

# County of Santa Clara

## Registrar of Voters

1555 Berger Drive, Building 2  
San Jose, California 95112  
Mailing Address: P.O. Box 1147, San Jose, CA 95108  
(408) 299-VOTE (8683) (866) 430-VOTE (8683) FAX (408) 998-7314  
[www.sccvote.org](http://www.sccvote.org)



March 29, 2007

The Honorable Debra Bowen  
Secretary of State  
1500 11<sup>th</sup> Street  
Sacramento, CA 95814  
Attn: Voting Systems Review, 6<sup>th</sup> Floor

### RE: COMMENTS ON TOP-TO-BOTTOM REVIEW OF ELECTRONIC VOTING SYSTEMS DRAFT CRITERIA

Dear Secretary Bowen:

As Registrar of Voters for the County of Santa Clara, I appreciate the opportunity to submit our comments on the Top-to-Bottom Review of Electronic Voting Systems Certified for use in California Elections Draft Criteria.

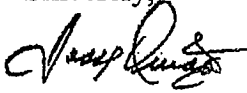
Public awareness of the elections process has never been higher. The scrutiny placed upon Direct Recording Electronic Voting Machines has never been more focused. For these and other reasons the County of Santa Clara has been a supporter of previous changes to our voting system including the AVVPAT and I was personally pleased to have served on the Secretary of State's working AVVPAT task force.

We have methodically and systematically reviewed the draft criteria as an operations staff and have come to the unanimous and regrettable conclusion that under these draft criteria our systems could become decertified. We are uncertain as to what systems would be made available to us to conduct elections beginning with the February 2008 Presidential Primary. It appears that all systems currently certified for use in California are vulnerable to decertification under this draft criteria.

Please find attached our suggested edits, as well as, questions regarding the draft criteria which we feel could have very serious consequences.

As the entity responsible for administering local elections we look forward to cooperating with you and your office, we respectfully request your consideration of these edits. I am confident that working together we can go a long way towards helping to restore the electorates confidence in the democratic process.

Sincerely,

A handwritten signature in black ink, appearing to read "Jesse Durazo", written in a cursive style.

Jesse Durazo  
Registrar of Voters

cc: Peter Kutras, Jr., County Executive, Santa Clara County  
Elaine Larson, Assistant Registrar of Voters, Santa Clara County

Attachment

**Comments on Top-to-Bottom Review of Electronic Voting Systems 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.

**ROV Response I.1.a:**

ROV has not experienced any consequence related to the suggested program features identified. These program features appear to be conceptual, and their design may result in further dependence on more "code" and "microchip" technology design which is subject to further speculation by electronic voting pundits.

In regards to EC 19251(b) "'Direct recording electronic voting system" means a voting system that records a vote electronically and does not require or permit the voter to record his or her vote directly onto a tangible ballot," we are unable to locate any relationship to code in regards to these added feature requirements

## Santa Clara County Draft Criteria Response

“untraceable vote tampering or denial of service attacks by any person with access;” being addressed.

- Question 1: These are new requirements for development and manufacturing. From a contractual point of view, can these new features be enforceable on existing Secretary of State (SOS) California approved contract requirements for system certification? If SOS incorporates these features into existing SOS California approved contract features, then is not de facto decertification introduced?
- Question 2: If this is a plan for decertification, what steps are required for recertification? What are the timelines for decertification, recertification and review prior to the February 2008 Election?
- Question 3: What are the processes and standards that will be used for appeals?
- Question 4: In the event of decertification, what certified systems and approved vendors including hardware, firmware and software programs will remain for the conduct of elections?
- Question 5: Under current budget constraints, funding becomes a big issue. Will the state fund new hardware, firmware and software programs, in addition to implementation costs to include facility modification and voter outreach? What will the procurement guidelines consist of?

Program Responsibility: SOS

**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.

### ROV Response I.1.b:

ROV has not experienced any consequence related to these newly suggested program features identified.

Decertification of our entire vote tabulating devices and system would occur automatically with any decertification of our DRE counting software. Our optical scan ballot counting system which includes absentee balloting would become decertified as well.

Program Responsibility: SOS

**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.

**ROV Response I.1.c:**

Santa Clara County has always taken high security measures to secure our vote tabulating computers, devices, software and electronic media. This includes strict key card access and security cameras.

"Untraceable vote tampering or "denial of service" attacks" is not an issue and has not been a previous requirement under Federal and State certification. Our system is in a secured location, off the network and access is not available.

Item a, b, and c are code issues that have been currently under SOS testing and safeguarding.

