

SEQUOIA SYSTEM 4.0

SEQUOIA VOTING SYSTEMS

SYSTEM 4.0:

WinEDS Software version 4.0.116

WinEDS Extended Services Software version 1.0.47

WinEDS Election Reporting Software version 4.0.44

Optech Insight Plus, Hardware version A or Higher with:

Optech Insight Plus HPX Firmware version

K1.44.080501.1500 and

Optech Insight Plus APX Firmware version

K2.16.08.626.1320

Memory Pack Reader (MPR), Hardware version D,

Firmware version 3.01.080422.0522

400-C Central Count Scanner, Hardware version 3.00P with

WinETP (400-C) Software version 1.16.6

Staff Review and Analysis

Prepared by:

Secretary of State Office of

Voting Systems Technology Assessment

September 19, 2008

Table of Contents

I. SUMMARY OF THE APPLICATION	3
II. SUMMARY OF THE SYSTEM	3
III. TESTING INFORMATION AND RESULTS	5
IV. COMPLIANCE WITH STATE AND FEDERAL LAWS AND REGULATIONS.....	8
V. RECOMMENDATION	13

I. SUMMARY OF THE APPLICATION

Procedures, hardware, firmware and software developed by Sequoia Voting Systems for use with the System 4.0 voting system, comprised of the following components: WinEDS Software version 4.0.116; WinEDS Extended Services Software version 1.0.47; WinEDS Election Reporting Software version 4.0.44; Optech Insight Plus, Hardware version A or higher, with Optech Insight Plus HPX Firmware version K1.44.080501.1500 and Optech Insight Plus APX Firmware version K2.16.080626.1320; Memory Pack Reader (MPR), Hardware version D, Firmware version 3.01.080422.0522; 400-C Central Count scanner, Hardware version 3.00P, with WinETP (400-C) Software version 1.16.6.

II. SUMMARY OF THE SYSTEM

System 4.0 consists of six components.

1. WinEDS, v. 4.0.116

WinEDS is a Windows-based software application used for managing an election. It allows jurisdictions to define and configure an election, including districts, precincts, contests, parties, and candidates. Once an election is configured, WinEDS can be used to define and format the ballot layouts, including rotation, for all ballot styles. Once the election and ballots are defined, WinEDS is used for programming the memory cartridges for the 400-C, Insights, and Edge (where applicable). On Election Day, WinEDS is used for tallying and reporting election results from the Optech Insight Plus, Optech 400-C, and Edge (where applicable). In addition to Election Day results, WinEDS has the capability to perform Post-Election operations, such as resolving provisional ballots and write-in votes.

2. WinEDS Extended Services, v. 1.0.47

WinEDS Extended Services provides additional functions to the WinEDS application. The WinEDS Extended Services application provides the snap-in shell for a suite of common services and features including database access, security features, cryptography, caching, logging, and exception handling.

During the State of California testing, the Office of Voting Systems Technology Assessment (OVSTA) staff and consultants configured the system with two snap-in modules, Database Manager and Ranked Choice Voting.

The Database Manager module allows jurisdiction users to access database utilities from a server that does not maintain the SQL Server Management Studio installation. Omitting SQL Server Management Studio increases the security of the database. Database Manager enables the jurisdiction to perform several administrative tasks,

such as Profile and Election database backups, Profile and Election database restoration, and Profile database copying.

Ranked Choice Voting (RCV) is a ballot structure, for single-winner contests, used in several electoral systems in which voters rank a list of candidates in order of preference. The RCV module, within WinEDS Extended Services, creates an interface to manage the RCV process and deliver reporting capabilities.

3. WinEDS Election Reporting, v. 4.0.44

WinEDS Election Reporting is an independent application to manage reports and flat file exports that are not available directly through WinEDS. WinEDS Election Reporting allows jurisdictions to produce reports while running the election night tally. The application gives additional reporting capabilities, such as the ability to suppress incomplete precincts and segregate data.

4. Optech Insight Plus, with HPX v. K1.44.080501.1500 and APX v. K2.16.080626.1320

The Optech Insight Plus (Insight) is a Marksense, Precinct Count Voting System that uses Optical Scan Read-Head technology to cast and tabulate ballots at the Polling Place. To operate the Insight, the voter places a marked ballot into the device in any orientation. If a ballot is over-voted, the Insight will reject the ballot with an error message to the voter, allowing the voter the opportunity to correct the ballot. In addition to recording votes, tabulating ballots and over-vote protection, the Optech Insight Plus can print precinct level results, and store election results in the removable MemoryPack, after the closing of Polls.

