March 28, 2007

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

Dear Secretary of State Bowen,

In response to your request for input on the Draft Criteria to guide the review of currently certified voting systems, the Voting Rights Taskforce (VRTF) of the Wellstone Democratic Renewal Club has gathered the following material for your consideration. These recommendations, questions, and requests have also been endorsed by the East Bay for Democracy. Both Wellstone and East Bay for Democracy Democratic Club are chartered Democratic clubs.

We thank you for all the election integrity work you have done so far and for your continuing efforts to make our elections secure. Please let us know if there is any way we can help support your forthcoming top to bottom review and to support as well any future election integrity activities.

Please address any questions or comments to: Voting Rights Taskforce, c/o Michelle Gabriel, 3800 Lakeshore Avenue, Oakland, CA 94610. Phone: 510-444-4370.

Sincerely,

Voting Rights Taskforce
Wellstone Democratic Renewal Club

Michelle Gabriel, Jim Soper and Jerry Berkman wrote this document with input from themselves and various VRTF members including Judy Bertelsen, Richard Tamm, RC, Jackie Riskin, Lucy Sells and Sharon Maldonaldo.

RECOMMENDATIONS

Additions or Changes to Current Sections

I. Security

A. The term "untraceable vote tampering" is mentioned throughout Section 1. For clarity's sake, we would suggest adding traceable tampering. As such, the amended phrase would read, "both traceable and untraceable vote tampering."

B. Under "Security Standards," we would like to suggest amending the last sentence of the first paragraph so that it reads "'Denial of service attack' means disabling a voting system." (The clause "other than through sheer physical destruction... inoperable for voting" could be removed.)

New Sections

The current draft criteria has four sections: Security, Access for Voters with Disabilities, Access for Minority Language Voters, and Usability for Elections Officials and Poll workers.

We recommend that two sections be added: Suitability for the Purpose Intended and Conditions for Performing Testing.

V. Suitability for the Purpose Intended per Section 19205a

"The machine or device and its software shall be suitable for the purpose for which it is intended."

1. The voting systems should support and facilitate manual tally and recount of the paper record and/or ballot.
    a. The difficulty of performing the manual tally and recount shall be evaluated.
    b. The time required to tally and recount shall be evaluated and determined if it is unduly burdensome.
    c. Accuracy in tally and recount criteria to include...
        i. ...Whether machine errors impair the ability to read the paper trail and
        ii. ...Ability to determine voter intent.

2. Since the manual tally and any further recounting is considered a security measure, any paper record marking, by human or machine, should be thoroughly tested for resistance to attack.
    a. Attack testing of machine marked paper records and ballots should include checking if regular voters in a mock election catch purposely introduced errors.
    b. Pre-marked optical scan ballots can be used to see if voters catch purposely introduced errors.

3. The voting system should be sufficiently reliable and rugged to perform in an Election Day environment.
    a. MTTF (mean time to failure) and MTBF (mean time between failures) shall be determined for printers and other mechanisms in mock elections using real poll

workers and real set up situations. The MTBF demonstrated during certification testing shall be at least 163 hours, per Voluntary System Guidelines 2005, Volume 1, page 100. NOTE: the MTBF levels should be reviewed to determine if it is acceptable or if the minimum should be raised.

4. The voting system should be accurate.
   a. VVPAT printouts should be errorless. Tallies and recounts must match 100%
   b. Optical Scan systems shall be tested for accuracy, including if a ballot is put in backwards or upside down, and still records the same results. (See Doug Jones and John Washburn, Arizona Study of Optiscan, for guidelines.)

5. The system should be shown to be secure for early voting.

VI. Conditions for Performing Red Team Testing

1. **Testers**
    a. The security testers need to be independent, which means they must not be employees of election equipment suppliers or members of the county staff that have now become "invested" in the current system.
    b. The security testers should be persons with unquestioned competence and experience in computer security.
    c. Mock elections under real conditions should be held, from beginning to end, including mock audits and recounts.
2. **System Hardware, Software, And Firmware to Be Tested**
    a. All equipment tested must be the actual equipment that the counties have used.
    b. Equipment must be pulled at random from county storage sites.
    c. The software on the county system must be confirmed to be the software in escrow that has been certified. If not....
        1. ...Follow up investigation will determine why.