Program Responsibility: SOS

**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.

**ROV Response I.2.a:**

All code programs are under the watchful eye of the SOS. They are clearly in the SOS's domain and have been available for inspection anytime the SOS made a requirement (California Elections Code 19103(a)).

## Santa Clara County Draft Criteria Response

- Question 1: Any system could be vulnerable to attack, given sufficient time. What would be the time constraints? Would these attacks occur under the actual security measures and constraints we place on them during an election?
- Question 2: Could you provide more clarification regarding, “vulnerable to attack in the actual cycle of manufacturing, programming, delivery, testing, storage, temporary storage and use in California elections?” Would testing occur in actual counties?

Program Responsibility: SOS

**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.

### ROV Response I.2.b:

In addition to our questions and response to 2a:

- Question 1: What would be the restrictions and security of the experts? Would this group include election employees?

Program Responsibility: SOS

**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.

### ROV Response I.3:

- Question 1: In the event there is a finding that the testing methodology finds unsupported documentation to the feature attacks of “voter tampering” and “denial of service” will the SOS declare a condition of certification?
- Question 2: If a feature failure is found, what is the process of constructive notification and response?
- Question 3: If there is conditional certification, what is the process for use and recertification?
- Question 4: Santa Clara County has at least two elections to conduct prior to any potential decertification and any security findings could be

released prior to these election dates. Would the technical reports be proprietary and/or provided to the counties prior to public release?

Program Responsibility: SOS

## **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."

#### **ROV Response II.1:**

Program Responsibility: SOS

### **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.

#### **ROV Response II.2.a:**

ROV has implemented the "Sip and Puff" devices.

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

**ROV Response II.2.b:**

This is not a current requirement for any certified system in California nor is it mentioned in the 2005 Voluntary Voting System Guidelines. The addition of this requirement would require a code change followed by Federal and State certification.

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

**ROV Response II.2.c:**

The contrast and display color settings are not certified or required under the 2002 Standards for our systems. The addition of this requirement would require a code change followed by Federal and State certification.

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

**ROV Response II.2.d:**

Sequoia Edge II meets these requirements.

- (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.

**ROV Response II.2.e:**

This would be a new requirement; recommend deletion. The addition of this requirement would require a code change followed by Federal and State certification.

- (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.

**ROV Response II.2.f:**

ROV believes Sequoia Edge II system meets this requirement

**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.



**ROV Response II.3:**

If the SOS makes a finding of deficiency, what is the process for conditional certification?

**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.

**ROV Response III:**

ROV believes our voting systems meet this requirement.

**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.

**ROV Response IV:**

ROV believes professionally designed documentation and training materials are available to independently and without assistance or intervention by employees or contractors carry out its mission. We believe that the required documents, designed both in house, and by our vendor, are in our possession for this itemized listing.

## Santa Clara County Draft Criteria Response

Question 1: Santa Clara County may have better materials and/or documentation not provided during the initial certification designed in house, what is the process to request documentation from the County?

We also suggest deleting "the SOS may immediately initiate the process to withdraw certification from the voting system" and add "The SOS will request specific additional documentation to enable certification prior to initiating the process to withdraw certification from the voting system."

# County of Santa Clara

## Registrar of Voters

1555 Berger Drive, Building 2  
San Jose, California 95112  
Mailing Address: P.O. Box 1147, San Jose, CA 95108  
(408) 299-VOTE (8683) (866) 430-VOTE (8683) FAX (408) 998-7314  
[www.sccvote.org](http://www.sccvote.org)



March 28, 2007

The Honorable Debra Bowen  
California Secretary of State  
1500 – 11<sup>th</sup> Street, Suite 600  
Sacramento, CA 95814

Dear Secretary Bowen:

It has been brought to my attention that you referenced a situation that occurred in Santa Clara County during the November 5, 2006 Election while addressing the Sub-Committee on Elections, Committee on House Administration on March 22, 2007. The situation was regarding an incident involving an inspector sending someone to make copies of ballots at Kinko's. There have been a number of media reports regarding this and I feel it is important to provide clarification on what actually happened.