There are two systems residing in and controlling the functions of the Optech Insight, the Hardware Program System (HPX) and the Application Program System (APX). The HPX and APX form a complete, self-contained, closed application. The HPX system performs a validity check on the hardware and verifies that a ballot is not present in the ballot path. The APX verifies the vote totals.

The Optech Insight is configured with a proprietary memory cartridge that has been programmed by WinEDS. During the election, vote results are saved to the memory cartridge as ballots are scanned. After the election, this memory cartridge is used to upload the vote results into WinEDS for tabulation.

5. Memory Pack Reader (MPR), v. 3.01.080422.0522

The Memory Pack Reader is a desktop device that burns ballot definition data for a specific election onto, and transfers election results from Optech Insight Plus MemoryPacks into the WinEDS database.

The MemoryPacks are hardware components, which store data on the APX chip and can be configured as either Erasable Programmable Read-Only Memory (EPROM) or

Random Access Memory (RAM). All testing was conducted with the EPROM configuration.

6. 400-C Central Scanner, with WinETP v. 1.16.6

The 400-C is a high-speed, high-volume scanner typically used for tabulating vote-by-mail ballots. Up to 150 ballots can be stacked in the automatic feed hopper, and the 400-C reads ballots at the rate of about 400 ballots per minute. A PC computer running Windows controls the 400-C. A diverter can be programmed to deflect certain ballots, such as ballots containing write-in votes, for separate handling.

The WinETP software/firmware, which controls the 400-C, is used in conjunction with the WinEDS application and database. The system is designed to count ballots in one of two modes: Precinct Header Mode (on a precinct-by-precinct basis) or Mixed Mode (without presorting of the ballots).

In an RCV Election, the 400-C is used to resolve write-ins. If a voter votes for a write-in candidate, in an RCV race, the Insight out-stacks that particular ballot and does not tabulate any of the votes on that ballot. During the canvass, the jurisdiction using the system tabulates the ballot containing the write-in with the 400-C and manually resolves the write-in candidate.

III. TESTING INFORMATION AND RESULTS

1. Voting Systems Testing Laboratory Testing

OVSTA staff has received a letter from iBeta Quality Assurance, dated August 4, 2008, stating that it has successfully completed the functional testing of the Sequoia Voting Systems WinEDS v.4.0 with WinETP and San Francisco Rank Choice Voting (RCV) as outlined in alternative implementation Section 2.3 of the *Sequoia Voting Systems Ranked Choice Voting Alternative Implementations for California* and the approved *City and County of San Francisco Ranked Choice Voting (RCV) Test Plan*.

Sequoia has not completed federal qualification testing of the Sequoia Voting Systems' System 4.0 to the Federal 2002 Voting System Standards. This system is currently in the Election Assistance Commission (EAC) Voting System Certification Program.

Under California Law, Elections Code section 19250 (a), the Secretary of State of California shall not approve a direct recording electronic (DRE) voting system unless the system has received federal qualification. The Sequoia System 4.0 does not include a DRE; therefore, federal qualification is not required prior to state approval. In addition, the Sequoia System 4.0 does not include an accessible device for voters with disabilities. If the Secretary of State approves the Sequoia System 4.0, a jurisdiction approved to use System 4.0 would need to request authorization to use a blended system that incorporates a previously approved accessible voting device under CA Elections Code section 19213.

2. State Testing by the Secretary of State and Consultant

Testing Overview

State examination and functional testing of this system was conducted by the Secretary of State's Office of Voting Systems Technology Assessment (OVSTA) staff in conjunction with the State's technical consultants, Mr. Paul Craft and Ms. Kathleen McGregor, at the Secretary of State's Office, 1500 11th Street, Sacramento, CA from August 18 through August 22, 2008.

General Testing Results

Testing of the Sequoia System 4.0 was completed successfully. During that testing, OVSTA staff and consultants built the entire voting system beginning with the installation of the operating system, commercial off the shelf (COTS) software, and trusted build of each software/firmware component of the voting system. After installation, the servers and workstation were hardened and secured to the Sequoia Use Procedure specifications. Prior to running the ballots, the last task performed in the system was the burning and configuring of the media for the Insight and 400-C. Sufficient ballots were processed for the standard state general test election contests to verify features of the system, as well as to test the system's capability to conduct elections in accordance with California law.

