. Verity Central records cast vote records only; it does not tabulate.

- Verity Count: Used by officials to complete post-voting functionality to tabulate election results and generate reports. Count receives the CVRs from portable media devices (vDrives) used to record CVRs from Hart voting machines or Verity Central workstations. Verity Count can be used by officials to resolve Verity Scan or Verity Central write-in votes for paper ballots that were manually marked. Count can also be used to collect and store all election logs from every Verity component/machine used in the election, allowing for complete election audit log reviews.

- Verity Election Management: The Election Management application is available only on Verity server workstations. This software enables authorized users to add, import, export, archive, restore, and manage elections. Once an election is added or imported into the Election Management application, the election can be opened and handled per the features available within the Verity software installed on that workstation.

- User Management: This software enables authorized users to create and manage user accounts within the Verity system.

- Verity Desktop: Allows authorized users to manage a very limited set of operating system functions. Verity Desktop is workstation management software used for:

    - Setting the system date and time.
    - Exporting Verity application file hashes to removable USB media.
    - Accessing the operating system for a limited time (less than twenty four hours per access code). User access to the operating system’s functionality is restricted to software updates and database management.
    - Importing printer configuration files.

2. Verity Print

Verity Print is a pre-voting ballot production machine for use by election officials and/or poll workers. Verity Print produces unmarked paper ballots. Verity Print is paired with a commercial off-the-shelf printer to allow the user to select and print the desired ballot style based on the precinct and voter registration information.

The Verity Print machine is activated so the election official can print one or more blank ballots from one selected precinct at a time. Ballots can be printed on-demand for immediate use, or they can be printed in advance for additional inventory.

3. Verity Touch Writer

Verity Touch Writer is a touch-screen Ballot Marking Device (BMD) that prints voter-marked ballots to a commercial off-the-shelf printer.

Voters use the electronic touch display interface to privately and independently make their selections on the ballot. Voters can also make selections with Verity Access, an Audio-Tactile interface (ATI) component with three tactile buttons, one audio port (for headphones), and one port for external two-switch machines. When voters finish making their selections, they print the marked ballot.

4. Verity Reader

Verity Reader is an optional paper ballot review machine suitable for use by all voters, including non-disabled voters and voters with disabilities. Voters insert their marked paper ballot to visually verify how their ballot will be counted when the ballot is cast in the Verity system, and/or hear audio read-back of their ballot choices. For voters with disabilities, Reader offers the same accessibility features as the Verity Touch Writer ballot marking machine.

5. Verity Scan

Verity Scan is Verity's digital scanning solution for paper ballots. Scan is paired with a purpose-built ballot box to ensure accurate, secure, and private ballot scanning and vote casting.

When opening the polls, authorized users activate the Verity Scan machine to prepare it to receive marked paper ballots. Scan indicates when it is appropriate to insert ballots, and when ballots have been successfully cast. Verity Scan records Cast Vote Records and audit log data in redundant, secure storage locations, including the Verity vDrive. vDrive storage is portable flash memory and allows the CVRs to be transferred to the Verity Count tabulation and reporting system.

6. Verity Access

Verity Access is an interface module that is connected to Verity Touch Writer and Verity Reader. The module has three tactile buttons, one audio port, and one port for external tactile buttons or sip-n-puff devices. Jacks for headphones and adaptive devices are located on the top edge of the machine, and the machine has grip surfaces on either side.

7. Verity AutoBallot

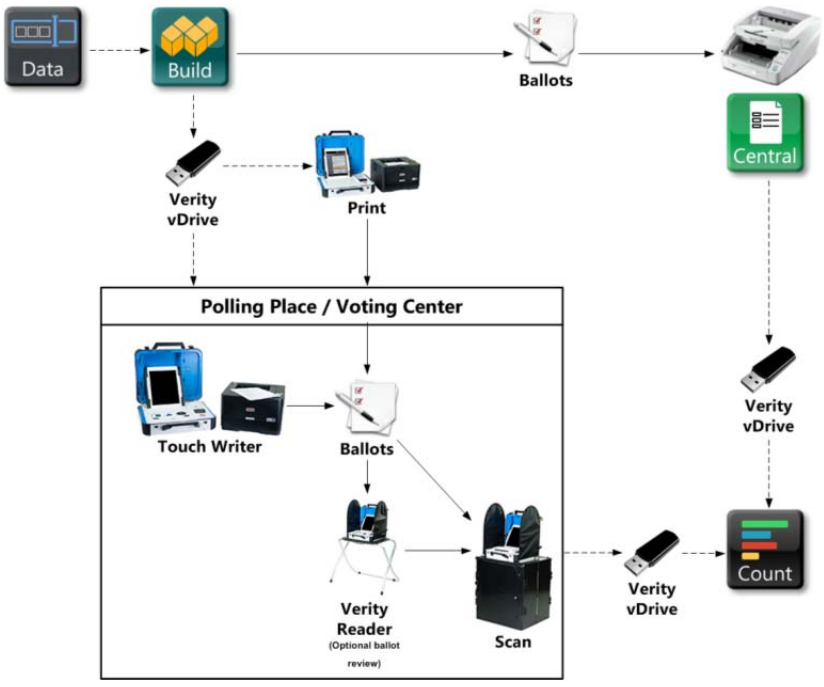
Verity AutoBallot is an optional barcode scanner kit for Verity Print and Verity Touch Writer that allows air-gapped integration between an electronic pollbook check-in process and the task of selecting the proper ballot style for the voting system. Particularly when Verity Print or Verity Touch Writer is configured with dozens or hundreds of ballot styles in Vote Centers, Verity AutoBallot simplifies and automates the ballot style selection process by allowing poll workers to scan a barcode output from an electronic poll book, and activate the correct ballot style with the click of a button, thereby reducing human error. Once the ballot style has been input with the barcode scanner, the poll worker confirms the ballot style on the Verity machine display and prints an unmarked ballot (Verity Print), or activates an accessible electronic voting session (Verity Touch Writer).

8. Verity vDrive

Verity vDrive is a required Verity Voting component, used as a portable media device generated by Verity Build. vDrive allows election definitions to be moved from Verity Build to Verity Scan, Verity Touch Writer, Verity Reader, and Verity Print. vDrive supports the transfer of Cast Vote Records in Verity Scan and Verity Central.

9. Verity Key

Verity Key is electronic media that is created by Verity Build for a specific election. Key is a required Verity component. Key is the electronic media that provides user authentication and configures election security throughout the Verity Voting system.



III. TESTING INFORMATION AND RESULTS

1. Background

California certification testing of the Verity Voting system began in April, 2018. The testing began with the Software Review, followed by Functional Testing, Security/Telecommunications Review, and finally Volume and Accessibility Testing.

2. Functional Test Data

The Functional Test of the Hart Verity Voting 3.0 system was conducted by Office of Voting Systems Technology Assessment Staff at the Secretary of State's Office located at 1500 11th Street, Sacramento, California from April 9, 2018, through May 4, 2018.

