WITHDRAWAL OF APPROVAL OF DIEBOLD ELECTION SYSTEMS, INC., GEMS 1.18.24/AccuVote-TSX/AccuVote-OS DRE & OPTICAL SCAN VOTING SYSTEM AND CONDITIONAL RE-APPROVAL OF USE OF DIEBOLD ELECTION SYSTEMS, INC., GEMS 1.18.24/AccuVote-TSX/AccuVote-OS DRE & OPTICAL SCAN VOTING SYSTEM

(October 25, 2007 Revision)

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, pursuant to my statutory obligations, I have undertaken such a review of voting systems approved for use in California, including the Diebold Election Systems, Inc., GEMS 1.18.24/AccuVote-TSX/AccuVote-OS voting system, 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, the study was completed on July 20, 2007, following which the expert reviewers delivered their written reports on their findings and methodology; and

Whereas, the expert reviewers found that the quality of the 2002 Voting System Standards (VSS) to which each of the three systems in their study were certified is inadequate, and noted further that questions have been raised about the effectiveness of the testing; for example, Ciber, Inc., a testing laboratory involved in testing of voting systems under the 2002 VSS, has been denied interim accreditation for testing voting systems by the Federal Election Assistance Commission after finding that Ciber "was not following its quality-control procedures and could not document that it was conducting all the required tests"; and

Whereas, the expert reviewers demonstrated that the physical and technological security mechanisms provided by the vendors for each of the voting systems analyzed 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 all of the voting systems studied contain serious design flaws that have led directly to specific vulnerabilities, which attackers could exploit to affect election outcomes; and

Whereas, the Diebold Source Code Review Team found that the Diebold software contains vulnerabilities that could allow an attacker to install malicious software on voting machines and on the election management system, which could cause votes to be recorded incorrectly or to be miscounted, possibly altering election results; and

Whereas, the Diebold Source Code Review Team found that the Diebold system is susceptible to computer viruses that propagate from voting machine to voting machine and even voting machines to the election management system, which could allow an attacker with access to only one voting unit or memory card to spread malicious code, between elections, to many, if not all, of a county's voting units; and

Whereas, the Diebold Source Code Review Team found that due to these shortcomings some threats would be difficult, if not impossible, to remedy with election procedures; and

Whereas, the Diebold Source Code Review Team found that both the electronic and paper records of the Diebold TSx direct recording electronic voting machine contain enough information to compromise the secrecy of the ballot; and

Whereas, the Diebold Red Team that conducted penetration testing on the Diebold voting system performed vulnerability scans of the Diebold voting system and discovered multiple vulnerabilities; and

Whereas, the Diebold Red Team members, with access only to the Windows operating system on the Diebold GEMS election management server supplied by Diebold and without requiring access to Diebold source code were able to access the Diebold voting system server software and to corrupt the election management system database, which could result in manipulated voter totals or the inability to read election results, rendering an election impossible to complete electronically; and

Whereas, without requiring access to Diebold source code, the Diebold Red Team members gained "root access" to the voting system that allowed manipulation of every setting on the networking devices and on the election management system server; and

Whereas, the Diebold Red Team members, without accessing Diebold source code, were able to violate the physical security of every aspect of the TSx direct recording electronic voting machine under polling place conditions using tools found in a typical office; and

Whereas, the Diebold Red Team members identified attacks on the TSx direct recording electronic voting machine that could allow a voter to delete all electronic records of ballots cast up to the time of the attack, including backup records; and

Whereas, the Diebold Red Team found a simple attack that can put the AVPM voter verifiable paper audit trail (VVPAT) printer out of service until the TSx unit is rebooted, using only tools that can be found in a typical office, in which voters who were not aware that they should expect a printed version of their ballot for review would not observe anything unusual, because the attack also causes the TSx to stop issuing reminders to voters that they should verify the printed record of their selections; and