In addition to the standard state general test election, OVSTA and consultants tested the logic and capability to conduct an RCV election according to the specifications set forth in the San Francisco City Charter. OVSTA staff and consultants developed an RCV ballot with three contests, so that they could run three different test case scenarios in a single election. Twelve test cases, in four elections, were created to test the complexity of an RCV election.

During testing, the following issues were noted:

- On the first attempt to open WinEDS Extended Services, directly after closing out of WinEDS 4.0.116, an error occurred resulting in the following error message: "An unhandled exception was caught. The application may be in an unsafe state, so it will now close." OVSTA staff and consultants closed the WinEDS Extended Services application and reopened it trying to replicate the error message, but the attempt was unsuccessful. Later in the testing, the error message was duplicated while opening WinEDS Extended Services, directly after closing out of WinEDS Election Reporting.

Sequoia personnel explained that this error was a known issue that had been discovered in earlier testing and was due to COTS encryption software that they use for security purposes. When a user closes the database the COTS encryption software creates a security and encryption wrapper around the executable and supporting code of the Sequoia software applications; if the encryption software is not allowed enough time to secure executable and supporting code of the Sequoia applications, the error message appears. The vendor noted that this was a bug that they could not fix in their own software, but they were working with the manufacturer of the COTS application to have the issue addressed. The vendor

stated that they would be informing the California Secretary of State when a fix for the error is developed. In the meantime, Sequoia has addressed the issue on page Addendum-9 of their Use Procedures, by notifying the jurisdictions using this system to wait a few seconds between closing out of one application and opening up a second application.

- When configuring the system, OVSTA staff and consultants followed the procedures and created three folders, in the D drive located on the PC designated as the server. The three folders created were WINEDSBackup, WINEDSData, and WINEDSLogs. While working on the WinEDS workstation, OVSTA staff and consultants received an error message when trying to restore the Election Database from the WINEDSBackup folder in D:\ residing on the server.

After concluding the functional testing, Sequoia personnel proposed a one-time manual change to the user.config file so that the paths lead to D:\ instead of C:\. This workaround proved to be successful and instructions for this procedure are included on page Addendum-10 and Addendum-11 of the Use Procedures.

- An anomaly arose during Washington State certification testing on a previous build of this system. OVSTA staff had been told that Sequoia had fixed the software so that the anomaly could not be replicated in this build of WinEDS and the Insight. In order to prove that this anomaly had been addressed, OVSTA staff and consultants replicated the anomaly, on the previous firmware build of the Insight, and loaded the MemoryPack into the current WinEDS software build. In the attempt to do so, WinEDS detected that an error occurred and displayed the error message “Inconsistent Data Detected. Please recreate the memory pack.” The data would not load from the MemoryPack into WinEDS, proving that a fix had been made in the WinEDS software. Sequoia assured OVSTA staff and the consultants that the Insight firmware has also been fixed, but as functional testing cannot prove a negative, the changes to the code are also addressed in the Source Code Report.

Source Code Review

atsec information security corp. performed a source code review on Sequoia’s System 4.0 for the Secretary of State. atsec compared the source code for System 4.0 to the code that was tested in the Top-to-Bottom Review (WinEDS 3.1.012) to determine if the issues in the prior version have been resolved. System 4.0 has two new modules, WinEDS Extended Services and WinEDS Election Reporting that were not previously reviewed. atsec conducted a thorough review of the code for these two new modules. In addition, atsec was asked to verify that the issue discovered in Washington State’s testing, of an earlier version of the Sequoia RCV system, has been resolved in the version tested by California.

atsec found that many of the problems identified in the Top-to-Bottom Review report had not been corrected in System 4.0. The high-level security architectural issues previously reported remain issues in System 4.0. Out of the forty-seven specific security defects that

were identified in the Top-to-Bottom Review report, twenty have not been addressed by code modifications in the new version. . Twenty-seven defects have been addressed through code modifications. Of those twenty-seven, nine defects have been resolved sufficiently, two modifications have partially resolved the defects, and two modifications do not resolve the defect. The effectiveness of the code modifications for the remaining fourteen defects could not be determined solely by a source code review.

