CALIFORNIA ASSOCIATION OF
CLERKS AND ELECTION OFFICIALS

Statement of Steve Weir, President
California Association of Clerks and Election Officials

TOP-TO-BOTTOM REVIEW PUBLIC HEARING, JULY 30, 2007

I was truly excited when I met with Secretary Bowen on January 10, 2007 and heard of her plans to do a comprehensive review of all of California's voting systems. I offered the assistance of California's Registrars.

I support independent review of voting systems including source code, and I support legitimate, real-world penetration testing as part of system certification.

I am sorry to say that I find the approach of the so-called Top-to-Bottom Review to be more to do with headlines than with definitive science or the pursuit of legitimate public policy.

We have been told that no malicious code was found during the source-code examination. Unfortunately, while this issue is a matter of public debate nationwide, no such comprehensive review was even attempted. If true, this is a tragic missed opportunity and a public-policy blunder.

In all honesty, California Registrars have expected and California voters have deserved a definitive answer to the question: Is there malicious code in our voting systems source code or not?

Equally troubling to me is the lack of published, clear, sound and testable standards for the penetration portion of the testing. Matt Bishop stated, in "Communications of the ACM, March 2007 / Vol. 50, No. 3, Fixing Federal E-Voting Standards" concerning systems testers: "They need the computer science community's help and active engagement in writing clear, sound, and testable standards." (Part of the original document calling for this review references the National Institute of Science and Technology (NIST) and its call for penetration testing **under written standards.** NIST stated that those standards did not exist and needed to be developed before testing.)

If such written clear, sound and testable standards are not forthcoming from this effort, this, too, will be another lost opportunity and public-policy blunder.

Lastly, the choice to test voting systems in a theoretical laboratory setting, without even considering the real-world use of systems, has deprived all of us, testing personnel included, of the definitive answer to the real-world use of voting systems. (All materials presented readily admit to this over and over.)

In the real world, California has the toughest voting-system requirements and testing in the nation. For electronic-voting systems, which are used in over half of California's counties, we are required to produce a voter-verifiable paper-audit trail of all votes. Every manual audit of this paper-trail document against machine totals has shown that the systems reported every vote accurately.

The Secretary of State has mandated and has conducted an additional check on electronic-voting systems. Called parallel monitoring, the Secretary of State has published the results of several tests and has concluded that in every case, machines have: "…accurately recorded all of the votes cast in those machines."

What I consider these materials to represent is a theoretical hologram, an image if you will, of what could exist without the mitigating conditions of every day, real-world reality.

What I consider these materials Not To Be is a comprehensive, top-to-bottom review. They lack published testing standards, they lack any examination or consideration of real-world mitigation, and they lack the involvement of hands-on election experts, including the Registrars of California or the 100,000+ citizen poll workers who conduct our elections with honesty and conscientious dedication.

There is not one piece of evidence here that any voter in any election has had their vote compromised.

There is no smoking gun here.

The question of the legitimate use of California's voting systems is squarely before the Secretary of State.

There are five questions I would hope that the Secretary of State asks and answers as part of her consideration of these issues over the next few days:

1) Are there any factual inaccuracies in these materials?

2) Do any system procedures or county policies follow a prohibited or vulnerable practice?

3) Do existing security policy and procedures mitigate any identified threats, and if any do not, are there policies and procedures that can be implemented to address those threats?

4) Are there any good ideas in the materials that we have not thought of, and how can we incorporate them into our standards?

5) Based upon the materials presented, is there anything to warrant any drastic action by the Secretary?

I am very concerned that these materials have been released without presenting the obvious and legitimate answers to the proposed threats. Matt Bishop, one of the expert team leaders has written (op cit):

> "The moral is that one can never verify that a system has no flaws, even if all source code is available." … "Perfect voting systems do not exist. The goal is to build voting systems that are as good as possible." … "…these goals involve policies and procedures, as well as software assurance." … "…unless they are taken into account, reviewing only software may give a misleading idea of the security of a system."

California Registrars of Voters want to emphasize that we remain ready and willing to work to review and improve our internal and external policies and procedures for secure and proper handling of election materials. However, there is no reason to doubt the accuracy of California's voting systems.

SLW:ceb