Whereas, the Diebold Red Team members also found that the design of the AVPM VVPAT printer enabled attacks on the printed records of voter's ballots using a common household substance that could covertly destroy the VVPAT records, particularly notable because the attack (1) affects records printed before the attack is executed, (2) affects records printed after the attack is executed, (3) does not affect the way records are displayed to voters as they are produced – so as to avoid raising voter suspicion before the close of polls, (4) does not affect the printer mechanisms or jam the printer – again, to avoid raising suspicion, (5) the impact of these attacks is to make many of the VVPAT-printed records completely unreadable and most of them barely or only partially readable, destroying records already printed by the VVPAT at the time of the attack and potentially destroying all records produced throughout the rest of the day by that particular VVPAT, and (6) the attack is particularly viable on the TSx because the design of the VVPAT printer and the security casing for printed records allows the attack substance to linger undetected inside the machine until the end of election day; neither subsequent voters nor poll workers would know the attack had taken place until the printed records were removed at the end of Election Day; and

Whereas, the impact (once discovered) of the household substance attack on the VVPAT is highly visible, but when combined with an electronic attack that destroyed ballots, it could serve to effectively nullify most – if not all – of the votes cast on a particular TSx unit; and

Whereas, the Diebold Red Team members, without accessing Diebold source code, gained access to the election management server to manipulate and corrupt the election management system database; and

Whereas, some of these attacks could be carried out in a manner that is not subject to detection by audit, including review of software logs; and

Whereas, intellectual property is in any event notoriously difficult to protect against theft or unauthorized access, voting system source code being no less vulnerable; and

Whereas, Diebold left source code for one of its direct recording electronic voting machines unprotected on the Internet, from which it was downloaded and subsequently examined by many people, including computer security experts and other computer scientists; and

Whereas, a Diebold direct recording electronic voting machine was offered for sale on eBay, the Internet auction site; and

Whereas, tampering with optical scan equipment such as the Diebold AccuVote-OS precinct scanner and the AccuVote-OS Central Count can be readily detected and corrected through hand counting of the optical scan paper ballots marked and directly verified by voters; and

Whereas, voted and unvoted optical scan paper ballots can be secured through well-developed and tested physical security policies and procedures; and

Whereas, tampering with direct recording electronic voting machines such as the TSx can be difficult or impossible to detect, and is also difficult or impossible to correct through hand counting of VVPAT records, particularly when combined with successful attacks on VVPAT printing systems such as the AccuView Printer Module used with the TSx; and

Whereas, studies have shown that many voters do not review VVPAT records and that test voters who do review VVPAT records do not detect many discrepancies that have been intentionally introduced between selections shown on the paper record and selections shown on the review screen of a direct recording electronic voting machine; and

***Whereas*,** on July 30, 2007, a duly noticed public hearing was held to give interested persons an opportunity to express their views regarding the review of various voting systems, including the Diebold Election Systems, Inc., GEMS 1.18.24/AccuVote-TSX/AccuVote-OS voting system. At this hearing, approximately 60 individuals testified. Many more submitted comments by letter, facsimile transmission, and electronic mail; 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*,** I have reviewed the Diebold GEMS 1.18.24/AccuVote-TSX/AccuVote-OS voting system 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 July 30, 2007; and the comments submitted by letter, facsimile transmission, and electronic mail; and

***Whereas*,** pursuant to Elections Code section 19222, six months' notice must be given before withdrawing approval previously granted of any voting system or part of a voting system unless

I, as Secretary of State, for good cause shown, make a determination that a shorter period is necessary; and

Whereas, pursuant to Elections Code section 19222, any withdrawal by the Secretary of State of the previous approval of a voting system or part of a voting system is not effective as to any election conducted within six months of that withdrawal; 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:**

For the reasons set forth above, the Diebold Elections Systems, Inc., voting system, comprised of GEMS software, version 1.18.24, AccuVote-TSX with AccuView Printer Module and Ballot Station firmware version 4.6.4, AccuVote-OS (Model D) with firmware version 1.96.6, AccuVote-OS Central Count with firmware version 2.0.12, AccuFeed, Vote Card Encoder, version 1.3.2, Key Card Tool software, version 4.6.1, and VC Programmer software, version 4.6.1, which was previously approved, is found and determined to be defective or unacceptable and its certification and approval for use in subsequent elections in California is ~~immediately~~withdrawn effective August 3, 2007, except as specifically provided below.

1. In order to provide accessible balloting to voters with disabilities in compliance with HAVA, jurisdictions may use no more than one AccuVote-TSx per ~~polling place~~precinct on Election Day. Jurisdictions may have one unit available at each precinct for fail-over redundancy purposes and/or one unit for the purpose of creating voter access cards. To protect voter privacy, in instances in which at least one voter has cast their ballot on the device, jurisdictions are required to ensure that at least five persons voluntarily cast their ballot on ~~each such~~the device over the course of Election Day.

