SEQUOIA
voting systems

30 March 2007

The Honorable Ms. Debra Bowen
California Secretary of State
1500 11th Street, 6th floor
Sacramento, California 95814

Re: Public Comment after review of the Draft "**TOP-TO-BOTTOM-REVIEW OF ELECTRONIC VOTING SYSTEMS CERTIFIED FOR USE IN CALIFORNIA ELECTIONS**"

Dear Secretary Bowen:

As the provider of voting technology solutions and services to over twenty counties throughout the State of California, we commend your efforts to increase voter confidence and ensure that the voting systems in California continue to be accessible, secure, and reliable; and that the testing process for these systems continues to be thorough, rigorous, and transparent serving as an example to the nation. Below are some comments generally meant to clarify the test program and its requirements so that we can better understand and fulfill the scope of Review by your office.

Thank you for the opportunity to comment on this Draft Review standard.

Respectfully Yours,

[signed and sent via electronic mail]

Edwin Smith
VP, Compliance/Quality/Certification
Sequoia Voting Systems

Public Comment after review of the Draft "**TOP-TO-BOTTOM REVIEW OF ELECTRONIC VOTING SYSTEMS CERTIFIED FOR USE IN CALIFORNIA ELECTIONS**"

1. While definitions are provided for both "untraceable vote tampering" and "denial of service attack", there is no definition provided for "effective security". What does the Secretary plan to use as a definition of "effective security" and how will that term be applied in practice?
2. Paragraph I.1. provides that untraceable vote tampering means to "...change the result of an election in a manner that leaves no electronic record of tampering". What about paper records? Paper records are audited by State Law, so they should be included as an indicator of possible tampering. Also, what about tamper evident seals and their role in protecting the voting system and preventing a more common definition of "untraceable"?
3. Paragraph I.1.b. and c. regarding the vote tabulating devices and ballot tally computers – the design and manufacture of central count computers are generally outside of the scope of the voting systems vendor community and the customer jurisdictions. How does the Secretary plan to evaluate these areas in light of the fact that these are off-the-shelf systems and thus changing the design and monitoring the manufacture would pose a high burden on the vendors and jurisdictions?
4. Paragraph 2- There are few details provided regarding the conduct of the tests in this section, making public comment difficult. Will the Secretary be publishing detailed Scope of Work, Test Plan, or similar documentation?
5. Paragraphs 2 and 2.b. – what limits on public disclosure of source code will be enforced during the review process? The Secretary could enact a process by which the expert reviewers would be allowed to perform their review in view of the public and to make their report unfettered, but with no person being able to remove source code, their reviewer's notes, or any work product from the review room. This review process structure would provide the best balance between transparency and protection of vendor intellectual property.
6. Paragraph 2.a. – If the testing is structured as a "red team" exercise, who will be the "blue team"? If the goal is to properly emulate the election cycle as implied, then "blue team" election judges should be employed, as well as security guards and other actors where both required by State Law and in place due to common jurisdiction practice.
7. Paragraph II.1. It is clear from the latest NIST-EAC TGDC meeting held 3/22 and 3/23 that there are no Federally certified accessible VVPAT devices available on the market, nor are any that that have been placed into the Federal voting system certification process. How does the Secretary reconcile this with the requirement?