Verifiedvoting.org

March 30, 2007

Secretary Debra Bowen
State of California
1500 11th Street
Sacramento, CA 95814

Attn: Voting Systems Review, 6th Floor
Submitted by email to: votingsystems@sos.ca.gov

Dear Secretary Bowen,

VerifiedVoting.org herewith submits to you our statement of strong support of the draft criteria circulated for public comment on voting system top to bottom review[1] in the State of California. We congratulate you and your team on taking this step to improve California's elections.

We include for your consideration some suggestions which we believe would strengthen the document. Please do not hesitate to contact us for further information or if you should have any questions.

Best regards,

Robert Kibrick
Legislative Analyst, VerifiedVoting.org

Pamela Smith
President, VerifiedVoting.org

[1] http://ss.ca.gov/elections/voting_systems/draft_top_to_bottom_review.pdf

1. Section I.1 (Security Standards):
"For the 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"*

This definition of "untraceable vote tampering" defines it with respect to "chang[ing] the result of the election", but does not define what it means by "the result". That phrase could be read in more than one way. For example, in a contest between two candidates, "Smith" and "Jones", assume that 200 voters cast ballots for Smith and 100 voters cast ballots for Jones. In the absence of tampering, the phrase "the result" of that election could be interpreted to mean:

a. Smith wins, or
b. Smith received 200 votes and Jones received 100 votes.

Since "untraceable vote tampering" is defined to occur only if it "change[s] the result of an election", whether or not such tampering is considered to have occurred may depend on how one interprets the meaning of the phrase "the result".

Now assume that tampering (leaving no electronic record) occurs, and 25 of the votes intended for Smith are diverted to Jones (i.e., Smith=175, Jones=125), leaving Smith the victor. If "the result" is interpreted as in case "a", then under the current definition, no "untraceable vote tampering" has occurred because "the result" of the election is unchanged. But if interpreted as in case "b", then such tampering is defined to have occurred because "the result" of the election has changed.

> **Recommendation**: To avoid ambiguity, modify this definition to replace the phrase "*the result of an election*" with the phrase "*the vote tally of an election*".

2. Section I.1.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 voter tampering or denial of service attacks by any persons 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."*

a. What does it mean to "*effectively secure*" a system against a risk, as opposed to ensuring that a system is "*secure*" against a risk? Is it necessary to include "*effectively*"?

> **Recommendation**: For clarity, we suggest eliminating the word "*effectively*" in this phrase, or restatement of the phrase to explain the distinction.

b. "*Access*" is not defined, and could be read in more than one way, e.g., direct physical access or indirect (i.e., remote) access, such as by means of a wired or wireless network connection.

> **Recommendation**: Restate the phrase so that it explicitly includes, but is not limited to, both such types of access.

c. The specified list of access opportunities: *"manufacture, storage, temporary storage, programming, testing, and use"* is somewhat incomplete.

Recommendation: Amend the list to read "manufacture, *delivery*, storage, temporary storage, programming, *configuration*, *upgrading*, testing, *repair*, *maintenance/servicing*, *transport*, and use".

The changes recommended under items "a" through "c" above should be applied not only to this section, but to each of the other comparable provisions in the other sections of the document.

3. Section I.1.b (Vote Tabulating Devices):
This section presumably applies to devices such as optical scan tabulators, and contains similar language to that provided for DRE voting systems in Section I.1.a above. However, conspicuously absent from the language for this section is a concluding phrase comparable to the one found at the end of Section I.1.a, namely:
*"... testing, and use, **including the electronic ballot definition or layout process.**"*

Since ballot programming errors or corruption are not only a very significant source of non-malicious mis-tabulations of optical scan ballots, they represent a significant vulnerability in terms of malicious vote tampering.

Recommendation: Include language at the end of this section to ensure that tabulator's ballot programming is itself secure against such tampering.

And, as noted earlier, the previously-described changes with respect to "effectively secure", "access", and the "list of access opportunities" should be applied to this section as well.

4. Section I.1.c (Ballot Tally Computers and Ballot Tally Software):
As noted earlier, the changes with respect to "effectively secure", "access", and the "list of access opportunities" should be applied to this section.

