



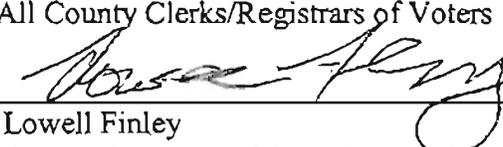
DEBRA BOWEN | SECRETARY OF STATE | STATE OF CALIFORNIA
OFFICE OF VOTING SYSTEMS TECHNOLOGY ASSESSMENT
1500 11th Street | Sacramento, CA 95814 | Tel (916) 653-7244 | www.sos.ca.gov

October 25, 2010

County Clerk/Registrar of Voters (CC/ROV) Memorandum #10303

TO: All County Clerks/Registrars of Voters

FROM:



Lowell Finley

Deputy Secretary of State, Voting Systems Technology & Policy

RE: Recount Regulations: County Security Measures Template

This is a follow-up to CC/ROV #10298, issued on October 14, 2010. The Secretary of State's Office has created the attached template that may be used as a guide to the recount security measures document as required by California Code of Regulations, Title 2, Division 7, section 20817. Section 20817(a) states:

The elections official shall, within six (6) months of the effective date of these regulations, submit to the Secretary of State written security measures for recounts to ensure the integrity of the recount proceedings. The security measures shall include, but not be limited to, chain of custody controls and signature-verified documentation for all voter verified paper audit trail paper copies, voted, spoiled and unused ballots, and all "relevant material" as described in section 20811(f). If submission by the vendor of a security plan to the Secretary of State is a condition of approval of voting system use, written notice to the Secretary of State of designation of that security plan to govern recounts satisfies the requirement of this subdivision.

These security measures are likely to be similar, if not identical to, the security measures employed on Election Day and during the one percent manual tally process conducted pursuant to Elections Code section 15360.

If you have not submitted your county's recount security measures to the Secretary of State, please do so as soon as possible but no later than Monday, November 15, 2010.

Counties conducting the special primary election for Senate District 1 must submit the recount security measures no later than Friday, November 5, 2010.

If your county has submitted this document to the Secretary of State's Office as part of a package of documents, please submit the recount security measures as a separate document.

CC/ROV # 10303

October 25, 2010

Page 2

All submissions can be emailed to Jason Heyes at jason.heves@sos.ca.gov. If you have any questions regarding this requirement you may contact Jason at the above address or at (916) 651-9163.

Attachment (1)

[Template]
_____ County Recount Security Measures

California Code of Regulations section 20817 requires California counties to submit to the Secretary of State written security measures for recounts to ensure the integrity of the recount proceedings. *(Name of County)* developed and submitted this document to the Secretary of State's office detailing the security measures that will be used in the event of an election recount. These security measures will be used in accordance with California Code of Regulations Chapter 8.1 titled Recounts and with county recount procedures.

1. Security Measures for Voted Ballots

Detail here how your county will ensure the security of voted ballots (e.g., chain of custody controls and signature verified documentation).

2. Security Measures for Spoiled and Unused Ballots

Detail here how your county will ensure the security of spoiled and unused ballots (e.g., chain of custody controls and signature verified documentation).

3. Security Measures for VVPAT

Detail here how your county will ensure the security of VVPAT records (e.g., chain of custody controls and signature verified documentation). If your county does not use a DRE voting system that produces VVPATs, please enter "Not Applicable."

4. Security Measures for "relevant material" as described in section 20811(f). "Relevant material" includes, but is not limited to, unvoted ballots, vote-by-mail and provisional ballot envelopes, voting system redundant vote data, ballot definition files, language translation files and the central database or other electronic repository of results for the election in which the contest subject to recount occurred, election data media devices, audit logs, system logs, pre- and post-election logic and accuracy testing plans and results, polling place event logs, precinct tally results, central count tally results and consolidated results in a structured, non-proprietary format, surveillance video recordings and chain of custody logs, including logs of security seals and access to election-related storage areas.

Detail here how your county will ensure the security of "relevant material" (e.g., chain of custody controls and signature verified documentation).

5. Any additional security measures your county takes to ensure the security and accuracy of a recount.

Detail here any additional recount security measures.