As you know, Santa Clara County is a touch screen county and DREs are used in all voting locations. The November Election was the second election using the Voter Verifiable Paper Audit Trail (VVPAT) and each precinct was issued 55 Sample Ballots as a paper back-up. Arthur Keller was the Inspector working at Precinct 2065, St. Albert Great Church in Palo Alto. The November 5, 2006 ballot consisted of 17 DRE screens and approximately four to five printed VVPAT pages to review. The AVVPATs can handle approximately 83 voters before running out of paper. This particular voting precinct experienced a higher than projected turnout and many voters took an unusually long time to vote and review their choices resulting in long lines at the precinct. To alleviate the long line, Mr. Keller offered the voters the option to vote on paper. Below is what Mr. Keller reported in an email sent to our office on November 15, 2006:

"When the third machine's printer ran out of tape, and we were down to three working voting machines, and the line for a voting machine was getting longer, I figured it was only a matter of time until we were down to just one voting machine (the one with the replaced printer tape). So a poll worker and I gathered a bunch of sample ballots from the voter books, carefully opening the staples to remove the sample ballots without tearing them. I then offered them to anyone in the line for a voting machine and said it would likely take a while before they got to vote on the electronic voting machine. About a dozen voters took me up on the offer, shortening the line to a more manageable number. Soon all the voting machines with the original printers had run out of tape. Given the size of the ballot, and that some confused voters had printed the paper ballot record copy more than once, a paper tape roll can only handle about 83 ballots.

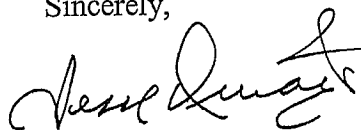
Now with only one working voting machine, we reserved that machine for provisional ballots, voters with kids, and those who insisted on voting electronically. Sometimes we had 20 people at a time voting on paper. Hand-marked paper ballots are clearly more scaleable and more resilient than electronic voting machines. However, our supply of sample ballots was dwindling. So I called the County hot line, who reported the problem of running out of tape was widespread and I was on my own. At about 7:10pm, I sent one of my poll workers with \$40 of my own money and my car keys and one of the remaining paper ballots (one of the foreign language ones, because they're more sturdy and still have English on them—the Spanish and English ones are printed on newsprint) to Kinko's to print more ballots. In about 20 minutes, he returned with a stack of ballots, my car keys, and just over \$20 in change.

The remaining voters had their choice of "paper or plastic." Most chose paper. The rate of voters slowed down. When the last voter was done at 8:05pm, we started the close out process. We were done just after 9pm. Of the 501 ballots cast in our precinct, 63 were on sample paper ballots, about 10 of which were on Kinko's ballot stock. The ballots were two tabloid (11x17) sheets printed double-sided. We counted 501 signatures in the roster book, which exactly matched the number of paper ballots plus the total number of ballots reported by the electronic voting machines. And the number of provisional ballots reported by the electronic voting machines exactly matched the number of provisional forms we had."

As instructed in Election Officer training, voters could have used the sample ballots in their Sample Ballot Voter Information Pamphlet. While the inspector was not instructed to send someone to make additional copies of the ballot at Kinko's, he was reimbursed the \$20 to cover his out of pocket expense. To lessen the probability of this from reoccurring in Santa Clara County, our office will be expanding its permanent absentee voter program and increasing the number of polling places. Additionally, optical scan ballots will be deployed to voting precincts to be used prior to the contingency plan of voting on the sample ballots. Attached is copy of the memo dated February 1, 2007 from Philip Chantri which provides further details about Precinct 2065.

Santa Clara County takes pride in its successful elections using the Sequoia Edge II voting machines. Please let me know if you have any questions or need further clarification.

Sincerely,



Jesse Durazo  
Registrar of Voters

cc: Peter Kutras, Jr., County Executive, Santa Clara County  
Elaine Larson, Assistant Registrar of Voters, Santa Clara County

Attachment

# County of Santa Clara

Registrar of Voters

1555 Berger Drive, Building 2

San Jose, California 95112

Mailing Address: P.O. Box 1147, San Jose, CA 95108

(408) 299-VOTE (8683) (800) 430-VOTE (8683) FAX (408) 998-7314

www.sccvotes.org



## Memo

To: Jesse Durazo, Registrar of Voters

From: Philip Chantri, Acting Assistant Registrar of Voters PC

Date: February 1, 2007

Re: Media Reports Regarding PCT 2065 in the November 7, 2006 Election

Several media outlets have carried stories regarding a Santa Clara County Precincts' need to copy ballots at a local Kinko's due to voting failures on Election Day. The following are the facts gleaned from the Precinct Inspector, the Assistant Registrar of Voters, The Canvass Manager, The Ballot Duplication Manager and the Precinct Operations Division Manager.