The review of the two new modules (WinEDS Extended Services and WinEDS Election Reporting) found that the modules are susceptible to SQL injection attacks and that they provide inadequate error handling. As implemented, the modules do not incorporate safeguards into the system itself, but instead rely on users to protect data integrity. atsec identified vulnerabilities that have the potential to leave the software applications in an insecure state. This could result in data corruption.

atsec compared the section of the source code responsible for the defect that was discovered in Washington State testing to the revised source code section for System 4.0 currently under review for California. They verified that the code modifications were successful in preventing the problem identified by Washington.

atsec found that System 4.0 has continued the improper use of cryptography. Several of the modules continue to use hardcoded encryption and hashing keys. The Secure Hash Algorithm (SHA) hash continues to be used in a method known to be insecure. The Cyclic Redundancy Check (CRC) checksum algorithm is not cryptographically secure, leaving an opening for attack.

The 400-C, which contains crucial election information, does not provide sufficient integrity protection. System 4.0 should not have any network connection, but atsec found that when the system is connected to a network and information is transmitted to a workstation or server the hashes are not computed. Portions of the software only use the CRC algorithm to integrity check election files.

IV. COMPLIANCE WITH STATE AND FEDERAL LAWS AND REGULATIONS

A review of the appropriate Elections Code sections was conducted.

§19300 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.

§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.

§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.

§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 these requirements.

§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.

§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.

§19370. As soon as the polls are closed, the precinct board, in the presence of the watchers and all others lawfully present, shall immediately lock the voting machine against voting and open the counting compartments, giving full view of all counter numbers. A board member shall in the order of the offices as their titles are arranged on the machine, read and distinctly announce the name or designating number and letter on each counter for each candidate’s name and the result as shown by the counter numbers. He or she shall also in the same manner announce the vote on each measure.

If the machine is provided with a recording device, in lieu of opening the counter compartment the precinct board shall proceed to operate the mechanism to produce the statement of return of votes cast record in a minimum of three copies, remove the irregular ballot, if any, record on the statement of return of votes cast record. The irregular ballot shall, be attached to the statement of result record of votes cast for the machine and become a part thereof. One copy of the statement of return of votes cast for each machine shall be posted upon the outside wall of the precinct for all to see. The statement of return of votes cast for each machine for the precinct shall constitute the precinct statement of result of votes cast.

The system supports this requirement.

§19380. During the reading of the result of votes cast, any candidate or watcher who may desire to be present shall be admitted to the polling place. The proclamation of the result of the votes cast shall be distinctly announced by the precinct board who shall read the name of each candidate, or the designating number and letter of his or her counter, and the vote registered on the counter. The board shall also read the vote cast for and against each measure submitted. The board shall not count votes cast for write-in candidates, but shall have these counted by the elections official. During the proclamation, many opportunities shall be given to any person lawfully present to compare the result so announced with the counter dials of the machine, and any necessary corrections shall immediately be made by the precinct board, after which the doors of the voting machine shall be closed and locked.

If the machine is provided with a recording device, the alternate procedures in Section 19370 may be used.

The system meets this requirement.

§19381. In each election district where voting machines are used, statements of the results of the vote cast shall be printed to conform with the type of voting machine used.

The designating number and letter on the counter for each candidate shall be printed next to the candidate's name on the statements of result of the vote cast. Two such statements shall be used in each election district.

The system meets this requirement.

§19382. The statement of the result of votes cast, which shall be certified by the precinct board, shall contain:

- (a) The total number of votes cast.**
- (b) The number of votes cast for each candidate and measure as shown on the counter.**
- (c) The number of votes for persons not nominated.**
- (d) Printed directions to the precinct board for their guidance before the polls are opened and when the polls are closed.**
- (e) A certificate, which shall be signed by the election officers before the polls are opened, showing:
 - (1) The delivery of the keys in a sealed envelope.**
 - (2) The number on the seal.**
 - (3) The number registered on the protective counter.**
 - (4) Whether all of the counters are set at zero (000).**
 - (5) Whether the public counter is set at zero (000).**
 - (6) Whether the ballot labels are properly placed in the machine.****

(f) A certificate that shall be filled out after the polls have been closed, showing:

- (1) That the machine has been locked against voting and sealed.**
- (2) The number of voters as shown on the public counter.**
- (3) The number on the seal.**
- (4) The number registered on the protective counter.**
- (5) That the voting machine is closed and locked.**

The system supports this requirement.

§19383. A member of the precinct board shall enter the vote, as registered, on the statements of result of votes cast, in the same order on the space that has the same name or designating number and letter, after which another member shall verify the figures by calling them off in the same manner from the counters of the machine.

