State of California

SECRETARY OF STATE

CONDITIONAL APPROVAL OF ELECTION SYSTEMS AND SOFTWARE INKAVOTE PLUS PRECINCT BALLOT COUNTER VOTING SYSTEM, VERSION 2.1

Whereas, pursuant to Elections Code section 19201, no voting system, in whole or in part, may be used unless it has received the approval of the Secretary of State; and

Whereas, Elections Code section 19222 requires that I, as Secretary of State for the State of California, conduct periodic reviews of voting systems to determine if they are defective, obsolete, or otherwise unacceptable; and

Whereas, at my inauguration as Secretary of State on January 8, 2007, I announced my intention to conduct a top-to-bottom review of voting systems approved for use in California; and

Whereas, on March 22, 2007, I circulated for public comment draft criteria for a review of voting systems approved for use in California, covering system security issues, access for voters with disabilities, access for minority language voters, and usability for elections officials and poll workers; and

Whereas, on March 26, 2007, pursuant to my statutory obligations and to the conditions set forth in the approval, dated April 21, 2006, for use of the InkaVote Plus Precinct Ballot Counter Voting System (Comprised of the Inkavote Plus Precinct Ballot Counter with Audio Ballot Unit, Firmware Version 1.10 and the Unisyn Election Management System, Version 1.1, which includes Ballot Generation, Version 1.1, Election Converter, Version 1.1, Election Loader, Version 1.1, Vote Converter, Version 1.1, and Vote Tabulation, Version 1.1), I gave Election Systems and Software, Inc. ("ES&S"), written notice that it must provide within thirty days a working version of the voting system, including the source code for any software or firmware contained in the voting system and payment for the reasonable costs associated with the review of the source code; and

Whereas, on May 7, 2007, I gave ES&S written notice that all of the items previously requested must be delivered no later than May 11, 2007, followed by further written and oral demands on June 8, 2007, and June 15, 2007; and

Whereas, the review of voting systems approved for use in California commenced on May 31, 2007, with a scheduled completion date of July 20, 2007, pursuant to a contract with the Regents of the University of California and conducted by experts selected and supervised by principal investigators from the computer science faculties of the Berkeley and Davis campuses, to determine if the voting systems are defective, obsolete, or otherwise unacceptable for use in the February 5, 2008, Presidential Primary Election and subsequent elections in California; and

Whereas, ES&S did not agree until June 25, 2007, to participate in the review, and did not provide all of the items requested for the review until June 26, 2007, when insufficient time remained to test the InkaVote Plus Precinct Ballot Counter Voting System; and

Whereas, the study was completed with respect to the voting systems of Diebold Election Systems, Inc., Sequoia Voting Systems, Inc. and Hart InterCivic, Inc. on July 20, 2007, following which the expert reviewers delivered their written reports on their findings and methodology; and

Whereas, pursuant to Elections Code section 19222, I, as Secretary of State, am authorized to withdraw approval previously granted of any voting system or part of a voting system if I determine that voting system or any part of that voting system to be defective or otherwise unacceptable; and

Whereas, in an order dated August 3, 2007, I determined that, by preventing the Secretary of State from conducting a periodic review of the InkaVote Plus Precinct Ballot Counter Voting System, ES&S's failure to cooperate in the review rendered the voting system unacceptable pursuant to Elections Code section 19222, and for that reason withdrew approval for its use in the February 5, 2008, Presidential Primary Election and all subsequent elections in California; and

Whereas, in the same order dated August 3, 2007, I determined that ES&S had failed to comply with the conditions set forth in the approval of the ES&S InkaVote Plus Precinct Ballot Counter Voting System, dated April 21, 2006, and for that reason rescinded the approval with respect to the February 5, 2008, Presidential Primary Election and all subsequent elections; and

Whereas, when Election Systems and Software, Inc. finally submitted the InkaVote Plus Precinct Ballot Counter Voting System for the top-to-bottom review, it was no longer possible to conduct the review under the contract with the Regents of the University of California or to use experts selected and supervised by principal investigators from the computer science faculties of the Berkeley and Davis campuses; and

Whereas, I contracted with Freeman, Craft & McGregor Group ("FCMG") to select and supervise experts to perform the security review of the InkaVote Plus Precinct Ballot Counter Voting System; and