2. The AccuVote-TSx may be used in early voting prior to Election Day, subject to the following restrictions:
   - After the close of the polls each day of early voting, all voting equipment must be secured against tampering and returned by jurisdiction elections employees for storage in a jurisdiction facility that meets the security standards that apply to the jurisdiction's election headquarters;
   - Early voting centers may only be staffed by jurisdiction elections employees;
   - The jurisdiction must staff the early voting so that one employee, who is not required to be the same employee at all times, is responsible solely for monitoring the voting equipment to ensure no unauthorized access to the equipment occurs. That employee shall have no other duties while monitoring the voting equipment;
   - The jurisdiction must maintain a chain of custody log for each piece of equipment, in which two or more jurisdiction employees record, verify and sign off on the public counter numbers on the device, the integrity of the tamper-evident-seals and the serial number of those seals at the opening and closing of the polls each day of early voting; and
   - The jurisdiction must conduct a 100% manual ~~count~~tally, by the process described in Elections Code section 15360, of all votes cast on an AccuVote-TSx. 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.

3. The elections official must reset the encryption key used for all AccuVote-TSx units to change the key from the factory default setting to a unique value for each election prior to programming any units.

4. 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.

5. Within 30 days of the ~~date of this document,~~original issuance of this document on August 3, 2007, the vendor must present a plan and ~~uniform~~ jurisdiction Use Procedures to the Secretary of State for approval that will prevent future viral propagation of malicious software from one system component to another, such as from a voting system component located in one precinct to voting system components located in other precincts. The plan and Use Procedures must incorporate, or employ methods at least as effective as, a configuration of parallel central election management systems separated by an "air-gap" where (1) a permanent central system known to be running unaltered, certified software and firmware is used solely to define elections and program voting equipment and memory cards, (2) a physically-isolated duplicate system, reformatted after every election to guard against the possibility of infection, is used solely to read memory cards containing vote results, accumulate and tabulate those results and produce reports, and (3) a separate computer dedicated solely to this purpose is used to reformat all memory devices before they are connected to the permanent system again. (This "air-gap" model was proposed by the Source Code Review Team that reviewed the Diebold Election Systems, Inc., GEMS 1.18.24 voting system. Further details concerning the model are provided in Section 6.10 of the Source Code Review of the Diebold Voting System, dated July 20, 2007, and available on the Secretary of State website at http://www.sos.ca.gov/elections/voting_systems/ttbr/diebold-source-public-jul29.pdf.)

6. Within 30 days of the ~~date of this document,~~original issuance of this document on August 3, 2007, 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.

7. 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.

8. 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.

9. Within 30 days of the ~~date of this document,~~original issuance of this document on August 3, 2007, 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.

10. Within 45 days of the ~~date of this document,~~original issuance of this document on August 3, 2007, the vendor, working with ~~jurisdiction users,~~elections officials, must develop and submit to the Secretary of State for approval,~~uniform~~ 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.

11. ~~Network connections~~No network connection to any device not directly used and necessary for voting system functions ~~are prohibited.~~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.

12. Within 45 days of the ~~date of this document,~~original issuance of this document on August 3, 2007, the vendor, working with ~~jurisdiction users,~~elections officials, must develop and submit to the Secretary of State for approval, detailed~~uniform~~ 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:

~~Application of two-person rule;~~

- 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.

Following meetings with vendor and county representatives in the period from September 28, 2007, through October 5, 2007, the Secretary of State has determined that, at a minimum, the Use Procedures must require the jurisdiction to secure all voting system components in one or more uniquely serialized, tamper-evident container(s) 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 the same requirements for signed logging of the inspection of security containers and the removal and return of voting system components to security containers that apply to security seals and locks on the voting system components themselves. The following are examples of acceptable tamper-evident containers:

- A uniquely serialized, sealed banker's bag;
- A zippered nylon or canvass bag or case on which the zipper(s) that prevent access to the voting system component(s) inside are kept closed by a uniquely serialized, tamper-evident lock; or
- A hard lid that blocks access to all doors, ports or other points of access to the inside of the voting system component(s) and that is held in place by a latch or latches closed with a uniquely serialized, tamper-evident lock or locks.