The Secretary of State ran the Functional Test as if it were a jurisdiction that just purchased the voting system. The Functional Testing began by installing the complete system. The eight computerized components of the EMS tested were all Hewlett Packard Z240 computers: Central Server, Central Client, Data Build Standalone, Count Standalone, Count Server, Count Client, Data Build Server, and Data Build Client. The proprietary machines tested (Scan, Print, Reader, and Verity Touch Writer) are all tablet computers running in custom cases designed for polling place applications. The system is modularized so that all the polling place machines are running one of two versions of the same hardware. Following the TDP procedures, Functional Testing started by building the operating system. Hart is licensed by Microsoft to build their own versions of the Windows 7 Operating System. The version built is a scaled down operating system without any unneeded applications or utilities included. Hart does not have access to the Microsoft Source Code, and there is no proprietary Hart code in the operating system. This reduces the attack surface of the operating system to only those components needed to operate the voting system. Two versions of the OS were built, a thirty-two bit version for the tablets that Scan, Print, Verity Touch Writer, and Reader are built on, and a sixty-four bit version for Data, Build, Count, and Central. Next, the trusted build of the application installers was compiled from Source code. FCMG witnessed the build and took possession of a duplicate copy of the source code for Source Code Review testing. Following the California Use Procedures, the testing continued with the installation of the operating system, commercial-off-the-shelf software, voting system trusted build software, and then continued through the security hardening process. Upon completion of the installation of the system, it was run through an acceptance and readiness test to determine that each piece of equipment was functioning properly and that all networking and permissions were configured correctly. A second complete set of the system was built at this time for the FCMG Security team to utilize for the Security/Telecommunications portion of testing.

Functional Testing of the system included six main election types, a Presidential Primary, a Presidential General, a Special Recall, a Single Seat Ranked Choice Voting (RCV), and a Vote Center Election. The specific election definition databases used in testing were based on a modified version of the 2012 Sacramento County Presidential Primary in English and Spanish, a modified version of the 2012 Contra Costa

Presidential General in English, Korean, Chinese, and Vietnamese, the 2003 California Statewide Special Recall Election in English, Khmer, Japanese, and Hindi, a fictitious single seat RCV Election with six candidates in English, Ilocano, Tagalog, and Thai, and a modified 2012 Presidential Primary for the vote center election. The vote center election ballots were machine pre-folded in a tri-fold format.

The mock elections were conducted as if the system had just been purchased by a county. The vote center/precinct machines were setup for either early voting or Election Day voting. Ballots were produced on demand and as needed with Print. The Verity Touch Writer ballot marking device was utilized for accessible voting sessions, and the Reader machines were used to validate the ballots marked on the Verity Touch Writers. On demand ballots were produced on the Verity Print, and accessible sessions initiated on Verity Touch Writer utilizing either manual input or the Verity AutoBallot barcode scanning machine. Ballots were scanned on Scan machines, and validated by scanning a second time on Central. Polls were opened, and repeatedly suspended and re-enabled on the Scan machines setup for early voting. At the close of polls, the vDrives from the Scan machines were loaded onto Central to scan again, and then were brought into Count to tabulate and generate all reports. Ballots containing an exception condition, a write-in, under-votes, or over-votes were resolved using the resolve screen on the Central or Count machines. The resolve screen will allow an election official to import qualified write-ins, and review unqualified write-ins to verify voter intent. After all ballots were tabulated, the Cumulative Report was printed, and all other reports were generated. Additionally, the Secretary of State Statement of Vote (SOV) and Supplemental Statement of Votes (SSOV) reports were generated. Comma separated text files were generated to simulate election night auto-reporting, however, the templates for the test elections were not available so it was impossible to test. Note that the above description was followed for all test elections, however, each election was also used to test specific items, such as ballot layout rules and laws, battery backup capacity, scanner read-head tests to determine the consistency and accuracy of different types of marks using different marking machines simulating actual voters who vote by mail, language tests to determine if the system can populate all fonts used in California correctly and accurately, as well as the capability of the system to operate in a vote center environment that may constitute many more voters both for early voting and on election day.

Presidential Primary Election: The Presidential Primary Election was based on a modified version of the 2012 Sacramento County Presidential Primary in English and Spanish. The election included ten precincts and eight party splits per precinct. It included nineteen contests and sixty four choices. English ballots were pre-printed single sided on eight and a half by twenty inch stock. The Hart vDrive duplicator was used to generate vDrives to transfer the election definition to one Print machine and two Verity Touch Writer machines. Print was utilized manually (the poll worker enters the precinct number for ballot style) to print fifty single sided Spanish, and six Spanish/English ballots, utilizing eight and a half by twenty inch stock. These ballots were marked by hand. Eight ballots (one from each party), and one Spanish ballot were generated on the Verity Touch Writer ballot marking machine, and then verified on Reader. It was discovered that the instructions were clear to understand, and the write-in functionality was used with no difficulty. Voting for a write-in did not require cycling

through the entire alphabet, but allowed for easy back and forth using the on screen keyboard. One Scan machine was configured for early voting, and one Scan machine was configured for precinct voting. Once the precinct scanners are setup, they will not accept anything that is not signed for this election. The Scan machines were configured to reject under-votes and over-votes which allowed for voter review. When a ballot is rejected for review, the voter can choose to both remove the ballot and edit it, or to cast the ballot as-is. Ballot rejection for voter review on the Scan machines is election wide and cannot be set by precinct. Polls were opened and zero tapes printed. Ballots in English and Spanish were scanned on both the early and election day Scan machine without problem. Ballots were fed in all four orientations. The landing lights, in conjunction with the audible tone, make it very apparent that the ballot has been read, and the machine is ready for another ballot. The Scan machines processed the twenty inch ballots at a steady rate of six to eight per minute. Ballots were fed two at a time, and the machine correctly identified the problem. The Scan machine configured for early voting was suspended, powered off, powered on, and re-enabled without problem. Polls were closed, and the results were transferred to the Central machine by signed export. A qualified write-in was created in the resolve screen, and both qualified and unqualified write-ins were resolved. All reports were generated and saved.

Recall Election: The Recall Election was comprised of one precinct and two contests. A dependent contest was used per the election at that time, and one hundred and thirty five choices with one write-in in a gubernatorial contest, printed on eight and a half by twenty inch stock. The Recall Election was tested in English, Khmer, Japanese, and Hindi. The ballots were machine pre-printed in English, and Verity Print was utilized to print twenty five ballots each in Khmer, Japanese, and Hindi. Verity Touch Writer was used to successfully mark several ballots each in all languages, and the ballots were verified on Reader, but we could not verify the accuracy of the actual translations. The vDrive duplicator was used to duplicate additional vDrives to distribute the election to Scan, Print, Verity Touch Writer, and Reader. One Scan machine was setup for early voting, and one for Election Day voting. The Scan machine setup for early voting was repeatedly suspended, powered off and back on again, and re-enabled without problem. Three ballots were fed together, and the machine correctly identified the problem and would not pick them up. The machine also correctly identified when two ballots were fed together. The Scan machine threw a “cannot read barcode error” three times, and each time the error was easily mitigated by simply feeding the ballot in a different orientation. The Verity ballot utilizes redundant bar codes on the front and back of the ballot for timing, and it was discovered that an unclear print or discrepancy on the bar code could cause problems with timing. Using a Sharpie black marker, a ballot was marked with additional lines at the bar code, effectively extending the bar code by four lines, and Scan was unable to read the ballot. The polls were closed, the results were exported to Central using a signed export, and the cast vote records were tabulated again. All reports were generated successfully on Count.