Whereas, FCMG subcontracted with atsec information security corporation to perform the source code review and red team security penetration test of the InkaVote Plus Precinct Ballot Counter Voting System; and

Whereas, I contracted with accessibility experts, Noel Runyan and Jim Tobias, to conduct a voting system accessibility review of the InkaVote Plus Precinct Ballot Counter Voting System; and

Whereas, the expert reviewers demonstrated that the physical and technological security mechanisms provided by the vendor for the InkaVote Plus Precinct Ballot Counter Voting System were inadequate to ensure accuracy and integrity of the election results and of the systems that provide those results; and

Whereas, the expert reviewers reported that the InkaVote Plus Precinct Ballot Counter Voting System contains serious design flaws that have led directly to specific vulnerabilities, which attackers could exploit to affect election outcomes; and

Whereas, the source code reviewers identified multiple vulnerabilities in the area of cryptography and key management, including inappropriate use of symmetric cryptography for authenticity checking, use of a very weak homebrewed cipher for the master key algorithm, and key generation with artificially low entropy which facilitates brute force attacks. In addition, the code and comments indicated that a hash (checksum) method that is suitable only for detecting accidental corruption is used inappropriately with the claimed intent of detecting malicious tampering; and

Whereas, the source code reviewers found and documented a vulnerability in the Unisyn Election Management System ("EMS") software to SQL injection attacks that could potentially be used to modify any of the information stored in the election results database, bypassing the sanity checks and logging that the code would normally do; and

Whereas, the source code reviewers found a potential vulnerability related to Zip File directory traversal that an attacker could use to create or overwrite files on the system in attacker-specified locations outside of the intended storage directory; and

Whereas, the source code reviewers found that the voting system's design depends on data provided at runtime, specifically the election definition file, providing avenues of attack that can affect the integrity of data, including the integrity of installed software components; and

Whereas, the source code reviewers found that the "least privilege" principle is not exercised in any of the voting system's applications, all of which run at a privilege level that provides full read/write access to all security critical application data, and that this lack of privilege separation in the design does not support reliable detection of security failures; and

Whereas, the source code reviewers found that design documents and code comments do not provide any evidence that audit logs are protected from tampering, while the code segments doing logging have sufficient privileges to modify or delete logs due to the lack of privilege separation; and

Whereas, the red team security penetration testers found that wire and tamper proof paper seals intended to protect the InkaVote Plus Precinct Ballot Counter Voting System were easily removed without damage to the seals using simple household chemicals and tools and could be replaced without detection. Once the seals are bypassed, simple tools or easy modifications to simple tools could be used to access the computer and its components. The key lock for the InkaVote Plus Precinct Ballot Counter Voting System's Transfer Device was unlocked using a common office item without the special 'key' and the seal removed, permitting undetected use of the USB port to attach a USB memory device which can be used to gain control of the system; and

Whereas, the red team was able to use the keyboard connector for the Audio Ballot unit to attach a standard keyboard, providing access to the operating system without reopening the computer; and

Whereas, the red team found files containing critical information in clear text or partially in clear text on the Election Distribution CD that is used to pass the election definition from the Election Converter application to the Election Loader, which in turn loads the election definition to the InkaVote Plus Precinct Ballot Counter Voting System. The red team used that information to decrypt the Election Distribution CD and demonstrated an attack in which it revised the election definition to disable the overvote protection feature of the InkaVote Plus Precinct Ballot Counter Voting System used by Los Angeles County and the City of Los Angeles; and

Whereas, the red team determined that the method used in its successful attack on the overvote protection feature of the InkaVote Plus Precinct Ballot Counter Voting System could also be used to alter vote tallies in the tally function of the Election Management System that is not used by Los Angeles County and the City of Los Angeles; and

Whereas, the accessibility experts determined that, for some test voters using the audio ballot feature of the InkaVote Plus Precinct Ballot Counter Voting System, the device printed a ballot that indicated an attempt to cast a write-in vote by printing the title of the office in the write-in area but did not print any candidate's name. This missing candidate name error occurred when a voter attempted a write-in entry in a fully voted contest without first de-selecting the candidate the voter had previously selected. The InkaVote program allowed the voter to go through the whole write-in process without warning the voter about the overvote condition. The resulting ballot

was marked for the previous candidate, although as far as the voter knew, the system had successfully accepted the write-in name and printed it on the ballot; and