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.

13. Where application of tamper-evident seals directly to a system component is~~are~~ required to detect unauthorized access to the~~a system~~ 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.

14. 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.

15. 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~~and audit log~~ 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.

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

17. Poll workers are not permitted to have access to any AVPM audit records, nor may they participate in any audits or recounts involving AVPM audit records. Poll workers may participate in audits involving AVPM audit records from a precinct other than the one in which they were a poll worker.

18. Within 60 days of the ~~date of this document,~~original issuance of this document on August 3, 2007, the vendor, working with ~~jurisdiction users,~~elections officials, must develop and submit to the Secretary of State for approval, specific detailed~~uniform~~ 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 AVPM audit trails;
    - ~~Escalation of audit sampling when significant discrepancies exist between electronic and manual audit vote results;~~ and
    - Reconciliation of ~~discrepancies~~variances between electronic and manual audit vote results.

19. Any post-election auditing requirements imposed as a condition of this certification shall be paid for by the vendor. ~~Jurisdiction users~~Elections officials are required to conduct the audits and the vendor is required to reimburse the jurisdiction.

20. After consultation with ~~jurisdiction users,~~elections officials, the Secretary of State shall establish additional post-election manual count auditing requirements, including:
    - Increased manual count sample sizes for close races, based on an adjustable sample model, where the size of the initial random sample depends on a number of factors, including the apparent margin of victory, the number of precincts, the number of ballots cast in each precinct, and a desired confidence level that the winner of the election has been called correctly. In establishing sampling requirements for close races, the Secretary of State may impose a specific sampling threshold for a given

vote differential or percentage of the margin of victory, taking into account the number of electors and the number and size of precincts in the race;
- Escalation requirements for expanding the manual count to additional precincts when ~~discrepancies~~variances are found; and
- ~~Uniform procedures~~Procedures to increase transparency and effectiveness of post-election manual count audits.

Elections officials must comply with these requirements as set forth by the Secretary of State in the document entitled "Post-Election Manual Tally Requirements" and any successor document. The vendor shall reference compliance with the "Post-Election Manual Tally Requirements" in its Use Procedures for the voting system.

21. ~~User jurisdictions~~Elections officials are required to conduct a 100% manual ~~count audit~~tally, by the process described in Elections Code section 15360, of the electronic results tabulated on each DRE machine in use on Election Day. 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.

22. Each polling place must be equipped with a method or log in a format specified by the Secretary of State after consultation with ~~the jurisdiction users~~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
- Election**s** official(s) who observed and/or recorded the event.

23. 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 ~~jurisdiction election~~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.

24. Training of poll workers must include the following:
- Secure storage of voting equipment while in the poll worker's possession;
- Chain-of-custody procedures~~(including two person rule)~~ 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 purpose served by the Voter Verified Paper Audit Trail (VVPAT), the importance of its use by voters, and how to handle problems such as paper jams;

- How to ensure, when required, that a minimum of five voters vote on each DRE in a polling place;
- The public right to inspect voting equipment and security seals, and how to handle requests for such inspection;
- How to handle equipment failure or lack of sufficient paper ballots in a polling place 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.

25. 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.~~26. 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.

~~26.~~27. 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.

~~27.~~28. 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 ~~audit~~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-only~~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.

~~28.~~29. 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 election~~s~~ 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 ~~audit~~tally, by the process described in Elections Code section 15360, over and above the normal manual ~~audit~~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-only~~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.

~~29.~~30. The Secretary of State will review and finalize all plans, requirements and procedures submitted pursuant to the foregoing requirements above within thirty 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.

~~30.~~31. 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.

~~31.~~32. The Secretary of State reserves the right, with reasonable notice to the vendor and to the ~~counties~~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.

~~32.~~33. Any ~~county~~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.

~~33.~~34. 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.

~~34.~~35. 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 voting equipment.

~~35.~~36. 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.

~~36.~~37. 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.

~~37.~~38. 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.

~~38.~~39. 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.

~~39.~~40. 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.

~~40.~~41. 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.

42. 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 ~~3~~~~rd~~25th day of ~~August,~~October, 2007.

DEBRA BOWEN
Secretary of State