The counter compartment of the voting machine shall remain open until the official returns and all other reports have been fully completed and verified by the precinct board.

If the machine is provided with a recording device, the alternate procedures in Section 19370 may be used.

The system supports this requirement.

§19384. The precinct board shall, before it adjourns, post conspicuously on the outside of the polling place a copy of the result of the votes cast at the polling place. The copy of the result shall be signed by the members of the precinct board.

If the machine is provided with a recording device, the statement of result of vote's cast produced by operating its mechanism may be considered the "result of the votes cast" at the polling place.

The system supports this requirement.

§19385. The precinct board shall immediately transmit unsealed to the elections official a copy of the result of the votes cast at the polling place, the copy shall be signed by the members of the precinct board, and shall be open to public inspection.

The system supports this requirement.

The Voting Rights Act 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 six VRA

languages (Spanish, Chinese, Japanese, Vietnamese, Korean and Tagalog) as prescribed under the law.

The system meets this requirement.

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

The system meets this requirement.

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 22 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 vote-by-mail ballots, all envelopes in which vote-by-mail ballots are returned for tabulation, all documents containing oaths of voters, all documents relating to challenges to voters or vote-by-mail 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.

V. RECOMMENDATION

Staff recommends certification of the System 4.0 voting system, comprised of the following components:

WinEDS Software version 4.0.116; WinEDS Extended Services Software version 1.0.47; WinEDS Election Reporting Software version 4.0.44; Optech Insight Plus, Hardware version A or higher, with Optech Insight Plus HPX Firmware version K1.44.080501.1500 and Optech Insight Plus APX Firmware version K2.16.080626.1320; Memory Pack Reader (MPR), Hardware version D, Firmware version 3.01.080422.0522; 400-C Central Count scanner, Hardware version 3.00P, with WinETP (400-C) Software version 1.16.6 with the following conditions:

1. Jurisdictions are prohibited from installing any software applications or utilities on any component of the voting system that have not been identified by the Vendor and approved by the Secretary of State.
2. Prior to sale or use of the system in California, the Vendor must provide to all jurisdictions approved to use the system the revised version of its Use Procedures, entitled "Optech Insight, AVC Edge 5.0, & Optech 400C California Procedures, including all appendices and addendums, which the Secretary of State hereby approves. The revised Use Procedures address issues identified in the functional, source code and accessibility testing reports from the state testing of the voting system. Compliance with the Use Procedures by the Vendor and jurisdictions is a condition of the approval of this voting system. Compliance with all requirements set forth in the Use Procedures is mandatory, whether or not a particular requirement is identified in this Approval document.
3. No substitution or modification of the voting system shall be made with respect to any component of the voting system, including the Use Procedures, until the Secretary of State has been notified in writing and has determined that the proposed change or modification does not impair the accuracy or efficiency of the voting systems sufficient to require a re-examination and approval.
4. Before any use in the November 4, 2008, General Election, jurisdictions must reformat all hard disk drives and reinstall the operating system, where applicable, before installing software and firmware on all election management system servers and workstations. Jurisdictions must install voting system application software using the currently approved version obtained directly from the federal testing laboratory or the Secretary of State.
5. The Vendor and jurisdictions must implement the specifications for the hardware and operating system platform for all applicable components of the voting system, as set forth on pages Addendum-1 through Addendum-3 of the Use Procedures. The Vendor and jurisdictions must comply with the requirements for "hardening" the configuration of that platform, as set forth in Appendix R, Addendum-5 and Addendum-6 of the Use Procedures, including, but not limited to:
 - BIOS configuration;
 - Essential services that are required and non-essential services that must be disabled;
 - Essential ports that are required and non-essential ports that must be disabled and, if feasible, removed or physically blocked;
 - Audit logging configuration;
 - Definition of user security roles and associated permissions to assure all users have only the minimum required permissions for their role;