Presidential General Election: The Presidential General Election was modeled from the 2012 Contra Costa Presidential General, on single and double sided, eight and a half by eleven inch ballot stock. The election was comprised of ten precincts, and eighteen contests with forty seven options. The election was tested in English, Korean, Chinese, and Vietnamese. English ballots were machine pre-printed, and Print was

used to print twenty five ballots each in Korean, Chinese and Vietnamese. The Scan machine was configured for early voting, and we opened the polls and scanned the eight and a half by eleven ballots at a steady rate of one every three seconds. The double sided ballots incremented the ballot and sheet counters and the single sided ballots only incremented the ballot counter. Four ballots were folded into quarters, and then unfolded and scanned without error. Two ballots were slightly shredded along the edges, and when straightened, fed without error. A black Sharpie marker was used to mark over most of the white space on several ballots, and the Scan machine digested them without error. An under-voted ballot was fed into the Scan machine, rejected for the voter to edit or accept, and then left for ten minutes. When the voter returned, the ballot was finished without error. Twenty-five ballots each in English, Korean, Chinese, and Vietnamese were generated on Print, and five ballots in each language were marked on Verity Touch Writer, and then verified on Reader without error, however the actual translations were not verified.

A second election utilizing the Presidential General Election was setup on another Scan machine. Three ballots were tested for marginal marks, and marked with pencil, red-blue-black Sharpie, red wet erase pen, blue and black ink pen, and yellow highlighter. The ballots were marked with completely filled in bubbles, 'snowmen' where the mark was on top of the bubble, circles around the bubble, a small dot in the bubble, one end of the bubble was filled in, Xs, check marks, and various small dots. The ballots were all resolved in Count, simulating a small county that had only purchased Count and not Central. Anything outside the bubble was not picked up as a vote. All marks inside the bubble, including very small dots, were picked up as a vote. Only the yellow highlighter was not picked up as a vote.

RCV Election: The Ranked Choice Voting Election consisted of one ballot style with one contest containing six ranked choice candidates in English, Tagalog, Ilocano, and Thai. Twenty each of Tagalog, Ilocano, and Thai ballots were printed on the OKI C911 printer, as well as twenty each of Ilocano/English, Tagalog/English, and Thai/English. Print was utilized to print one dozen additional ballots of each. The test deck was hand marked, and the polls were opened. Zero reports for all machines were printed and verified. Ballots were scanned on Central simulating a jurisdiction that only uses central tabulation, and the first round of voting was verified. Verity Voting 3.0 does not perform RCV tabulation. Rather, it tabulates the number of votes for each candidate in each ranking and produces a "cast vote record" in an XML file for each ballot. This file shows the ranking assigned to each candidate and can be used either to tabulate the vote manually or to process the cast vote record through applications outside of the system. Count will export the XML file for this purpose. Polls were closed and all reports generated and saved.

Vote Center Election: The Vote Center Election was a fictitious election based on several different elections and included five contests, ten choices, and three thousand precincts. The Vote Center Election was printed in English on eight and a half by eleven stock and the ballots were machine tri-folded, stored for a week, and then unfolded by hand to simulate vote by mail ballots. One Scan machine was configured for Election Day voting, to simulate a small jurisdiction that only purchased one or more Scan machines to use as central scanners, and one Scan machine was configured for early

voting as in a vote center. Twenty eight hundred and sixty six ballots were fed through the two Scan machines, approximately half through each machine. The Scan machine configured for early voting was suspended, powered down and back on, and re-enabled during the election. All ballots were then scanned on Central to simulate a larger jurisdiction.

AutoBallot was tested utilizing a paper list of barcodes that matched every precinct/ballot style in the election to simulate barcodes generated from an electronic pollbook. AutoBallot utilizes a 1D or 2D barcode. Fifty barcodes were scanned at random, and fifty ballots printed on Print throughout the entire list to simulate voters arriving at the vote center, and requesting a replacement ballot for a spoiled one. AutoBallot initiated Print ballots printed as expected. Barcodes can be scanned either straight up or upside down, and at up to a forty five degree angle with no problem. The bar code reader will not function sideways. AutoBallot can be used for Verity Touch Writer to initiate an accessible session for a voter. We scanned twenty five barcodes at random from the list, to simulate a voter with disabilities who arrived at a vote center wanting to vote. During these AutoBallot initiated Verity Touch Writer voting sessions, the audio, text size, ability of Verity Touch Writer to back up through all previous screens, and all options were exercised again, and the generated/marked ballots were verified with Reader. If a voter personalizes a session in Verity Touch Writer by for instance choosing large print, the ballot automatically shows up as large print on Reader. Whatever language the ballot is printed in also shows up in Reader correctly. Autoballot initiated Verity Touch Writer sessions functioned as expected, and Reader checked all ballots successfully.

During the Vote Center Election, the Scan machine was unplugged and ran on battery power for the required two hour minimum without problem. However, it was discovered that once the battery is used up, it must be removed from the Scan machine and charged using a battery charger.

Test results showed that the voting system performed in a manner consistent with California Elections Code and all test cases were executed successfully and accurately. The testing did uncover several issues in the California Use Procedures. All were clarity issues and each of the issues discovered was resolved by editing the California Use Procedures.

4. Volume Test

The Secretary of State conducts a Volume Test on all voting machines under test with which the voters will directly interact. The Volume Test took place between June 11, 2018, and June 13, 2018. The Volume Tests used a modified version of the 2012 Contra Costa General Election as the basis for the election definition files. The Verity Scan precinct tabulators and the Verity Touch Writer ballot marking machines presented for the Verity Voting test are new components that have never been tested in California. Per the California Volume Test Protocol, the Volume Test consisted of a total of fifty Scan machines, and twenty Verity Touch Writer machines. The Secretary of State used a total of eighteen voters, ranging in age, skill, and voting experience, to vote ballots on

the machines. The fifty Scan machines were labeled in numerical order of #1 through #50, and the twenty Verity Touch Writer machines were labeled in numerical order of #51 through #70 for proper identification.

Hart provided fifty test decks, each with one thousand ballots for the Scan machines. The Scan machines were tested first, and a total of one thousand ballots were tabulated by each machine to simulate the voters a precinct or vote center would have on Election Day. As the test was being conducted, all incidents were documented. The zero tapes created when the polls were opened were kept on the machines, and along with the results after the polls were closed, were saved as artifacts.