        2 ...Software will have to be installed. This software should come from the Secretary of State's escrowed software and not from the vendor.

        Where COTS software is involved, the testers will install it on the test machines. The state will supply the software.

    d. Test mode must not be used for any of this certification review. Actual election mode must be used.
3. **Test Protocols**
    a. The whole system will be tested.
    b. Testers will use their own test plans, not plans provided by the Vendor.
    c. The testing team(s) may make multiple attempts at different parts of the system.
    d. The testers will know the version of the tabulator's SQL data base management system at least two weeks before the start of testing.
    e. The testers may use any equipment they wish to, including, but not limited to, laptops, card readers, EEPROM readers, etc.
    f. The testers may use video, photographic, and audio equipment and take notes.
    g. Any installation of software by anybody must be observed by a tester.
4. **Timing**
    a. The testers must set the date on the computer equipment to Election Day.
    b. The testers shall have a minimum of two weeks with the machines.

QUESTIONS

1. What is actually going to be tested? There is additional confusion because of the wording: the Draft Criteria's title says: "Electronic Voting Systems Certified" while the first paragraph says: "voting systems currently certified. DREs are explicitly mentioned, but optical scanners are not mentioned.

   a. Should it be made explicit whether optical scanners are or are not to be tested also? We are assuming that you will be reviewing optical scanners.
   b. Are access card enablers covered? And the access cards themselves? There were many failures of these also during past elections.
   c. Will the Automark be tested?

2. These criteria are specific to electronic voting systems. But will these criteria be extended to all voting systems? For example, will the Vote Pad be ineligible for certification in California if it does not have Sip and Puff capability?

3. The draft criteria include sections/tests for security, accessibility, and usability, but not sections/tests for ballot secrecy and accuracy. We have addressed the above recommendations for accuracy. Will you be covering ballot secrecy in your review?

4. Can you please clarify what are "standards" vs. "guidelines" vs. "requirements" and confirm that these terms are being used correctly and legally in the draft? For example, are the Voluntary Voting System Guidelines actual guidelines, or are they standards?

5. Can you please define "risk assessment" as used on Page 3. I 2. b. Source Code Review? Is a risk assessment or a certification review being performed?

6. The Elections Code states that the voter may verify:

   "the information that is contained on the paper record copy" (19250(d))
   "the information provided on the paper record copy" (19251(a))

via a nonvisual means. Yet, section II 2 f references an undefined "electronic data stream". Why would information from the electronic data stream be allowable, since that data stream is NOT the paper record copy?

7. Will there be a separate review of procedures?

REQUESTS

1. **Key attack point** areas were NOT tested by ITA testers and should be tested by the county. See Appendix B Brennan Center report, Software Attacks section.

2. Publication of results
There will be two reports. One, a complete report by the testing team, to be delivered to the vendor, the county, the SoS, and other relevant, responsible government officials at all levels.

Two, redacted reports shall be released to the public. Redactions should be kept to a minimum, and redactions should be permitted only to (a) protect the legitimate intellectual property of the vendor, or to (b) conceal any information whose disclosure could compromise election security.

The unredacted report should be published at least one month before the next certification hearing of the system, so that the public has an opportunity to make informed comments. The testing team may make recommendations for earlier publication of certain sections, depending on the severity of the vulnerability, and the risks involved.

The findings at the end of the process must make clear exactly how much source code review was done, as it may not be possible to have full source code review of all software in a timely manner.

3. Observation of Testing
The testing should be public, if possible. If that is not possible, in accordance with section 15004 of the California Elections Code, each political party may have present two qualified observers and any organization may have observers at any stage of testing. Observers may use video, photographic, and audio equipment and take notes. All testing should be videotaped in a manner for meaningful observation.

4. Confirmation of Federal Testing and Qualification

The systems that were qualified by the ITA Ciber, which was found to be doing insufficient testing, should be reviewed and retested to all of the Federal standards. The list of Federally qualified systems and software revision levels should be reviewed against what is currently in use in each county to determine that BOTH Federally qualified and State certified systems are in use.