- Password policies, including password strength, expiration, and maximum attempts, along with all related user account control settings; and
 - Specifications for the installation, configuration and use of all utilities and software applications necessary for operation of the voting system (e.g., security software, data compression utilities, Adobe Acrobat, etc.), as set forth on pages Addendum-2 and Addendum-3 of the Use Procedures under the heading “COTs Components.”
6. Immediately after any repair or modification of any voting system component that requires opening the housing, the integrity of the firmware and/or software must be verified using the automated mechanisms described above, or all software must be reinstalled by the jurisdiction from a read-only version of the approved firmware and/or software supplied directly by the federal testing laboratory or Secretary of State before the equipment can be put back into service.
 7. No network connections to any device not directly used and necessary for voting system functions may be established. Communication by or with any component of the voting system by wireless or modem transmission is prohibited at any time. No component of the voting system, or any device with network connectivity to the voting system, may be connected to the Internet, directly or indirectly, at any time.
 8. Upon request, members of the public must be permitted to observe and inspect, without physical contact, the integrity of all externally visible security seals used to secure voting equipment in a time and manner that does not interfere with the conduct of the election or the privacy of any voter.
 9. Where voting equipment is used to record and tabulate vote results in a polling place, upon close of the polls, the poll workers are required to print two copies of the accumulated vote results and one audit log from each device. Each poll worker must sign every copy. One copy of the vote results from each device must be publicly posted outside the polling place. The second copy, along with the audit log, must be included with the official election material that is returned to the jurisdiction headquarters on election night.
 10. No poll worker or other person may record the time at which or the order in which voters vote in a polling place.
 11. Poll workers are not permitted to participate in any post-election manual count auditing of precinct results from a precinct in which they were a poll worker.
 12. Each polling place must be equipped with a method or log to record all problems and issues with the voting equipment in the polling place as reported

by voters or observed by poll workers. Such records must include the following information for each event:

- Date and time of occurrence;
- Voter involved, if any;
- Equipment involved;
- Brief description of occurrence;
- Actions taken to resolve issue, if any; and
- Elections official(s) who observed and/or recorded the event.

13. All such event logs or reports must be made available to the public for inspection and review upon request. Prior to or concurrent with the certification of the election, the elections official must submit a report to the Secretary of State of all reported problems experienced with the voting system and identifying the actions taken, if any, to resolve the issues.
14. Training of poll workers must include each of the topics identified on pages N-18 through N-20 of the Use Procedures.
15. Elections officials must develop appropriate security procedures for use when representatives of qualified political parties and bona fide associations of citizens and media associations, pursuant to their rights under Elections Code section 15004.
16. All voters voting on paper ballots in a polling place must be provided a privacy sleeve for their ballot and instructed on its use in accordance with Elections Code section 14272.
17. A warning must be posted in each voting booth stating that, pursuant to Elections Code sections 18564, 18565, 18566, 18567, 18568 and 18569, tampering with voting equipment or altering vote results constitutes a felony, punishable by imprisonment.
18. With respect to any piece of voting equipment for which the chain of custody has been compromised or for which the integrity of the tamper-evident seals has been compromised, the following actions must be taken:
 - The chief elections official of the jurisdiction must be notified immediately;
 - The equipment must be removed from service immediately and replaced if possible;
 - Any votes cast on the device prior to its removal from service must be subject to a 100% manual tally, by the process described in Elections Code section 15360, as part of the official canvass. Notice to the public of this manual tally may be combined with the notice required by any other manual tally required in this order or by Elections Code section 15360;

- Any memory card containing data from that device must be secured and retained for the full election retention period;
 - An image of all device software and firmware must be stored on write-once media and retained securely for the full election retention period; and
 - All device software and firmware must be reinstalled from a read-only version of the approved firmware and software supplied directly by the federal testing laboratory or the Secretary of State before the equipment is placed back into service.
19. If a voting device experiences a fatal error from which it cannot recover gracefully (i.e., the error is not handled through the device's internal error handling procedures with or without user input), such that the device must be rebooted or the device reboots itself to restore operation, the following actions must be taken:
- The chief elections official of the jurisdiction must be notified immediately;
 - The equipment must be removed from service immediately and replaced as soon as possible;
 - Any votes cast on the device prior to its removal from service must be subject to a 100% manual tally, by the process described in Elections Code section 15360, over and above the normal manual tally conducted during the official canvass as defined in Elections Code section 336.5. Notice to the public of this manual tally may be combined with the notice required by any other manual tally required in this order or by Elections Code section 15360;
 - Any memory card containing data from that device must be secured and retained for the full election retention period;
 - An image of all device software and firmware must be stored on write-once media and retained securely for the full election retention period;
 - The Vendor or jurisdiction shall provide an analysis of the cause of the failure;
 - Upon request by the Secretary of State, the Vendor or jurisdiction shall retain the device for a reasonable period of time to permit forensic analysis; and
 - All device software and firmware must be reinstalled from a read-only version of the approved firmware and software supplied directly by the federal testing laboratory or the Secretary of State before the equipment is placed back into service.
20. The Secretary of State reserves the right, with reasonable notice to the Vendor and to the jurisdictions using the voting system, to modify the Use Procedures used with the voting system and to impose additional requirements with respect to the use of the system if the Secretary of State determines that such modifications or additions are necessary to enhance the accuracy, reliability or

security of any of the voting system. Such modifications or additions shall be deemed to be incorporated herein as if set forth in full.