During the Volume Test, the Scan machines threw three different errors. The "Your ballot did not Scan" error was encountered fifty four times on twenty-three machines for an error rate of .00108. In every case, the error was mitigated by pulling the ballot from the machine, and re-inserting it. Several of the voters suggested this was actually a result of inserting the ballot too quickly, or not inserting the ballot straight into the machine. An error was encountered twelve times on six machines in which the machine read the ballot correctly, but the pickup rollers on the machine kept spinning. The machines recovered gracefully on their own from this error three times, and the other nine times the error was mitigated by lifting the cover where the ballots are inserted and pushing it closed again. This represents an error rate of .00018 for the nine errors that the machine did not gracefully recover from. Finally, there was one error in which a printer ran out of toner. The Verity Touch Writer machines did not encounter any errors.

During the Volume Test, the battery capacity was tested on the Verity Touch Writer machine and printer combination. Several tests were run utilizing an external UPS (Uninterruptible Power Supply), and the Verity Touch Writer machine lasted approximately one and a half hours with six ballots printed. A larger capacity UPS would prolong the capacity.

The Verity Touch Writer ballot marking machines were tested next. Fifty ballots were marked and created on each Verity Touch Writer machine, for a total of one thousand ballots created. No incidents were reported on the Verity Touch Writer machines. Out of the one thousand ballots generated on the Verity Touch Writer machines, there were no ballot marks outside of the square, and all marks were exactly as expected.

After the test concluded, the Secretary of State verified the results of vote totals against the expected results. There was one error, which was attributed to a printing error in which a dot the size of the point of a ball point pen was in a box on the ballot. The tabulator correctly counted this as an overvote. The verification resulted in a 100% accuracy rate. Based on the fact that the Verity Touch Writer performed with a 100% accuracy rate and the incidents and poll worker intervention rates were well below the 2% ballot rejection rate allowed by the California Voting System Standards, the Volume Test for the Scan precinct tabulator, and the ballot marking functionality of the Verity Touch Writer was deemed successful.

5. Accessibility Test

The Accessibility Test used a modified version of the 2012 Contra Costa General Election as the basis for the election definition files. Accessibility Testing took place in two sessions. The first session was May 3, 2018, and the second was June 14, 2018, and June 15, 2018. The Secretary of State partnered with volunteers from the voters with disabilities communities to complete the heuristic evaluation of the accessibility features of the Verity Touch Writer and Reader components, as well as to provide findings in this report. The Accessibility Test consisted of Verity Touch Writers, Readers, and Scan components. The machines were setup in voting stations, giving enough space in between to allow some privacy. Each voting station contained one Verity Touch Writer component, one Reader component, one video recording camera with microphone, one table, two chairs and a laptop or clipboard for note taking by Secretary of State Staff. The voters all used a common Scan component to simulate casting their ballot.

Voters who were voting an Accessible Voting Session (AVS) had the ability to use any of the following components: the Audio Tactile Interface (ATI), lap pad, adaptive/paddle switches, headphones, sip and puff device, or rubber coated lap pad with ATI.

The Verity Touch Writer component has the capability to support voters with the following disabilities:

- Cognitive - ballot display via paper and large LCD screen;
- Perceptual and Partial Vision - ability to change screen color scheme, contrast, and font size;
- Low or No Vision - audio, tactile interface;
- Dexterity - integrated ballot marking machine that does not require the voter to manipulate the ballot, low force buttons for voter interface;
- Mobility –California Voting System Standards required reaches and wheelchair access, Verity Touch Writer product requires voter to mark the ballot on the Verity Touch Writer component, then go from the ballot marker to the Reader to verify, and then to the Scan component to cast their vote;
- Hearing - audio interface, same as for low/no vision; and
- Speech - no speech is required to operate the voting system.

The Secretary of State tested the voting system for usability and accessibility with ten volunteer voters from the general population with the various disabilities mentioned above. These volunteer voters were asked to vote at least one ballot each on the Verity Touch Writer component.

The Secretary of State also had the assistance of three staff members who documented the test process and experience for each volunteer voter, and two Hart representatives, who acted as poll workers. The voters were trained by Hart personnel on the system and how to use the accessible features.

The Secretary of State provided a survey for each voter. The survey asked ten questions describing the voter's experience with the voting system. To categorize responses, the first ten questions were specific to the voting system. The questions and responses can be viewed in Appendix B.

The consensus of the volunteers was that they felt the technologies implemented for accessibility and usability improved the experience for voters that are most in need of them. From a privacy point of view, all volunteers seemed to feel that their privacy was kept intact and none expressed any issue or concern.

6. Security & Telecommunications Review

The Security & Telecommunications Review conducted by FCMG took place at the Secretary of State's test lab between May 14, 2018, and May 18, 2018.

FCMG discovered eight vulnerabilities:

- Locks and tamper seals are subject to picking and removal (Table 1);
- Unrestricted access to workstation cases (Table 2);
- Lack of Full Disk Encryption (Table 3);
- Server Spoofing Credential Disclosure (Table 4);
- Shared/Hardcoded Secrets (Table 5);
- Unnecessary Applications Available on System (Table 6);
- Weak Authentication Encryption for Verity Key allowing unauthorized modification of election result (Table 7); and
- Code Execution via Untrusted Deserialization (Table 8).

Table 1: Locks and tamper seals are subject to picking and removal

Category	Component	Vendor Comments	Vendor Mitigation
Locks and tamper seals are subject to picking and removal.	Hardware devices	Hardware devices are designed to allow jurisdictions to apply additional physical security devices.	Modified in Verity Voting 3.0.1. See Section 8 below, Regression Testing Version 3.0.1.

Table 2: Unrestricted access to workstation cases

Category	Component	Vendor Comments	Vendor Mitigation
Unrestricted access to workstation cases.	EMS	Workstations are designed to allow jurisdictions to apply additional physical security devices.	Modified in Verity Voting 3.0.1. See Section 8 below, Regression Testing Version 3.0.1.

Table 3: Lack of full disk encryption

Category	Component	Vendor Comments	Vendor Mitigation
Lack of full disk encryption.	EMS and hardware devices	Physical security and chain of custody for all elements of the voting system are of paramount importance in maintaining the integrity of election systems.	Modified in Verity Voting 3.0.1. See Section 8 below, Regression Testing Version 3.0.1.

Table 4: Server spoofing credential disclosure

Category	Component	Vendor Comments	Vendor Mitigation
Server spoofing credential disclosure.	EMS	An additional "man in middle" computer must be installed in the system network to exploit this vulnerability.	Modified in Verity Voting 3.0.1. See Section 8 below, Regression Testing Version 3.0.1.

Table 5: Shared/static secrets

Category	Component	Vendor Comments	Vendor Mitigation
Shared/static secrets.	EMS and hardware devices	They are stored in encrypted form in the file system.	Modified in Verity Voting 3.0.1. See Section 8 below, Regression Testing Version 3.0.1.

Table 6: Unnecessary applications available on system

Category	Component	Vendor Comments	Vendor Mitigation
Unnecessary applications available on system.	EMS	Vendor agrees with and follows the best practice to not install applications that are unnecessary.	Modified in Verity Voting 3.0.1. See Section 8 below, Regression Testing Version 3.0.1.