Precinct 2065, St. Albert the Great Church in Palo Alto, Ballot Type 84, processed 421 regular and 17 Provisional Voters using electronic voting equipment. In addition 63 Voters voted using Sample Ballot Pages. The Roster and Official Ballot Statement from Election Day shows 501 Voters. This precinct balanced on the first round of the canvass. All 63 voted sample ballots were duplicated and tallied during the canvass process. The final Statement of Vote shows a total of 496 precinct ballot cast. This five ballot discrepancy is due to the fact that 5 of the 17 provisional votes could not be counted due to lack of ID.

The Precinct was issued 55 Sample Ballots with their precinct supplies and all Voters in the County are mailed one prior to Election Day. The Precinct Inspector sensing the high turnout felt that the precinct might run out of sample ballots, and at 7:10 pm dispatched a clerk to make additional copies at Kinko's and return them to the precinct. The precinct processed all voters by 8:05 pm and completed their Election Day duties just after 9 pm.

The Precinct Inspector and Clerks in this polling place did an excellent job and performed as trained on Election Day. All of the forms were properly and completely filled out with 438 electronic Voters Processed, 63 Paper Ballot Voters processed and 114 Absentee Ballots dropped off at the precinct.

In addition, to lessen the probability of this from reoccurring the Registrar of Voters Office will be increasing by greater than 27 percent from the 786 Precincts used on Election Day to 1000 precincts in future elections. Additionally, we will be deploying 55 Optical Scan Ballots to each of our Precincts in future elections to be used prior to the contingency plan of voting on sample ballot pages. The Registrar of Voters Office is committed to ensuring all eligible Voters have the opportunity to cast their Vote. They did so in this case and we will continue to ensure they are able to in future elections.

# County of Santa Clara

## Registrar of Voters

1555 Berger Drive, Building 2  
San Jose, California 95112  
Mailing Address: P.O. Box 1147, San Jose, CA 95108  
(408) 299-VOTE (8683) (866) 430-VOTE (8683) FAX (408) 998-7314  
www.sccvote.org



March 29, 2007

The Honorable Debra Bowen  
Secretary of State  
1500 11<sup>th</sup> Street  
Sacramento, CA 95814  
Attn: Voting Systems Review, 6<sup>th</sup> Floor

### RE: COMMENTS ON TOP-TO-BOTTOM REVIEW OF ELECTRONIC VOTING SYSTEMS DRAFT CRITERIA

Dear Secretary Bowen:

As Registrar of Voters for the County of Santa Clara, I appreciate the opportunity to submit our comments on the Top-to-Bottom Review of Electronic Voting Systems Certified for use in California Elections Draft Criteria.

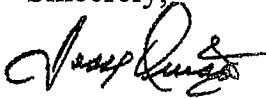
Public awareness of the elections process has never been higher. The scrutiny placed upon Direct Recording Electronic Voting Machines has never been more focused. For these and other reasons the County of Santa Clara has been a supporter of previous changes to our voting system including the AVVPAT and I was personally pleased to have served on the Secretary of State's working AVVPAT task force.

We have methodically and systematically reviewed the draft criteria as an operations staff and have come to the unanimous and regrettable conclusion that under these draft criteria our systems could become decertified. We are uncertain as to what systems would be made available to us to conduct elections beginning with the February 2008 Presidential Primary. It appears that all systems currently certified for use in California are vulnerable to decertification under this draft criteria.

Please find attached our suggested edits, as well as, questions regarding the draft criteria which we feel could have very serious consequences.

As the entity responsible for administering local elections we look forward to cooperating with you and your office, we respectfully request your consideration of these edits. I am confident that working together we can go a long way towards helping to restore the electorates confidence in the democratic process.

Sincerely,

A handwritten signature in black ink, appearing to read "Jesse Durazo", written in a cursive style.

Jesse Durazo  
Registrar of Voters

cc: Peter Kutras, Jr., County Executive, Santa Clara County  
Elaine Larson, Assistant Registrar of Voters, Santa Clara County

Attachment

**Comments on Top-to-Bottom Review of Electronic Voting Systems 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.

**ROV Response I.1.a:**

ROV has not experienced any consequence related to the suggested program features identified. These program features appear to be conceptual, and their design may result in further dependence on more "code" and "microchip" technology design which is subject to further speculation by electronic voting pundits.

In regards to EC 19251(b) "'Direct recording electronic voting system" means a voting system that records a vote electronically and does not require or permit the voter to record his or her vote directly onto a tangible ballot," we are unable to locate any relationship to code in regards to these added feature requirements



“untraceable vote tampering or denial of service attacks by any person with access;” being addressed.

