DEBRA BOWEN | SECRETARY OF STATE | STATE OF CALIFORNIA
1500 11th Street, 6th Floor | Sacramento, CA 95814 | Tel (916) 653-7244 | Fax (916) 653-4620 | www.sos.ca.gov

TOP-TO-BOTTOM REVIEW OF ELECTRONIC VOTING SYSTEMS CERTIFIED FOR USE IN CALIFORNIA ELECTIONS

The Secretary of State intends within the next several weeks to begin a top-to-bottom review of voting systems currently certified for use in California elections. The goal of the review is to determine whether currently certified voting systems provide acceptable levels of security, accessibility, ballot secrecy, accuracy and usability under federal and state standards. For those that do not meet acceptable levels, the review will help determine whether certification should be withdrawn unconditionally, or withdrawn subject to re-certification with additional conditions on use for elections in 2007 and 2008.

Pursuant to Elections Code Section 19222, any decertification decision would only be effective for elections held more than six months later. Accordingly, a decertification decision made on or before August 3, 2007, would be effective for the February 5, 2008, presidential primary election. Every effort will be made to complete the top-to-bottom review of all voting systems before August. This will ensure that no voting system known to fall short of California's high standards will be used in any of the three major statewide elections scheduled for 2008. It will also assure local elections officials, poll workers and voters that they will not be required to change voting systems during the short intervals between the February and June 2008 elections and between the June and November 2008 elections, unless a serious new flaw is discovered that makes a later decertification unavoidable.

What follows is a set of draft criteria to guide the review of currently certified voting systems. The Secretary of State welcomes questions, comments and recommendations for changes from local elections officials, voting system vendors and any member of the public. This is only a draft; the final criteria may reflect substantial revisions based on the responses received and/or further review.

Please submit your questions, comments and recommendations regarding the draft criteria in writing no later than March 30, 2007 to:

By mail:

Secretary Debra Bowen
1500 11th Street
Sacramento, CA 95814
ATTN: Voting Systems Review, 6th Floor

By e-mail:

votingsystems@sos.ca.gov

After considering all questions, comments and recommendations submitted in response to the draft criteria, the Secretary of State will adopt final criteria no later than April 6, 2007.

DRAFT CRITERIA

Section 19205 of the Elections Code authorizes the Secretary of State to establish specifications for voting machines, voting devices, vote tabulating devices, and any software used for each, including the programs and procedures for vote tabulating and testing. These criteria must include suitability for the purpose for which a machine or device is intended, preservation of the secrecy of the ballot and safety of the voting system from fraud or manipulation. Pursuant to the authority established in Elections Code Section 19205, as well as the authority established by Section 12172.5 of the Government Code and Sections 10, 19222, 19227 and 19250 of the Elections Code, the Secretary of State hereby establishes criteria for the review of all voting systems currently certified for use in the State of California.

In each of the examination and testing processes set forth below, qualified reviewers selected by the Secretary will evaluate compliance with the mandatory provisions of the Elections Code, voluntary federal voting system standards as incorporated into California law by the Elections Code, and other applicable requirements imposed by state and federal law, including, but not limited to, Article II, Sections 2.5 and 7 of the California Constitution.

I. SECURITY.

1. Security Standards.

For purposes of these standards, "untraceable vote tampering" means preventing the accurate electronic recording of votes, or altering the record of votes, to change the result of an election in a manner that leaves no electronic record of tampering. "Denial of service attack" means disabling a voting system other than through sheer physical destruction in a manner that renders the voting system inoperable for voting.

a. DREs. Each direct recording electronic voting system ("DRE"), as defined in Elections Code Section 19251(b), must incorporate, as part of its design, hardware, firmware and/or software program features that effectively secure the DRE and all electronic media used with the DRE against untraceable vote tampering or denial of service attacks by any person with access to the DRE, its firmware, software and/or electronic media during their manufacture, transport, storage, temporary storage, programming, testing and use, including the electronic ballot definition or layout process.

b. Vote Tabulating Devices. Each "vote tabulating device," as that term is defined in Elections Code Section 358, must incorporate, as part of its design, hardware, firmware and/or software program features that effectively secure the vote tabulating

device and all electronic media used with the vote tabulating device against untraceable vote tampering or "denial of service" attacks by any person with access to the vote tabulating device, its firmware, software and/or electronic media during their manufacture, transport, storage, temporary storage, programming, testing and use.

c. Ballot Tally Computers and Ballot Tally Software. Each computer used to tally ballots and each "ballot tally software program," as that term is used in Elections Code Section 19103, must incorporate, as part of its design, hardware, firmware and/or software program features that effectively secure the computer, the ballot tally software program and all electronic media used with the computer and program against untraceable vote tampering or "denial of service" attacks by any person with access to ballot tally software program, the ballot tally computer, its firmware, software and/or electronic media during their manufacture, transport, storage, temporary storage, programming, testing and use.