Table 7: Weak authentication encryption for Verity Key allowing unauthorized modification of election results

Category	Component	Vendor Comments	Vendor Mitigation
Weak authentication encryption.	EMS and hardware devices	Risk is mitigated because an attacker would need to access multiple assets.	Modified in Verity Voting 3.0.1. See Section 8 below, Regression Testing Version 3.0.1.

Table 8: Code execution via untrusted deserialization

Category	Component	Vendor Comments	Vendor Mitigation
Code execution via untrusted deserialization.		For a successful exploit, an attacker would have to run software on the platform to execute	Modified in Verity Voting 3.0.1. See Section 8 below, Regression Testing Version 3.0.1.

		code.	

7. Software Review

FCMG conducted the Software Review between May, 2018, and July, 2018. FCMG discovered nine public search vulnerabilities and ten system specific vulnerabilities:

Table 9: Public Search Vulnerabilities

Name (Vulnerable component)	Description	Vendor Mitigation
CVE-2016-2243 (HP Z240 Workstation)	Local users can cause the system to fail to recover the BIOS.	This vulnerability does not apply to any new HP Z240 that vendor will deploy. Per the HP website, the vulnerability was addressed in BIOS v. 01.11, and all new workstations are shipped with BIOS v. 01.71A as of 06/27/18.
Meltdown/Spectre (HP Z240 Workstation)	The computer system is susceptible to the Meltdown/Spectre malware.	This vulnerability does not apply to any new HP Z240 that vendor will deploy. The HP website indicates that this vulnerability was addressed in Z240 BIOS version 01.67, and all workstations are shipped with BIOS v. 01.71A as of 06/27/18.
Outdated version (SQLServer 2012)	The software version being used (11.0.2100) is out dated. There have been numerous Service Packs and Security updates since this release.	No specific security issue is reported. A SQL Server upgrade to 2014 or 2016 will be addressed in future product development.
SP1 installation failure (Windows Embedded System 7)	Certain updates related to SP1 may fail when updating the OS. Some updates that could fail are: • KB2949927: Availability of SHA-2 Hashing Algorithm for Windows 7 and Windows Server 2008 R2 • KB3033929: Security Update for Windows 7 for x64-based Systems • KB3110329: Security Update for Windows 7	No specific security issue is reported. The operating system is a WES7 COTS build. This build is documented and was witnessed during the 3.0 trusted build. This WES7 build toolchain does not install service packs in the way an end user would install them. Instead, updates are individually selectable. Hart selects and installs updates that apply to the voting system. Hart has confirmed that the selected updates from the list of those that might fail during SP1 update have been successfully installed.

Name (Vulnerable component)	Description	Vendor Mitigation
Meltdown (Windows Embedded System 7)	The operating system used is susceptible to the Meltdown malware.	The threats identified affect specific CPUs, and vendor's voting system devices do not use a vulnerable CPU. An exhaustive list of vulnerable Intel CPUs is available here: https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00088&languageid=en-fr. Furthermore, this vulnerability does not apply to any new HP Z240 that vendor will deploy. The HP website indicates that this vulnerability was addressed in Z240 BIOS version 01.67, and all workstations are shipped with BIOS v. 01.71A as of 06/27/18.
Bugs (NHiberate)	The reviewer was unable to determine the version of NHibernate the system is using. The link provided will list bugs found in all versions of the software.	Consultant offers a reference to the bug list as an advisory only. No specific vulnerability issue is reported. Hart has extensive quality procedures to ensure that issues are identified and addressed.
Bugs (Fluent NHibernate)	The reviewer was unable to determine the version of Fluent NHibernate the system is using. The link provided will list bugs found in all versions of the software.	Consultant offers a reference to the bug list as an advisory only. No specific vulnerability issue is reported. Hart has extensive quality procedures to ensure that issues are identified and addressed.
DLL Hijacking (InnoSetup/Inno Script Setup)	The software is susceptible to including a Trojan horse DLL that is located in an untrusted path on the system.	Inno Script is not part of the voting system software and is not present in the delivered system. It is used to create installers during the trusted build and is present only in the support files. Furthermore, the support files were included in the consultant package at their request to assist in the review. They are not a security risk, as the support files are not included in the trusted build images.
Malformed Windows binary not protected (McAfee Application Control for Devices)	The reviewer noticed how the developer has whitelisted what files should run on the system. The following CVE is something to be aware of in the event a file is added that the program may think is non-executable.	To exploit this vulnerability, an attacker would need to make changes to the voting system which would render the voting device inoperable, due to the system's Secure Boot process. In addition, physical security controls and a kiosk environment reduce this risk on workstations. An upgrade to McAfee Application Control will be assessed in future product development.

Table 10: System Specific Vulnerabilities

Description	Assessment	Categorization	Vendor Mitigation
Usage of SHA-1 to sign data and sign hash.	The use of SHA-1 for signatures is not approved by NIST, some weaknesses have been found in SHA-1 and it is recommended to use the SHA-2 family.	**Type:** potential vulnerability and non-conformity (FIPS) **Severity:** Medium	Modified in Verity Voting 3.0.1. See Section 8 below, Regression Testing Version 3.0.1.
Microsoft SQL Server 2012 (MSSQL) is not patched.	Not having the latest version of the software leaves the system open to undiscovered and unpatched vulnerabilities. The version of MSSQL installed is 11.0.2100. There have been numerous Service Packs and Security updates since this release. In order to address any discovered (and potentially undiscovered) vulnerabilities, updating to the latest Service Pack is recommended (Service Pack 4).	**Type:** potential vulnerability **Severity:** Medium	No specific security issue is reported. A SQL Server upgrade to 2014 or 2016 will be assessed in future product development.
Ability to write directly to memory is a potential vulnerability.	The code has access to the system memory. Malicious code could be interjected and executed. Secure software lifecycle processes need to be implemented and followed to ensure no unwanted code is added.	**Type:** potential vulnerability **Severity:** Low	The code being referenced is only applicable to voting devices, which are protected by a Secure Boot process that renders the device inoperable prior to this attack being attempted. The code being referenced is used to disable the hardware watchdog on the voting device after a successful boot. The feature in question is non-mutable as it is protected by the device Secure Boot and Whitelisting capabilities which ensure that only known, trusted code is resident and executable on the device.
Password complexity does not follow best practices.	The algorithm used to determine if a user's password is strong enough is not using best practices. The algorithm does not enforce the use of lower case lettering, and the minimum length acceptable is too small.	**Type:** potential vulnerability **Severity:** Medium	Modified in Verity Voting 3.0.1. See Section 8 below, Regression Testing Version 3.0.1.
Password information is not being stored using an appropriate/suitable	The password field is being stored as a String in classes. Since this is sensitive	**Type:** potential vulnerability **Severity:**	Modified in Verity Voting 3.0.1. See Section 8 below, Regression Testing Version 3.0.1.