21. Any jurisdiction using this voting system shall, prior to such use in each election, file with the California Secretary of State a copy of its Election Observer Panel Plan.
22. The Vendor agrees in writing to provide, and shall provide, to the Secretary of State, or to the Secretary of State's designee, within 30 days of the Secretary of State's demand for such, a working version of the voting system, including all hardware, firmware and software of the voting system, as well as the source code for any software or firmware contained in the voting system, including any commercial off the shelf software or firmware that is available and disclosable by the Vendor, provided that the Secretary of State first commits to the Vendor in writing to maintain the confidentiality of the contents of such voting system or source code so as to protect the proprietary interests of the Vendor in such voting system or source code. The terms of the commitment to maintain confidentiality shall be determined solely by the Secretary of State, after consultation with the Vendor. The voting system shall not be installed in any California jurisdiction until the Vendor has signed such an agreement. Any reasonable costs associated with the review of the source code for any software or firmware contained in the voting system shall be borne by the Vendor.
23. The Secretary of State reserves the right to monitor activities before, during and after the election at any precinct or registrar of voters' office, and may, at his or her discretion, test voting equipment.
24. Elections officials must develop appropriate security procedures for use when representatives of qualified political parties and bona fide associations of citizens and media associations, pursuant to their rights under Elections Code section 15004, check and review the preparation and operation of vote tabulating devices and attend any or all phases of the election. The security procedures must permit representatives to observe at a legible distance the contents of the display on the vote tabulating computer or device. This requirement may be satisfied by positioning an additional display monitor or monitors in a manner that allows the representatives to read the contents displayed on the vote tabulating computer or device while also observing the vote tabulating computer or device and any person or persons operating the vote tabulating computer or device
25. By order of the Secretary of State, voting systems approved for use in California shall comply with all applicable state and federal requirements, including, but not limited to, those voting system requirements as set forth in the California Elections Code and the Help America Vote Act of 2002 and

those requirements incorporated by reference in the Help America Vote Act of 2002. Further, voting systems shall also comply with all state and federal voting system guidelines, standards, regulations and requirements that derive authority from or are promulgated pursuant to and in furtherance of the California Elections Code and the Help America Vote Act of 2002 or other applicable state or federal law when appropriate.

26. Voting system manufacturers or their agents shall assume full responsibility for any representation they make that a voting system complies with all applicable state and federal requirements, including, but not limited to, those voting system requirements as set forth in the California Elections Code and the Help America Vote Act of 2002 and those requirements incorporated by reference in the Help America Vote Act of 2002. In the event such representation is determined to be false or misleading, voting system manufacturers or their agents shall be responsible for the cost of any upgrade, retrofit or replacement of any voting system or its component parts found to be necessary for certification or otherwise not in compliance.
27. Any voting system purchased with funds allocated by the Secretary of State's office shall meet all applicable state and federal standards, regulations and requirements, including, but not limited to, those voting system requirements as set forth in the California Elections Code and the Help America Vote Act of 2002 and those requirements incorporated by reference in the Help America Vote Act of 2002.
28. The Vendor must establish a California County User Group and hold at least one annual meeting where all California users and Secretary of State staff are invited to attend and review the system and ensure voter accessibility.
29. In addition to depositing the source code in an approved escrow facility, the Vendor must deposit with the Secretary of State a copy of the system source code, binary executables and tools and documentation, to allow the complete and successful compilation and installation of a system in its production/operational environment with confirmation by a verification test by qualified personnel using only this content. The Secretary of State reserves the right to perform a full independent review of the source code at any time.
30. The Vendor must provide printing specifications for paper ballots to the Secretary of State. The Secretary of State will certify printers to print ballots for this system based upon their demonstrated ability to do so. The Vendor may not require exclusivity in ballot printing and must cooperate fully in certification testing of ballots produced by other ballot printers.