

## **Review of the California Secretary of State's Conditional Recertification Directives for Sequoia Voting Systems**

*San Francisco Voting Systems Task Force, November 15, 2009*

*Investigators: Ka-Ping Yee and Jim Soper*

### **Notable items:**

1. Some recounting will be common, because a 100% manual recount is required for many ballots:
  - Ballots cast on an Edge Model I or II in early voting or on election day.
  - Ballots cast on any device prior to its removal from service due to broken seals or broken chain of custody.
  - Ballots cast on any device prior to being rebooted after a fatal error.
2. Firmware or software must be reverified after any repair that opens the housing of a voting system component.
3. Administrators must use three isolated EMS installations: one for preparation, one for tabulation, and one for erasing storage media.
4. End-of-day reports are to be printed and posted outside each polling place.

### **Relevance to VSTF scope:**

Items 1–3 above are identified as election administrator work items that could conceivably be facilitated through better designs or guidelines for voting systems. For example, systems could be designed to support the duplicate-EMS model, to facilitate the reverification of software, or to reduce the need to ever repair or open the housing of a component. Item 4 affects the transparency of the election.

### **Recommendations:**

1. The VSTF should review the DoE's manual counting and auditing procedures.
2. The VSTF should find out the "additional post-election manual count auditing requirements" that the SoS established per item #20.

### **Detailed summary:**

- This is a decertification, and conditional recertification. There are 41 conditions.
- Some of the conditions are Sequoia-specific.
- #1 requires 1 DRE with VVPAT per precinct. 1 backup machine, and/or 1 machine for creating voter access cards are allowed.
- In general, there are lots of security and chain of custody conditions (2). I will note some of them here:
  - Machines are to be reformatted prior to 2/5/08 election. All firmware & software must come directly from the office of the SoS, or the test labs. (3, 27, 28)
  - In general, whenever there is a breakdown, repair or modification of a system, the machines get reformatted with "known" firmware & software (7)
  - Use of duplicate Election Management Systems (4)
  - 2 election officials must sign many of the logs and other documents (12)
- Use as little software as necessary (8)
- No wireless, no modems (11)
- Voting systems are transported in uniquely serialized tamper-evident containers. 10 day "sleepovers" are allowed. (12)
- 2 end-of-day tapes, 1 posted outside the polling place. 1 audit log. (15)
- Escalating spot-checks will be developed by the SoS (20)

- 100% of all DRE VVPATS will be checked (21)
- Pollworker training shall include ... [it's complex] (23)
- Observers must be able to observe. Allows for 2nd monitor. (14, 22, 24, 32 [Observer panel])
- If a seal is broken, machine is taken out of service. 100% manual tally, etc. (27)
- If fatal error, machine is taken out of service. 100% manual tally, etc. (28)
- No modifications without OK from SoS (30)
- All voting systems must comply with Calif Elections Code & HAVA, and all required state and federal voting systems guidelines, standards, regulations and requirements. (35, 37)
- Vendor may not misrepresent their wares (36)
- SoS reserves the right to adjust or suspend any of the procedures or conditions (30, 31, 41)
- What is striking is that the vendor has a lot of responsibility (costs) for creating plans and procedures (5, 6, 9 [patches], 10, 12, 18 [spot-checks])
- Vendor pays for the spot checks (19)
- Vendor must provide copy of complete system to SoS if required (33, 39)
- Vendor must establish a California User Group, with annual meetings (38)
- Vendor must supply printing specs for ballots (40)

- Escalating spot-checks will be developed by the SoS (20)