

Approval of Proposed Sequoia Voting Systems California Use Procedures and Appendices, Subject to Specified Modifications

The Office of the California Secretary of State hereby approves the California Use Procedures and Appendices submitted by Sequoia Voting Systems, Inc., dated August 31, 2007, subject to the following modifications.

Appendix N

Appendix N.5: All Appendix Q provisions that are referred to in Appendix N.5 are mandatory, without regard to any descriptions in Appendix Q of certain of its provisions as “recommended.” The exceptions are the background check requirements in Q.7.1 and Q.7.2, which are strongly recommended.

Appendix N.12.1: After the vendor had drafted this provision, the Secretary of State revised the corresponding Item 12 of the Revised Recertification document issued on October 25, 2007, by adding the requirement that, “at a minimum, the Use Procedures must require the jurisdiction to secure all voting system components in one or more uniquely serialized, tamper-evident container(s) before the jurisdiction transfers them to the custody of an Inspector, other poll worker, drayage company or other intermediary, or before jurisdiction personnel deliver them to a secure polling place or secure satellite distribution facility, as the case may be. Transportation of voting system components to the custody of an Inspector, other poll worker, drayage company or other intermediary, secure polling place, or secure satellite distribution facility shall not occur earlier than 10 calendar days prior to Election Day. Electronic components of a voting system not transported back to the jurisdiction headquarters on election night must be secured in one or more uniquely serialized, tamper-evident container(s) and placed in secured storage. The Use Procedures must impose the same requirements for signed logging of the inspection of security containers and the removal and return of voting system components to security containers that apply to security seals and locks on the voting system components themselves. The following are examples of acceptable tamper evident containers:

- A uniquely serialized, sealed banker's bag;
- A zippered nylon or canvass bag or case on which the zipper(s) that prevent access to the voting system component(s) inside are kept closed by a uniquely serialized, tamper-evident lock; or
- A hard lid that blocks access to all doors, ports or other points of access to the inside of the voting system component(s) and that is held in place by a latch or latches closed with a uniquely serialized, tamper-evident lock or locks.”

Accordingly, Appendix N.12.1 is approved, as modified to include this requirement.

Appendix N.17.2: The second “bullet,” currently states that poll workers may not participate in any audits or recounts involving VeriVote Printer audit records. After the vendor drafted this provision, the Secretary of State revised the corresponding Item 17 of the Revised Recertification document issued on October 25, 2007, by adding the sentence: “Poll workers may participate in audits involving VeriVote audit records from

a precinct other than the one in which they were a poll worker.” Appendix N.17.2 is approved with the addition of this sentence.

Appendix O

Appendix O.6.10, “A Segregated Dual-Edge Architecture,” is an acceptable method for satisfying Item 4 of the Revised Recertification document issued on October 25, 2007. However, this is not the only method by which jurisdictions may comply. The Secretary of State has determined that the “shortcut” process described in the final paragraph of Appendix Q.3.1.1 is an acceptable *alternative* to the “Air Gap” method for preventing viral spread of malware in subsequent elections. This method involves taking an “image” of the hard drive when its operating system and applications are in a trusted state, before use to prepare for or conduct an election. The image is then reinstalled on the reformatted hard drive of the same server computer after it is used in an election and prior to the next election. Jurisdictions may employ the method described in Appendix Q.3.1.1 as an alternative to the “Air Gap” method described in Appendix O.6.10, “A Segregated Dual-Edge Architecture,” avoiding the need to deploy two separate AVC Edge 5.0 installations at county headquarters.

Appendix Q

Appendix Q.3.1: As required in Item 3 of the Revised Recertification document issued on October 25, 2007, “jurisdictions must reinstall all software and firmware (including reformatting all hard disk drives and reinstalling the operating system where applicable) on all election management system servers and workstations, voting devices and hardware components of the voting system.” The “pre-preparation audit” referenced in Appendix Q.3.1. is *not* an acceptable substitute for this one-time reinstallation. The reinstallation procedure described in the first three paragraphs of Appendix Q.3.1.1 is *mandatory* prior to use in the February 5, 2008 election.

November 29, 2007

Lowell Finley
Deputy Secretary of State
Voting Systems Technology & Policy