Description	Assessment	Categorization	Vendor Mitigation
class.	information, a different class more suitable to this type of information should be used, such as the SecureString class. The password should be stored using a class, such as the SecureString object, that supports sensitive data processing.	Medium	
Usage of authorization check for a plugin.	There is use of AuthorizationException in the modules. A catch of the exception was detected but it did not handle the exception. There are checks to see if "Manage Users" permission exists, but could not find where the permission was set.	**Type:** vulnerability **Severity:** Medium	Modified in Verity Voting 3.0.1. See Section 8 below, Regression Testing Version 3.0.1.
The SQL query strings are being constructed in a way that does not follow best practices.	SQL statements are being constructed using '+' or append method on a class. Best practice is to use parameterized queries for constructing SQL statements.	**Type:** vulnerability **Severity:** Medium	Modified in Verity Voting 3.0.1. See Section 8 below, Regression Testing Version 3.0.1.
The configuration files don't appear to be protected from alteration.	Unable to determine security policy regarding configuration file access and modification. It is considered good practice to limit/restrict access to the configuration files used by the application.	**Type:** potential vulnerability **Severity:** Low	Modified in Verity Voting 3.0.1. See Section 8 below, Regression Testing Version 3.0.1.
Exception handling implementation is not consistent and doesn't follow best practices.	There are instances where exception/error handling doesn't follow a consistent implementation. Additionally, these instances do not follow best practices described by Microsoft or all the guidelines described in the Verity Logging Technical Requirements Document (section 5.3: Events that must be logged).	**Type:** potential vulnerability **Severity:** Low	Consultant described its observations as only a "potential vulnerability," and vendor believes the risk is low because the consequence is non-standard error reporting in rare cases.
Product is no longer FIPS 140-2 certified or compliant.	Product documentation states all cryptographic modules used are FIPS 140-2 validated. This was true at one time but is not true today.	**Type:** non-conformity, potential vulnerability **Severity:** Medium	Modified in Verity Voting 3.0.1. See Section 8 below, Regression Testing Version 3.0.1.

8. Regression Testing, version 3.0.1

The potential vulnerabilities discovered during Security and Telecommunications Testing and Software Testing of the Hart InterCivic Verity Voting 3.0 voting system required mitigating changes to the voting system. Hart's changes were sufficient to require a new version number. The new version is Verity Voting version 3.0.1. Regression Testing was performed to verify the effectiveness of the changes and ensure that the changes did not degrade the system's functionality, efficiency, or accuracy.

Functional Regression Testing and Security and Telecommunications Regression Testing of the Verity Voting 3.0.1 system were completed in Austin, Texas at the Hart InterCivic facility from August, 13, 2018, until August 30, 2018, by California Secretary of State and FCMG Staff. Hart Staff provided technical support and witnessed the testing. Source Code Review Regression Testing was completed by FCMG/atsec Information Security Corporation during this same time period.

A new trusted build was compiled from source code, followed by Functional Regression Testing, Security and Telecommunications Regression Testing, and finally an additional Source Code Review.

Functional:

Regression Testing was performed using the same mock elections as the original Functional Tests. The elections staged during the Functional Regression Test were:

- A Primary election based on a Sacramento County election that included both precinct voting and a countywide vote center;
- A General election based on a Contra Costa County election;
- A Recall election; and
- A Ranked Choice (RCV) election.

The system performed as described in the documentation with no tabulation or reporting errors. Despite the modifications to the system and subsequent change to the version number, when it was compared to the results recorded by the SOS in the initial functional test, FCMG found no evidence that the system performance was degraded.

Security and Telecommunications:

Regression Testing started with FCMG reviewing the updated Technical Data Package and Change Log provided by Hart with respect to updates made in response to earlier security findings.

For each of the previous findings it was determined whether the finding had been addressed, how it had been addressed and if the stated update met the requirements proscribed by the California Voting System Standards.

The system was retested, both physically and logically, to verify that the updates had been applied and to confirm that the function and improvements performed as documented.

The following table summarizes the original findings, Hart's mitigations and FCMG's supplemental findings:

Table 11: Regression Testing – Security & Telecommunications

Original Finding Description	Mitigation/Fix Reported by Hart	Supplemental Findings
Locks and tamper seals are subject to picking and removal.	Physical security has been revamped to include new, more effective, locks and seals.	Workstation cases have been modified and new, more effective, locks and tamper evident labels applied. The Verity devices and ballot boxes have new seals.
Unrestricted access to workstation cases.	Physical security applied to workstation cases.	Verified and effective.
Lack of full disk encryption.	BitLocker added to workstation O/S image. BitLocker whole disk encryption mode (AES-128) enabled.	Verified on Client/Server and Freestanding Workstations. Not implemented on Verity Print, Scan, Reader and Touch Writer devices.
Server spoofing credential disclosure.	Firewall configuration settings updated.	Verified.
Shared static secrets	Procedural	Recommend procedures to ensure that the Verity Keys are not lost and a plan in place for the event that a Verity Key or Device is stolen.
Unnecessary applications available on system.	The applications have been removed.	Verified.
Weak authentication encryption.	The device password for Verity Key is now required to be 8-10 alphanumeric characters.	Verified.
Code execution via untrusted deserialization.	Verity Key security has been increased by updating how the data on the Verity Key is written and read.	Verified.

Software Testing:

Table 12 summarizes the findings that arose from atsec Security Corporation's assessment of the updated TDP including code and documentation.

Table 12: Regression Testing – Software

Original Finding Description	Fix Reported by Developer	Regression Test Findings
Password information is not being stored using an appropriate/suitable class.	Use SecureString instead of String.	The modules listed in the work paper were indeed corrected to use SecureString for the password.
Usage of SHA-1 to sign data and sign hash.	Use SHA-256 for the sign-hash and sign-data functions.	The functions mentioned in the work paper were indeed fixed to use SHA-256 instead of SHA-1.
Usage of authorization check for a plugin.	Remove the file with no-op function since it was deprecated and no longer used.	The module had indeed been removed.
The SQL query strings are being constructed in a way that does not follow best practices.	Change the code to parameterize the query parameters.	The code addressed in the finding had been corrected to parameterize the parameters to the query function.
The configuration files don't appear to be protected from alteration.	Update TDP with the appropriate information.	The Technical Data Package was updated with information on using file encryption software to help increase configuration file security by encrypting the drive (which is where the configuration files are located). Using a Trusted Platform Module (TPM) only authentication model, only the person or people with the right credentials (passwords or USB fobs) can unencrypt the drive at boot time.
Microsoft SQL Server 2012 (MSSQL) is not patched.	atsec reviewed Verity_SQL Server 2012 Security Updates Risk Analysis dated July 20th, 2018, provided by the vendor summarizing the known open vulnerabilities in SQL Server and assessing the risk of each to the product. atsec performed a similar vulnerability search and confirmed the vendor's open vulnerability findings.	atsec agrees with the vendor's assessment that because all the currently known vulnerabilities require either remote authenticated user access or cross-site scripting in a browser to be exploitable, a product deployed in the field and configured properly will not be susceptible to any of these known open vulnerabilities. atsec agrees that having not patched SQL Server currently results in no additional vulnerability to the product.
Product is no longer FIPS 140-2 certified or compliant.	None	The third-party cryptographic module used by the product has

Original Finding Description	Fix Reported by Developer	Regression Test Findings
		an expired FIPS 140-2 certificate. Unless the provider of the cryptographic module performs such a certification the only resolution is to use another cryptographic module, that is FIPS 140-2 certified as a COTS component in this product. Note that FIPS 140-2 conformance is not the same as the pre-requisite CAVS certificates for the security functions used by the module, but includes conformance with many other requirements such as interfaces, self-tests, design assurance, and key management.

