State of California

SECRETARY OF STATE

ADDITIONAL CONDITIONS FOR USE OF
ELECTION SYSTEMS AND SOFTWARE, INC.
OPTICAL SCAN VOTING SYSTEM

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, on August 3, 2005, the Secretary of State granted conditional approval and use of the Election Systems and Software, Inc. Optical Scan Voting System comprised of AutoMARK Voter Assist Terminal version 1.0, AutoMARK Information Management System version 1.0, Model 100 Precinct Scanner version 5.0.0.0, Model 550 Central Scanner version 2.1.1.0, Model 650 Central Scanner version 1.2.0.0 and UNITY Election Management System 2.4.3 (Unity Version 2.4.3 with AutoMARK 1.0); 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, when I announced the top to bottom review I stated that if a vendor chose not to submit its certified system or systems to the review I reserved the right to exercise the clause in the existing certification for each system to add additional conditions that must be met in order for the system to retain its certification for the 2008 elections; and

Whereas, Election Systems and Software, Inc. declined to submit the Unity Version 2.4.3 with AutoMARK 1.0 system for a top-to-bottom review; and

Whereas, expert review of other voting systems 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, there is no reason to believe that many of these same vulnerabilities do not also exist in the Election Systems and Software Unity Version 2.4.3 with AutoMARK 1.0; and

Whereas, ES&S optical scanners have been shown to lose votes in election and test settings if the scanners are not precisely calibrated or the votes are marked in light inks; and

Whereas, pursuant to paragraph 5(c) of the conditional approval of the Election Systems and Software Optical Scan Voting System issued on August 3, 2005, the Secretary of State may impose additional requirements with respect to the use of any of the systems if the Secretary of State determines such modifications or additions are necessary to enhance the accuracy, reliability or security of any of the voting systems; 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 Election Systems and Software, Inc. Optical Scan Voting System, comprised of AutoMARK Voter Assist Terminal version 1.0, AutoMARK Information Management System version 1.0, Model 100 Precinct Scanner version 5.0.0.0, Model 550 Central Scanner version 2.1.1.0, Model 650 Central Scanner version 1.2.0.0 and UNITY Election Management System 2.4.3 (Unity Version 2.4.3 with AutoMARK 1.0), which was previously approved, is approved for use in subsequent elections in California subject to the following additional conditions.

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. Within 15 days the vendor must present a plan and 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.)

3. To prevent potential viral propagation of malicious software that could be introduced through an AutoMARK device, all memory cards used in the AutoMARK devices to configure them for an election must be reformatted by a physically and logically isolated computer using commercial software (not developed by ES&S) before the memory card can be reinserted into any other component of the voting system during that election or any subsequent election.

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.

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 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.

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. 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.

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

15. 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.

16. 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 ballots printed by AutoMARK voter assist terminals; and
    - Reconciliation of variances between electronic and manual audit vote results.

17. 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.

18. After consultation with 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 variances are found; and
    - Procedures to increase transparency and effectiveness of post-election manual count audits.

    Elections officials must comply with additional post-election manual count auditing 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.

19. Paragraph 5(g) of the Conditional Approval of Use of Election Systems and Software, Inc. Optical Scan Voting System issued on August 3, 2005, requires the vendor to provide all users of this system with test ballots and appropriate procedures to check and assess calibration of the Model 550 and Model 650 central tabulation scanners prior to each election. In addition to this requirement,

the vendor is hereby required to provide all users of this system who use the Model 100 precinct tabulation counter scanners with test ballots and appropriate procedures to check and assess calibration of the Model 100. In addition, elections officials must check and assess calibration of each Model 100, Model 550 and Model 650 scanner unit both before each election and following each election before the end of the official canvass. The vendor is required to reimburse the jurisdiction for the cost of the post-election calibration testing.

20. 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.

21. 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.

22. 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 AutoMARK voter assist terminal 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;
    - 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 AutoMARK ballot jams or other AutoMARK 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.

23. 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.

24. 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.

25. 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.

26. 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.

27. 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.

28. 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.

29. 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.

30. The Secretary of State reserves the right, with reasonable notice to the vendor and to the jurisdictions using the voting system, to modify the Use Procedures used with the voting system and to impose additional requirements with respect to the use of the system if the Secretary of State determines that such modifications or additions are necessary to enhance the accuracy, reliability or security of any of the voting system. Such modifications or additions shall be deemed to be incorporated herein as if set forth in full.

31. 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.

32. 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.

33. 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.

34. 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.

35. 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.

36. 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.

37. 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.

38. 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.

39. 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.

40. 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 6th day of December, 2007.

DEBRA BOWEN
Secretary of State