- Question 1: These are new requirements for development and manufacturing. From a contractual point of view, can these new features be enforceable on existing Secretary of State (SOS) California approved contract requirements for system certification? If SOS incorporates these features into existing SOS California approved contract features, then is not de facto decertification introduced?
- Question 2: If this is a plan for decertification, what steps are required for recertification? What are the timelines for decertification, recertification and review prior to the February 2008 Election?
- Question 3: What are the processes and standards that will be used for appeals?
- Question 4: In the event of decertification, what certified systems and approved vendors including hardware, firmware and software programs will remain for the conduct of elections?
- Question 5: Under current budget constraints, funding becomes a big issue. Will the state fund new hardware, firmware and software programs, in addition to implementation costs to include facility modification and voter outreach? What will the procurement guidelines consist of?

Program Responsibility: SOS

**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.

**ROV Response I.1.b:**

ROV has not experienced any consequence related to these newly suggested program features identified.

Decertification of our entire vote tabulating devices and system would occur automatically with any decertification of our DRE counting software. Our optical scan ballot counting system which includes absentee balloting would become decertified as well.

Program Responsibility: SOS

**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.

**ROV Response I.1.c:**

Santa Clara County has always taken high security measures to secure our vote tabulating computers, devices, software and electronic media. This includes strict key card access and security cameras.

“Untraceable vote tampering or “denial of service” attacks” is not an issue and has not been a previous requirement under Federal and State certification. Our system is in a secured location, off the network and access is not available.

Item a, b, and c are code issues that have been currently under SOS testing and safeguarding.

Program Responsibility: SOS

**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.

**ROV Response I.2.a:**

All code programs are under the watchful eye of the SOS. They are clearly in the SOS’s domain and have been available for inspection anytime the SOS made a requirement (California Elections Code 19103(a)).

## Santa Clara County Draft Criteria Response

- Question 1: Any system could be vulnerable to attack, given sufficient time. What would be the time constraints? Would these attacks occur under the actual security measures and constraints we place on them during an election?
- Question 2: Could you provide more clarification regarding, “vulnerable to attack in the actual cycle of manufacturing, programming, delivery, testing, storage, temporary storage and use in California elections?” Would testing occur in actual counties?

Program Responsibility: SOS

**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.

### **ROV Response I.2.b:**

In addition to our questions and response to 2a:

- Question 1: What would be the restrictions and security of the experts? Would this group include election employees?

Program Responsibility: SOS

**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.

### **ROV Response I.3:**

- Question 1: In the event there is a finding that the testing methodology finds unsupported documentation to the feature attacks of “voter tampering” and “denial of service” will the SOS declare a condition of certification?
- Question 2: If a feature failure is found, what is the process of constructive notification and response?
- Question 3: If there is conditional certification, what is the process for use and recertification?
- Question 4: Santa Clara County has at least two elections to conduct prior to any potential decertification and any security findings could be

released prior to these election dates. Would the technical reports be proprietary and/or provided to the counties prior to public release?

Program Responsibility: SOS

## **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.”

#### **ROV Response II.1:**

Program Responsibility: SOS

### **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.

#### **ROV Response II.2.a:**

ROV has implemented the “Sip and Puff” devices.

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

**ROV Response II.2.b:**

This is not a current requirement for any certified system in California nor is it mentioned in the 2005 Voluntary Voting System Guidelines. The addition of this requirement would require a code change followed by Federal and State certification.

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

**ROV Response II.2.c:**

The contrast and display color settings are not certified or required under the 2002 Standards for our systems. The addition of this requirement would require a code change followed by Federal and State certification.

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

**ROV Response II.2.d:**

Sequoia Edge II meets these requirements.

- (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.

**ROV Response II.2.e:**

This would be a new requirement, recommend deletion. The addition of this requirement would require a code change followed by Federal and State certification.

- (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.

**ROV Response II.2.f:**

ROV believes Sequoia Edge II system meets this requirement

**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.

**ROV Response II.3:**

If the SOS makes a finding of deficiency, what is the process for conditional certification?

**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.

**ROV Response III:**

ROV believes our voting systems meet this requirement.

**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.

**ROV Response IV:**

ROV believes professionally designed documentation and training materials are available to independently and without assistance or intervention by employees or contractors carry out its mission. We believe that the required documents, designed both in house, and by our vendor, are in our possession for this itemized listing.

## Santa Clara County Draft Criteria Response

Question 1: Santa Clara County may have better materials and/or documentation not provided during the initial certification designed in house, what is the process to request documentation from the County?

We also suggest deleting “the SOS may immediately initiate the process to withdraw certification from the voting system” and add “The SOS will request specific additional documentation to enable certification prior to initiating the process to withdraw certification from the voting system.”