Regarding the FIPS 140-2 finding above: Hart respectfully disagrees with this finding. The FIPS 140-2 program does not include the concept of expiration. NIST can move a FIPS 140-2 certificate to the "historical list" or they can revoke the certificate.

If NIST is aware of a security issue or flaw with a cryptographic method or module they revoke the corresponding certificate(s). The certificates for the approved modules listed in the TDP have not been revoked. The certificates for modules used have been moved to the historical list. NIST moves older certificates to the historical list regularly. This does not indicate a problem or deficit in the module, and does not indicate that a module is no longer certified or compliant. It simply indicates age.

On the FIPS Cryptographic Module Validation Program website, NIST explicitly states that a "historical" classification does not indicate revocation of the certificate: "…*This does not mean that the overall FIPS-140 certificates for these modules have been revoked, rather it indicates that the certificates and the documentation posted with them are more than 5 years old and have not been updated to reflect latest guidance and/or transitions and may not accurately reflect how the module can be used in FIPS mode."*

For these reasons, Hart's position remains that the system is FIPS 140-2 compliant.

IV. CONCLUSION

The Hart Verity Voting 3.0.1 voting system, in the configuration tested and documented by the Installation and Use Procedures, meets applicable California Voting System Standards and Elections Code requirements. Appendix A contains a detailed chart of the Elections Code sections that the Secretary of State tested the system against.

Appendix A: COMPLIANCE WITH CALIFORNIA ELECTIONS CODE

The following are the California Elections Code sections that the Secretary of State tested the Hart Verity Voting 3.0 voting system against. The list is broken down by Elections Code Section, language quoted from the section and how the system complies with the section.

10264 - As soon as the result of the election is declared, the elections official of the governing body shall enter on its records a statement of the result. The statement shall show: (a) The whole number of votes cast in the city. (b) The names of the persons voted for. (c) The measures voted upon. (d) For what office each person was voted for. (e) The number of votes given at each precinct to each person and for and against each measure. (f) The number of votes given in the city to each person and for and against each measure.

The voting system has the capability to produce the required report(s).

10550 - As soon as the result of the canvass by the county elections official is declared, the county elections official shall prepare and mail a statement of the result to the secretary of each district participating in the general district election. The statement shall be signed by the county elections official, authenticated by the seal of the county and shall show: (a) The number of ballots cast for elective offices of that district and, when directors of that district are elected by divisions, the number of ballots cast in each division. (b) The name of each candidate for an elective office of that district voted for and the office. (c) The number of votes cast in each precinct for each candidate. (d) When directors are elected by divisions, the number of votes cast in each division for each candidate for the office of director from that division. (e) The number of votes cast in the district for all other elective offices of that district.

The voting system has the capability to produce the required report(s).

14433 - If ballots are counted at precincts pursuant to Article 3 (commencing with Section 15340) or Article 5 (commencing with Section 15360) of Chapter 4 of Division 15, the precinct board immediately shall transmit, unsealed, to the elections official a statement showing the result of the votes cast at the polling place. The statement shall be open to public inspection.

The voting system has the capability to produce the required report(s).

15101(b) - Any jurisdiction having the necessary computer capability may start to process vote by mail ballots on the seventh business day prior to the election. Processing vote by mail ballots includes opening vote by mail ballot return envelopes, removing ballots, duplicating any damaged ballots, and preparing the ballots to be machine read, or machine reading them, but under no circumstances may a vote count be accessed or released until 8 p.m. on the day of the election. All other jurisdictions shall start to process vote by mail ballots at 5 p.m. on the day before the election.

The voting system has the capability to meet this requirement.

15101(c) - Results of any vote by mail ballot tabulation or count shall not be released prior to the close of the polls on the day of the election.

The voting system has the capability to scan, but not tabulate or report the results prior to the close of polls on Election Day.

15109 - Except as otherwise provided in this chapter, the counting and canvassing of vote by mail ballots shall be conducted in the same manner and under the same regulations as used for ballots cast in a precinct polling place.

The voting system has the capability to meet this requirement.

15110 - Reports to the Secretary of State of the findings of the canvass of vote by mail ballots shall be made by the elections official pursuant to Chapter 3 (commencing with Section 15150) and Chapter 4 (commencing with Section 15300).

The voting system has the capability to produce the required report(s).

15150 - For every election, the elections official shall conduct a semifinal official canvass by tabulating vote by mail and precinct ballots and compiling the results. The semifinal official canvass shall commence immediately upon the close of the polls and shall continue without adjournment until all precincts are accounted for.

The voting system has the capability to meet this requirement.

15151(a) - The elections official shall transmit the semifinal official results to the Secretary of State in the manner and according to the schedule prescribed by the Secretary of State prior to each election, for the following: (1) All candidates voted for statewide office. (2) All candidates voted for the following offices: (A) State Assembly. (B) State Senate. (C) Member of the United States House of Representatives. (D) Member of the State Board of Equalization. (E) Justice of the Court of Appeals. (3) All persons voted for at the presidential primary or for electors of President and Vice President of the United States. (4) Statewide ballot measures.

The voting system has the capability to produce the required report(s).

15152 - Neither the elections official, any member of a precinct board, nor any other person shall count any votes, either for a ballot proposition or candidate, until the close of the polls in that county. After that time, the ballots for all candidates and ballot propositions voted upon solely within the county shall be counted and the results of the balloting made public. However, the results for any candidate or ballot proposition also voted upon in another county or counties shall not be made public until after all the polls in that county and the other county or counties have closed. This paragraph applies regardless of whether the counting is done by manual tabulation or by a vote tabulating device.

The voting system has the capability to scan, but not tabulate or report the results prior to the close of polls on Election Day.

15153 - During the semifinal official canvass, write-in votes shall be counted in accordance with Article 3 (commencing with Section 15340) of Chapter 4.

The voting system has the capability to meet this requirement.

15212 - If voting at all precincts within a county is not conducted using the same voting system, the result as to the precincts not subject to this article shall be determined in accordance with other provisions of this code and the result of the vote at precincts subject to this article shall be determined as provided in this article. The statement of the vote in that case shall represent the consolidation of all the results and the results of the canvass of all vote by mail voter ballots.

The voting system has the capability to produce the required report(s).

15302(e), (f), (g), (h) - The official canvass shall include, but not be limited to, the following tasks: (e) Processing and counting any valid vote by mail and provisional ballots not included in the semifinal official canvass. (f) Counting any valid write-in votes. (g) Reproducing any damaged ballots, if necessary. (h) Reporting final results to the governing board and the Secretary of State, as required.

The voting system has the capability to produce the required report(s).