2. Security Testing.

The security of each DRE, vote tabulating device and ballot tally computer will be tested using two complementary methods, "red teaming" and source code review. The Secretary will select qualified industry and academic experts in computer and software security, including experts in electronic voting systems, to perform both types of tests.

a. Red Teaming. The "red teaming" process is analogous to military training exercises in which the members of the "red team" are adversaries trying to defeat friendly, "blue team" forces. The red team exercise will be designed to simulate conditions in which a voting system might be vulnerable to attack in the actual cycle of manufacturing, programming, delivery, testing, storage, temporary storage and use in California elections. Initially, the team will approach the system knowing nothing of its source code. Knowledge of source code may be used in subsequent attack attempts. The objective will be to determine whether and to what degree it is possible to compromise the security of the voting system to interfere with the accurate recording of votes or alter the record of votes to change the result of an election.

b. Source Code Review. The second component of security testing will be source code review. The objective of the source code review will be to identify anything in the code that could be used maliciously to interfere with the accurate recording of votes or alter the record of votes to change the result of an election. The source code review may be performed prior to, during or after completion of the risk assessment.

3. Security Findings.

Upon completion of either component of the security testing, the Secretary of State may make written findings that a DRE, vote tabulation device or ballot tally computer is not reasonably secured against untraceable vote tampering and "denial of service" attacks by features included in the design of its hardware, firmware and/or

software. On the basis of such written findings, the Secretary may immediately initiate the process to withdraw certification.

II. ACCESS FOR VOTERS WITH DISABILITIES.

1. Disability Access Standards.

The federal Help America Vote Act (HAVA) requires that all polling places in elections for federal office have at least one voting system that is "accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters."

Under Elections Code Section 19250(a), the Secretary of State may not certify a DRE unless the system "includes an accessible voter verified paper audit trail." Elections Code Section 19250(d) requires that all DRE voting systems "shall include a method by which a voter may electronically verify, through a nonvisual method, the information that is contained on the paper record copy of that voter's ballot." Under Elections Code Section 19251(a), "'[a]ccessible' means that the information provided on the paper record copy from the voter verified paper audit trail mechanism is provided or conveyed to voters via both a visual and a nonvisual method, such as through an audio component."

2. Disability Access Testing.

Each voting system will be examined to determine whether it complies with the accessibility requirements of HAVA and the Elections Code. The examination will be conducted with the assistance of persons from the disabled community. For purposes of this review, a voting system complies only if it provides all of the following features and capabilities in at least one voting system available for use in every polling place:

(a) A dual-switch input control interface that permits use of "sip and puff" or other adaptive devices by voters with paralysis or severe manual dexterity disabilities who are unable to use touch screens or tactile key inputs.

(b) The capability for the voter to select simultaneous and synchronized audio and visual outputs, audio outputs only or visual outputs only.

(c) Voter-adjustable magnification, contrast and display color settings to improve the readability of text on the video displays.

(d) Variable audio output levels and playback speed for voters with hearing impairments.

(e) Privacy curtains or shields that effectively prevent others from observing or hearing the selections of a voter using such features as audio output, simultaneous,

synchronized audio and visual output, display magnification or modified display font, contrast or color settings.

(f) In the case of a DRE, the capability to permit a voter to verify electronically, through a nonvisual method, the information that is contained on the voter verifiable paper record copy of that voter's ballot. This requirement is satisfied by a method of nonvisual confirmation that draws the information provided to the voter from either (1) the paper record copy itself or (2) the same electronic data stream used to print the voter verifiable paper record copy.

3. Disability Access Findings.

The Secretary of State may make written findings, based on the results of the disability access testing described above, that a voting system fails to include any of the foregoing disability access features and capabilities, in which case the Secretary of State may immediately initiate the process to withdraw certification from the voting system for disability access use.

III. ACCESS FOR MINORITY LANGUAGE VOTERS.

HAVA requires that every voting system used in an election for federal office "shall provide alternative language accessibility pursuant to the requirements of Section 203 of the Voting Rights Act of 1965 (42 U.S.C. 1973aa-1a)." Every certified voting system will be tested to determine whether it provides alternative language accessibility in the federally mandated language or languages for each county that uses or intends to use the system. If the Secretary of State makes written findings, based on the results of the minority language access testing, that a voting system does not provide alternative language access as required by federal law, the Secretary of State may immediately initiate the process to withdraw certification from the voting system with respect to the affected county or counties.

IV. USABILITY FOR ELECTIONS OFFICIALS AND POLL WORKERS.

Each certified voting system must be designed, configured and accompanied by sufficient documentation and training materials so that, in the absence of extraordinary circumstances, elections officials and poll workers can independently and without assistance or intervention by employees or contractors of an election system vendor, carry out all operations necessary to open the polls, set up and calibrate voting system equipment, instruct and assist voters in registering votes and casting ballots, respond to voting system error messages or temporary power failures, close the polls, print end-of-day vote totals, take down voting system equipment, transfer polling place results to central tally computers and tally final results.

The Secretary of State will conduct a review of each voting system's documentation and records regarding the use of the voting system by elections officials and poll workers in California elections. The Secretary of State may make written findings, based on the results of the review, that a voting system does not reasonably permit such independent operation. Based on such findings, the Secretary of State may immediately initiate the process to withdraw certification from the voting system.