Whereas, on November 26, 2007, a duly noticed public hearing was held to give interested persons an opportunity to express their views regarding the review of the ES&S InkaVote Plus Precinct Ballot Counter Voting System, Version 2.1. At this hearing, several individuals testified, and others submitted comments by letter, facsimile transmission, and electronic mail; and

Whereas, I have reviewed the ES&S InkaVote Plus Precinct Ballot Counter Voting System, Version 2.1, and I have reviewed and considered several reports regarding the use of this voting system; the public testimony presented at the duly noticed public hearing held on November 26, 2007; and the comments submitted by letter, facsimile transmission, and electronic mail; now

Therefore, I, Debra Bowen, Secretary of State for the State of California, find and determine, pursuant to Division 19 of the Elections Code, as follows:

1. Before any use in the February 5, 2008, Presidential primary election, jurisdictions must reinstall all software and firmware (including reformatting all hard disk drives and reinstalling the operating system where applicable) on all election management system servers and workstations, voting devices and hardware components of the voting system. Voting system application software must be reinstalled using the currently approved version obtained directly from the federal testing laboratory or the Secretary of State.

2. The InkaVote Plus Precinct Ballot Counter Voting System is approved for use only in the configuration deployed by Los Angeles County and by the City of Los Angeles, in which the Audio Ballot unit is used only to print ballot slips for voters selecting to use the Audio Ballot unit and the InkaVote Plus Precinct Ballot Counter ("PBC") device is used only to provide overvote and unvoted ballot notification but is not used to record, tally or report official vote counts.

3. Within 15 days the vendor must develop and submit to the Secretary of State for approval, a plan for post election procedures to prevent potential viral propagation of malicious software that could be introduced through an InkaVote Plus PBC device. The plan must include procedures for clearing all ballot definitions loaded by Election Loader before the InkaVote Plus PBC device can be connected to any other component of the voting system during that election or any subsequent election. The USB Transfer Device component of the voting system may not be used to transfer election data, via portable USB memory device or otherwise, from the InkaVote Plus PBC to any other component of the voting system or connected for any other reason to any other component of the voting system.

4. Within 15 days the vendor must submit to the Secretary of State for approval specifications for the hardware and operating system platform that must be used for all applicable components of the voting system. The vendor must identify the requirements for "hardening" the configuration of that platform, including, but not limited to:
   - BIOS configuration;
   - Identification of essential services that are required and non-essential services that must be disabled;
   - Identification of 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
   - All utilities and software applications, with specifications for their installation, configuration and use, that are necessary for operation of the voting system (e.g., security software, data compression utilities, Adobe Acrobat, etc.).

   The vendor must identify automated mechanisms for jurisdictions to confirm and document that their system has been configured to these standards, and that all updatable components are the approved version and level. The vendor must provide full instructions for the use of these mechanisms, including expected results.

5. 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. Removal of the printer attached to the InkaVote Plus PBC device and accessing transport media through the panel door on the side of the InkaVote Plus PBC device do not constitute opening the housing.

6. 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.

7. Within 15 days the vendor must develop and submit to the Secretary of State for approval, a plan and procedures for timely identification of required security updates (e.g., operating system security patches, security software updates, etc), vendor testing of the updates, and secure distribution and application of vendor-approved security updates.

8. Within 15 days the vendor, working with elections officials, must develop and submit to the Secretary of State for approval, requirements and Use Procedures for operating and maintaining the physical and logical security of the system, including, but not limited to:
   - Physical security and access to the system and all components;
   - Network security;
   - Data security (including data backup requirements and procedures); and
   - Separation of roles and responsibilities for jurisdiction personnel.

9. No network connection 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.

10. Within 15 days the vendor, working with elections officials, must develop and submit to the Secretary of State for approval, detailed requirements and Use Procedures for programming, pre and post-election logic and accuracy testing, transporting and operating voting equipment that will prevent or detect unauthorized access to or modification of any component of the voting system, including, but not limited to:
    - Chain of custody controls and signature-verified documentation;
    - Requirements for secure interim storage of any system component; and
    - Employment of mechanisms to detect unauthorized access to the equipment.