5. Section I.2.a (Red Teaming):

Recommendations:

a. The "list of access opportunities" (i.e., "manufacturing, programming, delivery, testing,..." etc.) should be amended as described for the previous sections.

b. Consistent with the justification provided under suggested change #1, change the end of the last line of this section from:
" ... or alter the record of votes to change the result of an election."
to read:
" ... or alter the record of votes to change the vote tally of an election."

6. Section I.2.b (Source Code Review):
At the end of this section, reference is made to "*the risk assessment*", but such a "*risk assessment*" has not been explicitly mentioned.

Recommendation: Change the end of this section from:
"... or after completion of the risk assessment."
to read:
"... or after completion of the 'red team' exercise."

7. Section II.1 (Disability Access Standards)

Recommendations: Include language to provide for the following:

1. The accessibility features (e.g., audio ballots) of DREs should be enabled at all times, and should not require special intervention by the poll workers (e.g., rebooting the DRE into a special accessibility mode) to enable those features.

2. Voters should have direct control over the blanking/un-blanking of the screen display at any time, and should receive audio confirmation of any change in the blanked / un-blanked status of the screen.

3. Any accessibility features that are adjustable by the voters (e.g., audio output levels and playback speed) should revert to reasonable default values at the start of each voting session.

8. Section II.2.a (Disability Access Testing, dual-switch input):
This section should also require that the use of the dual-switch input should not reduce or otherwise limit the choice of output modes (e.g., visual, audio, or both) by which the ballot is presented to the voter as compared to the choices provided when the dual-switch input is not used. For example, on the Sequoia AVC Edge II, use of the dual-switch input forces the voter to use the audio ballot, a restriction which should not be imposed on a sighted voter with a manual dexterity impairment.

Recommendation: Include language to support full choice of output modes (visual, audio, or both) for ballot presentation to any voter using dual-switch input.

9. Section II.2.b (Disability Access Testing, simultaneous and synchronized audio and video output, etc.):

Recommendation: To the end of this section, add the following bracketed text: "... or visual outputs only *[, regardless of the type of input interface (e.g., touch screen, keypad, dual-switch/sip-and-puff) selected for use by the voter*]."

10. Section II.2.d (Variable audio output levels and playback speed):
This section conflates two different types of accommodation intended for two different classes of voters. Adjustable audio levels are indeed intended for voters with hearing impairments, but adjustable playback speed may be useful not only to such voters (who might want to slow down the pace of the audio output) but for blind or visually-impaired voters, who may want to speed it up. Similarly, if the playback speed is to be adjustable, it should be pitch-compensated, so that it remains intelligible.

Recommendation: Change the language of this section to read:

"Adjustable audio output levels for voters with hearing impairments, and adjustable, pitch-compensated playback speed for voters with either hearing and/or visual impairments."

11. Section II.2.f (Non-visual verification of the VVPAT):
This provision allows the non-visual verification method to derive the information provided to the voter from either:

(1) the paper record copy (VVPAT) itself or
(2) the same electronic data stream used to print the voter verifiable paper record copy.

Option (2) provides no safeguard for visually impaired voters in the case that the printer fails to print the VVPAT, either because the paper jams or because some careless poll worker loaded the paper backwards so that the thermal print head tries to print on the non-sensitive side of the paper. In that sense, this option fails to alert visually-impaired voters of a condition that would easily be detected by sighted voters (at least those sighted voters who bother to look at the VVPAT), and thus put those voters at a disadvantage.

> **Recommendation**: Employ only option (1), as option (2) is not an adequate accessible solution.

12. Section IV (Usability for Elections Officials and Poll Workers):

In addition to establishing documentation requirements, this section ought to require voting systems to be designed to prevent poll workers from accidentally configuring the voting system in a manner that would prevent votes from being accurately recorded, either in the electronic ballot record or on the VVPAT. For example, one could require the voting system software to provide an "opening the polls procedure" in which the voting system prints a "printer test message" on the VVPAT and includes in that message a randomly-generated number (i.e., one that the poll worker could not guess and would not know in advance). The poll worker would then be required to read that random number off of the VVPAT printout and enter it on the touch screen before that DRE would be enabled for voting. Such a procedure would ensure that voting could not proceed on a DRE whose VVPAT printer had the paper loaded in backwards.

> **Recommendation:** Require vendors to implement effective designs and procedures to ensure that poll workers cannot accidentally misconfigure the voting systems in a way that prevents votes from being accurately recorded on the VVPAT.