15342(a) - Any name written upon a ballot for a qualified write-in candidate, including a reasonable facsimile of the spelling of a name, shall be counted for the office, if it is written in the blank space provided and voted as specified below: (a) For voting systems in which write-in spaces appear directly below the list of candidates for that office and provide a voting space, no write-in vote shall be counted unless the voting space next to the writein space is marked or slotted as directed in the voting instructions, except as provided in subdivision (f). (d) Neither a vote cast for a candidate whose name appears on the ballot nor a vote cast for a write-in candidate shall be counted by a combination of marking and writing, a choice of more names than there are candidates to be nominated or elected to the office. (e) All valid write-in votes shall be tabulated and certified to the elections official on forms provided for this purpose, and the write-in votes shall be added to the results of the count of the ballots at the counting place and be included in the official returns for the precinct.

The voting system has the capability to meet this requirement.

15372(a) - The elections official shall prepare a certified statement of the results of the election and submit it to the governing body within 28 days of the election or, in the case of school district, community college district, county board of education, or special district elections conducted on the first Tuesday after the first Monday in November of odd numbered years, no later than the last Monday before the last Friday of that month. (b) The elections official shall post the certified statement of the results of the election on his or her Internet Web site in a downloadable spreadsheet format that may include,

but is not limited to, a comma-separated values file or a tab-separated values file and that is compatible with a spreadsheet software application that is widely used at the time of the posting. The certified statement of the election results shall be posted and maintained on the elections official's Internet Web site for a period of at least 10 years following the election. This subdivision shall apply only to an elections official who uses a computer system that has the capability of producing the election results in a downloadable spreadsheet format without requiring modification of the computer system.

The voting system has the capability to produce the required report(s).

15374(a) - The statement of the result shall show all of the following: (1) The total number of ballots cast. (2) The number of votes cast at each precinct for each candidate and for and against each measure. (3) The total number of votes cast for each candidate and for and against each measure. (b) The statement of the result shall also show the number of votes cast in each city, Assembly district, congressional district, senatorial district, State Board of Equalization district, and supervisorial district located in whole or in part in the county, for each candidate for the offices of presidential elector and all statewide offices, depending on the offices to be filled, and on each statewide ballot proposition.

The voting system has the capability to produce the required report(s).

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

The voting system meets this requirement.

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

The voting system meets this requirement.

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

The voting system has the capability to meet this requirement.

19203 - The Secretary of State shall not certify or conditionally approve a voting system or a part of a voting system that uses paper ballots unless the paper used for the ballots is of sufficient quality that it maintains its integrity and readability throughout the retention period specified in Chapter 4 (commencing with Section 17300) of Division 17.

According to the documentation submitted with the voting system, the voting system has the capability to meet this requirement.

19204 - The Secretary of State shall not certify or conditionally approve any voting system that includes features that permit a voter to produce, and leave the polling place with, a copy or facsimile of the ballot cast by the voter at that polling place.

The voting system has the capability to meet this requirement.

19205 - A voting system shall comply with all of the following: (a) No part of the voting system shall be connected to the Internet at any time. (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. (c) No part of the voting system shall receive or transmit wireless communications or wireless data transfers.

The voting system has the capability to meet this requirement.

19240 - It is the intent of the Legislature that California voting system standards and elections comply with the provisions of the federal Help America Vote Act of 2002 (42 U.S.C. Sec. 15301 et seq.) that require voting systems be accessible 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, as provided to other voters who are not disabled.

The voting system has the capability to meet this requirement.

19242(b) - At each polling place, at least one voting unit certified or conditionally approved by the Secretary of State shall provide voters with disabilities the access required under the federal Help America Vote Act of 2002 (42 U.S.C. Sec. 15301 et seq.). The voting system has the capability to meet this requirement. 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 voting system has the capability to meet this requirement.

19301(a) - 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 or which they designated pursuant to Section 8002.5. (b) With respect to a party-nominated office, the designation may be by usual or reasonable abbreviation of party names. With respect to a voter-nominated office, the voting machine shall conform to the format specified in subdivision (a) of Section 13105.

The voting system has the capability to meet this requirement.

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 therefor (sic) 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 therefor (sic) 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 voting system has the capability to meet this requirement.

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 voting system has the capability to meet this requirement, including the generation of an electronic report that meets numbers (1) and (4).

Appendix B: VOTERS WITH SPECIFIC NEEDS SURVEY RESULTS

1. Survey Results

The Secretary of State conducted an exit survey with the voters who participated in the Accessibility Test regarding their voting experience utilizing the Verity Touch Writer and Verity Reader. The majority of participants found that the voting system would allow them to vote privately and independently; that the voting instructions were clear and complete; the display was easy to read; the speech output was understandable; the assistive machines were easy to reach and use; the system was not confusing to use; and that the time it took to vote was within their expected timeframe.

Question # 1: The voting method was private.

Nine out of ten participants agreed either somewhat or strongly that the voting method was private. One participant disagreed strongly. All agreed that with proper placement, and the privacy screen in place, their voting experience was private.

Question # 2: I feel I can use this system to vote independently.

100% of participants agreed either somewhat or strongly with this statement. Individuals with all types of disabilities agreed that the system allowed them to vote independently.

Question #3: I am confident that my vote was recorded accurately.

100% of participants agreed either somewhat or strongly with this statement, however, it is not possible for voters using the Scan component to verify their actual paper ballot after voting and casting their ballot because it has been dropped into the ballot box.

Question # 4: The voting instructions were clear and complete.

Nine out of ten participants agreed somewhat or strongly with this statement, while one participant disagreed somewhat with this statement.

Although most of the survey respondents either agreed strongly or agreed somewhat that the voting instructions were clear and complete, they were able to utilize the voting machines much better the second time they voted on the machine.

Question # 5: The voting method was easy to use.

Eight out of ten participants agreed somewhat or strongly that the voting method was easy to use, while two participants disagreed somewhat with this statement.

Although most of the survey respondents either agreed strongly or agreed somewhat that this voting method was easy to use, they were able to utilize the voting machines much better the second time they voted on the machine.

Question # 6: I could read the display easily.

Two participants with visual impairments rated this N/A. 100% of the other participants agreed with this statement.

Question # 7: I could understand the speech output.

Six out of ten participants responded Not Applicable to this statement because they preferred to use the screen. 40% of participants agreed with this statement. One felt the speech output was too slow, even after she adjusted it to the fastest setting.

Question # 8: The assistive machine(s) were easy to reach and use.

Nine out of ten participants agreed somewhat or strongly with this statement, while one participant disagreed somewhat with this statement. The participant who disagreed was able to utilize the machine much better after we placed the machine on a table. One participant had trouble voting using the ATI, until we put the ATI device on a surface provided by Hart for this reason, he was then able to vote without assistance.

Question # 9: I found the system was confusing to use.

Six out of ten participants disagreed either somewhat or strongly with this statement. One had no opinion, and three agreed either somewhat or strongly with this statement.

Although three participants either agreed strongly or agreed somewhat that the voting instructions were confusing to use, they were able to utilize the voting machines much better the second time they voted on the machine.

10: The timeframe it took to vote was what I expected.

Eight out of ten participants agreed somewhat or strongly that the timeframe it took to vote was what they expected, while two participants disagreed somewhat with this statement.