State of California

SECRETARY OF STATE

APPROVAL OF USE OF *SEQUOIA VOTING SYSTEMS'* SYSTEM 4.0 VOTING SYSTEM

I, DEBRA BOWEN, Secretary of State of the State of California, do hereby certify that:

I. Sequoia Voting Systems, Inc. of Denver, Colorado ("Vendor"), has requested approval for use in California elections of its SYSTEM 4.0 voting system comprised of 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 submitted on or about July 9, 2008.

II. The request for approval of the voting system as described in Paragraph 1, was considered at a public hearing held September 26, 2008, in Sacramento, California.

III. STATE FUNCTIONAL TESTING RESULTS

1. I, as Secretary of State, tasked Freeman, Craft, McGregor Group (FCMG) to perform functional testing of the voting system, including the system's ability to accurately record, tabulate and report votes in Ranked Choice Voting elections. FCMG did not perform accessibility or Red Team penetration testing because System 4.0 used the same hardware as the WinEDS 3.1.012 voting system (System 3.1.012), which had undergone accessibility and Red Team testing as part of the Top-To-Bottom Review (TTBR) in 2007. The reports of results of the accessibility and Red Team testing of System 3.0.012 apply equally to System 4.0.

2. FCMG found that System 4.0 passed all state functional test requirements, including tests of the system's capacity to accurately record, tabulate and report votes in Ranked Choice Voting elections, using the Ranked Choice Voting rules in the Charter of the City and County of San Francisco.

IV. STATE SOURCE CODE TESTING RESULTS

1. I, as Secretary of State, tasked atsec information security corporation (Source Code Reviewers), working under contract to FCMG, to conduct an analysis of the source code of the Sequoia 4.0 Voting System, with the goal of assessing the security and integrity of the system, and in particular, of identifying any security vulnerabilities that could be exploited to alter vote recording, vote results, or critical election data such as audit logs, or to conduct a "denial of service" attack on the voting system.

2. The Source Code Reviewers assessed whether the System 4.0 source code resolves high-level security architecture issues and specific security defects of the Sequoia System 3.1.012 voting system identified in the TTBR reports on the testing of that system.

3. The Source Code Reviewers found that the previously reported security architecture issues remain issues in version 4.0. Specific architectural issues are identified in paragraphs 4-9 below.

4. The Source Code Reviewers found no effective mechanism to protect the integrity of data that is transferred between components of the system via removable media.

5. The Source Code Reviewers found a potential vulnerability for SQL injection attacks that would allow unauthorized access to election data stored in the database or execution of malicious code on the database server machine to crash the system.

6. The Source Code Reviewers found that a user can exploit a system weakness to gain access to the database without going through the WinEDS user interface, and then add, delete and modify any data in the database.

7. The Source Code Reviewers found that cryptographic methods are improperly used.

8. The Source Code Reviewers found that access control management in System 4.0 is still cumbersome, subject to user error and also can be circumvented.

9. The Source Code Reviewers found that while password management has been improved in System 4.0, because of an architecture defect, the strengthening of password management does not necessarily lead to a strengthened access control system.

10. The Source Code Reviewers also found that most of the specific security defects identified in the TTBR reports on the Sequoia System 3.1.012 voting system are also present in System 4.0. Specific security defects are identified in paragraphs 11-13 below.

11. The Source Code Reviewers verified that 9 of the 47 defects that were previously reported in the TTBR have been sufficiently resolved in the System 4.0 source code to mitigate the identified vulnerability. Code modifications for two defects partially resolve the reported issues. Code modifications for two defects do not sufficiently mitigate the

reported vulnerabilities they are intended to resolve. Resolution of 10 issues could not be determined by static review of the source code. Based on the code review, the reviewers found that approximately 24 of the 47 issues identified in the TTBR in the Sequoia System 3.1.012 voting system have not been addressed by code modifications in System 4.0.

12. The Source Code Reviewers found that a new mechanism was included in the build of System 4.0 submitted for California approval. The new mechanism verifies successful completion of the initialize or zero operation on the Optech Insight Plus precinct optical scanner and should prevent occurrence of an error that had been detected in a test of a previous build by the State of Washington.

13. The Source Code Reviewers found that System 4.0 does not properly protect the integrity of ballot data or ballot images stored in the 400-C Central Count Scanner and Optech Insight Plus precinct scanner. Except for a simple cyclic redundancy check (CRC), there is no security on the data in the MemoryPack. As a result, program code or data could be easily manipulated by an attacker.

14. The Source Code Reviewers conducted a thorough review of the two new modules (WinEDS Extended Services and WinEDS Election Reporting) included in System 4.0. They found the modules are susceptible to SQL injection attacks via unauthorized access to election data stored in the database or execution of malicious code on the database server machine to crash the system; rely on user action to ensure data integrity rather than implementing a system safeguard; and provide inadequate error handling. Exploitation of any of these weaknesses could result in data corruption and/or incomplete or false results.

15. Overall, the Source Code Reviewers concluded that, while progress has been made, System 4.0 remains vulnerable to multiple attack scenarios. Those attack scenarios center around interception and modification of data that the system has no reliable ways to detect.

V. APPROVAL

Sequoia Voting Systems, Inc.'s System 4.0 voting system as described in Paragraph 1, is hereby approved for use, on a one-time basis for the November 4, 2008, General Election in the City and County of San Francisco, subject to a request by, and administrative approval for, use of System 4.0 by the City and County of San Francisco in a blended system incorporating the Sequoia AVC Edge Model II, firmware version 5.0.24, with VeriVote Printer, primarily for accessible voting for voters with disabilities, and also subject to the following terms and conditions:

1. The jurisdiction is 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 the jurisdiction 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, a public document, 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 jurisdiction 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, the jurisdiction 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. The jurisdiction 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 jurisdiction 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 jurisdiction 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. Elections officials must comply with additional post election manual count auditing requirements set forth in emergency regulations promulgated by the Secretary of State and any successor emergency or permanent regulations. Any post election auditing requirements imposed as a condition of this certification shall be paid for by the Vendor. Elections officials are required to conduct the audits and the Vendor is required to reimburse the jurisdiction.

13. 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.

14. 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. The report shall disclose all reported problems experienced with the voting system and identify the actions taken, if any, to resolve the issues.

15. Training of poll workers must include each of the topics identified on pages N-18 through N-20 of the Use Procedures.

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 jurisdiction 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 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.

IN WITNESS WHEREOF, I hereunto set my hand and affix the Great Seal of the State of California, this 14th day of October, 2008.

Debra Bowen

DEBRA BOWEN
Secretary of State