



# NEWS RELEASE

---

CALIFORNIA SECRETARY OF STATE **BRUCE McPHERSON**

BM06:021

FOR IMMEDIATE RELEASE  
Friday, February 17, 2006

Contact: Jennifer Kerns  
916-653-6575

## **Secretary of State Bruce McPherson Grants Certification with Conditions for Voting System**

*McPherson requires additional use procedures and security measures*

SACRAMENTO, CA - Secretary of State Bruce McPherson today announced his decision to certify with conditions the Diebold TSX and Optical Scan (OS) voting systems for use in California's 2006 elections. The decision comes after months of thorough review of both voting systems, their compliance with both state and federal laws and the completion of an additional security analysis by independent testers from computer labs at the University of California, Berkeley.

"As the State's chief elections official, the decision to certify voting systems is a very serious responsibility, and a number of factors must be carefully weighed before I determine whether to grant certification," said Secretary McPherson. "This is precisely why I created 10 strict standards that must be met for a voting system to be certified, making California's process the most stringent in the nation. We have applied these standards and after rigorous scrutiny, I have determined that these Diebold systems can be used for the 2006 elections."

Mikel Haas, San Diego County Registrar of Voters said, "I appreciate Secretary McPherson's leadership in establishing what must be the most comprehensive and rigorous certification process in the nation. To comply with new federal and state laws regarding elections, we need a new and different set of tools and Secretary McPherson made sure we got those tools." San Diego is home to California's first federal election of 2006, a special congressional vacancy election to be held in April.

The current voting system certification process was established by Secretary McPherson shortly after taking office in 2005. The certification process requires that each voting system or vendor meet 10 strict standards as conditions for use in the State's elections. The certification standards are designed to ensure that every voting system is secure, reliable and accurate for California's nearly 16 million voters. Among the requirements, systems must: undergo a first-in-the-nation requirement for a "volume test" to ensure the systems will withstand election day levels of activity, deposit a copy of the system source code and the binary executables with the Office of the Secretary of State, and establish a California County User Group to review the system and ensure voter usability.

-more-

After the completion of the federal and state certification requirements, as well as a complete and thorough review of the voting system components, Secretary McPherson requested that Diebold undergo an additional security analysis of the source code on the system's memory card. Computer scientists at the University of California, Berkeley laboratory conducted the additional security review of the memory card components for both systems. The independent reviewers concluded that while some of the code on the memory cards should be rewritten for an improved long-term solution, the problems identified are "manageable" and "the risks can be mitigated through appropriate use procedures."

In his certification of the systems, Secretary McPherson is mandating the additional use procedures from the independent reviewer's analysis to further bolster security and oversight of the use of these products. Counties wishing to use either the upgraded OS system or the upgraded, paper audit trail-retrofitted touch screen (TSX) system for elections in 2006 must comply with these requirements.

Diebold will be required to make all recommended long-term programming modifications contained in the report and submit the modified product to the Federal Independent Testing Authority (ITA) for requalification and state certification.

On December 20, 2005, Secretary McPherson requested that the ITA conduct an additional review of the Diebold systems. To date, that review is not yet complete. However, the additional security review conducted at the University of California, Berkeley addressed the identical issue that the federal testing authority was asked by this office to examine.

Currently, Diebold's OS is certified for use in 37 states including California, and the TSX is certified for use in 19 states including California. Eighteen of California's 58 counties used earlier versions of Diebold voting systems in the 2005 Special Election and in prior years. Both systems comply with federal and state laws.

For more information about California's certification process, visit the Secretary of State's website at

[http://www.ss.ca.gov/elections/voting\\_systems/ten\\_steps\\_to\\_vsys\\_certification.pdf](http://www.ss.ca.gov/elections/voting_systems/ten_steps_to_vsys_certification.pdf).

## **Use and Security Procedures Applicable to the Certification of the Diebold AV-TSX and AV-OS Voting Systems**

The county elections official must submit to the Secretary of State a plan for voter and poll worker education no later than 30 days prior to the election in which the system will be used. Training shall be conducted for all personnel, including poll workers, regarding proper treatment of memory cards and how to check for problems with seals, as well as how to record any problems discovered and what to do if such problems arise.

**In addition, the following security procedures will be in effect for use of the AV-TSX and AV-OS systems:**

- The elections official must reset the encryption key used for all AV-TSX units to change the key from the factory default setting prior to programming any units.
- Each memory card shall have a permanent serial number assigned to it.
- Each memory card must be programmed in a secured facility under the supervision of the registrar of voters/registrar of voters' staff. Once a memory card is programmed for the election, it must be immediately inserted into its assigned unit and sealed with a serialized, tamper-evident seal by the registrar of voters or the registrar's staff, and have its serial number logged into a tracking sheet designed for that purpose.
- The county must maintain a written log that records which memory cards and which serialized tamper-evident seals are assigned to which units. Any breach of control over a memory card shall require that its contents be zeroed, in the presence of two election officials, before it can be used again.
- On Election Day, prior to any ballots being cast on any unit, the integrity of the tamper-evident seal must be verified by the precinct officer before opening the compartment containing the memory card and unit power switch. The serial number of the seal must also be verified against the log provided the Precinct Inspector. This procedure must be witnessed by at least one other precinct officer or staff of the registrar of voters.
- If it is detected that the seal has been broken prior to the unlocking of the compartment, or if there is a discrepancy between the log and the serial number, the discrepancy must be confirmed by one or more of the remaining members of the precinct board, documented, and immediately reported to the county elections official for the jurisdiction. The elections official shall immediately investigate and determine appropriate action. If this potential breach occurs in unit, the specific unit must undergo a full manual reconciliation of the electronic votes cast and captured on the memory card against the paper audit record for that unit.
- The county must maintain a written log that accurately records the chain of custody of each memory card and unit from the point of programming the memory card for use in the election through the time of completion of the official canvass.
- Access to the GEMS server shall be tightly controlled and all persons having access to it at any time shall be pre-approved by the county elections official and

noted in a log that details name, time, and purpose of access to the room in which the GEMS is housed.

- If being used to meet the accessibility provisions of federal or state law, or if for any reason only one such unit is being used at the precinct, once one vote is cast on a TSX unit, the poll workers shall ensure that at least two more ballots are cast on the machine, even if not by a voter needing its accessibility components, in order to protect the privacy of the voter.
- Any issues that arise relating to voting equipment shall be reported to the Secretary of State's Office of Voting Systems Technology Assessment on Election Day, including a complete description of the problem and how it has been resolved. The Secretary of State will provide a telephone number for this purpose.

Prior to certification of the official canvass of returns by the county, the county will provide a written report to the Secretary of State addressing any issues related to the implementation and operation of the voting system. The county will make available for inspection by staff of the Office of the Secretary of State the chain of custody logs and/or documents relating to the system's use in that election.

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.

**Certification for use without the additional safety measures is contingent upon Diebold Election Systems Inc. making the suggested modifications to its software as outlined in the independent state audit report dated February 14, 2006, and successfully completing federal qualification by the Independent Testing Authorities or their successors as established by the federal Election Assistance Commission.**