    At a minimum, the Use Procedures must describe all processes for securing and sealing voting system components before the jurisdiction transfers them to the custody of an Inspector, other poll worker, drayage company or other intermediary, or before jurisdiction personnel deliver them to a secure polling place or secure satellite distribution facility, as the case may be. Transportation of voting system components to the custody of an Inspector, other poll worker, drayage company or other intermediary, secure polling place, or secure satellite distribution facility shall not occur earlier than 10 calendar days prior to Election Day. Electronic components of a voting system not transported back to the jurisdiction headquarters on election night must be secured in one or more uniquely serialized, tamper-evident container(s) and placed in secured storage. The Use Procedures must impose requirements for signed logging of the inspection of security seals and locks on voting system components.

    The Use Procedures must also require a minimum of two elections officials or poll workers to perform or directly observe critical security processes, such as sealing and locking equipment for transport, conducting logic and accuracy testing, verifying the integrity and authenticity of security locks and seals, setting up voting equipment, opening the polls, closing the polls and printing results.

11. Where application of tamper-evident seals directly to a system component is required to detect unauthorized access to the component, those seals must be serialized and the vendor must specify in each instance the type of the seal to be used and the exact placement of that seal using photographs.

12. 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.

13. No poll worker or other person may record the time at which or the order in which voters vote in a polling place.

14. 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.

15. Within 15 days the vendor, working with elections officials, must develop and submit to the Secretary of State for approval, specific detailed requirements and Use Procedures for vote results auditing and reconciliation, review of audit logs and retention of election documentation to validate vote results and detect unauthorized manipulation of vote results, including, but not limited to:
    - Precinct level ballot accounting;
    - Identification of abnormal voting patterns on ballot slips printed by InkaVote Plus Audio Ballot units; and
    - Reconciliation of variances between electronic and manual audit vote results.

16. Each polling place must be equipped with a method or log in a format specified by the Secretary of State after consultation with elections officials 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.

17. 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.

18. Training of poll workers must include the following:
    - Secure storage of voting equipment while in the poll worker's possession;

- Chain-of-custody procedures required for voting equipment and polling place supplies;
- Seal placement and procedures for verification of seal integrity;
- Placement and observation of voting equipment;
- Observation of activity that could indicate tampering or an attempt at tampering;
- The Voter Bill of Rights set forth in section 2300 of the Elections Code;
- The nature of the InkaVote Plus Audio Ballot unit as a device that marks official paper ballots and, unlike a direct recording electronic (DRE) voting machine, does not create an electronic record of votes;
- Within 15 days, the vendor, working with election officials, must develop and submit to the Secretary of State for approval, a plan and procedures for instructing or assisting voters in voting for write-in candidates when using the InkaVote Plus Audio Ballot Booth. The plan and procedures shall focus on the issues identified in the InkaVote Plus Voting System Access Review that was conducted as part of the Secretary of State's top-to-bottom review of voting systems.
- The public right to inspect voting equipment and security seals, and how to handle requests for such inspection;
- How to handle lack of sufficient paper ballots or equipment failure in a polling place, including InkaVote Plus paper jams or other InkaVote Plus operational problems, and how to ensure continuity of the election in the event of such a failure; and
- How to properly log all events and issues related to voting equipment in the polling place, including voter complaints of malfunctioning equipment.

19. 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.

20. 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.

21. 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 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.

22. 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 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.

23. The Secretary of State will review and finalize all plans, requirements and procedures submitted pursuant to the foregoing requirements above within 15 days of receipt. Upon approval, all such plans, requirements and procedures will automatically be incorporated into the official Use Procedures for the voting system, and will become binding upon all users of the system and all subsequent elections conducted using the system.

24. 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 and efficiency of the voting system sufficient to require a re-examination and approval.

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

26. 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.

27. 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 born by the vendor.

28. 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, conduct a random parallel monitoring test of the voting equipment for purposes of confirming the functionality of the voting equipment as authorized by this recertification document.

29. By order of the Secretary of State, voting systems certified 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 California Elections Code and the Help America Vote Act of 2002 or other applicable state or federal law when appropriate.

30. 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.

31. 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.

32. 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.

33. 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.

34. 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.

35. Where circumstances require it, the Secretary of State may adjust or suspend any of the conditions of recertification for a vendor or a jurisdiction, as the Secretary of State deems prudent and necessary to facilitate successful election administration. Such adjustments or suspensions shall be deemed to be incorporated herein as if set forth in full.

IN WITNESS WHEREOF, I hereunto set my hand and affix the Great Seal of the State of California, this 2nd day of January, 2008.

DEBRA BOWEN
Secretary of State