

## Dwight Shellman

---

**From:** Andrea Gyger  
**Sent:** Tuesday, October 08, 2013 3:44 PM  
**To:** Dwight Shellman  
**Subject:** Fwd: comments  
**Attachments:** VVF-CC Comments 10.8.13.pdf; ATT00001.htm

Sent from my iPhone

Begin forwarded message:

**Resent-From:** <[SoS.Rulemaking@sos.state.co.us](mailto:SoS.Rulemaking@sos.state.co.us)>  
**From:** Elena Nunez <[ENunez@commoncause.org](mailto:ENunez@commoncause.org)>  
**Date:** October 8, 2013 at 3:38:20 PM MDT  
**To:** SoS Rulemaking <[SoS.Rulemaking@SOS.STATE.CO.US](mailto:SoS.Rulemaking@SOS.STATE.CO.US)>  
**Cc:** Pamela Smith <[pam@verifiedvoting.org](mailto:pam@verifiedvoting.org)>  
**Subject:** comments

Hi Andrea,

Attached, please find comments on the election rules from Verified Voting Foundation and Colorado Common Cause.

Thanks,

Elena

Elena Nunez  
Executive Director, Colorado Common Cause  
(303) 292-2163 w | (720) 339-3273 c  
[@elenanunez](https://www.facebook.com/ColoradoCommonCause) | [@CommonCauseCO](https://www.facebook.com/ColoradoCommonCause) | [Facebook.com/ColoradoCommonCause](https://www.facebook.com/ColoradoCommonCause) |  
[CommonBlog/Colorado](http://CommonBlog/Colorado)

October 8, 2013

The Honorable Scott Gessler  
Secretary of State  
Department of State  
1700 Broadway  
Denver, CO 80290

**Re: Proposed Rulemaking Relating to Election Rules Recodification**

Dear Secretary Gessler:

Thank you for the opportunity to comment on Election Rules, Office of the Secretary of State, Notice of Proposed Rulemaking document dated September 26, 2013.

Verified Voting Foundation (“VVF”) is a nonpartisan organization that works to safeguard elections in the digital age. VVF believes the integrity and strength of our democracy relies on the citizen’s trust that each vote be counted as cast, and works to ensure that the means for verifying election outcomes are in place and are used for that purpose. Common Cause is a nonpartisan, nonprofit organization that is dedicated to restoring the core values of American democracy, reinventing an open, honest and accountable government that serves the public interest, and empowering ordinary people to make their voices heard in the political process. Both organizations believe that preserving the integrity of the voting process is critical to the achievement of their goals and to preserving a functioning democracy. We hope you find these comments useful, and we would be pleased to discuss any of these comments and suggestions further.

**1.1.16:** References an Electronic Ballot. As written, it does not appear to take into account that CO requires a voter verified paper record. It should be re-written to reference that important point, even if implementation of the requirement has not yet been completed for the whole state.

**1.1.37:** References "a voting system" and what that means. It should include, somewhere in there, a reference to that part of a system that transmits voted ballots. That would mean that Internet voting would have to be tested, among other effects.

**4.8.4 (B):** We strongly support the regulation allowing the county to add unique numbers to voted ballots after disassociation with the envelope for auditing and accounting purposes. This will help reduce workload for risk limiting audits.

**7.7.7 (b)(4):** There is a requirement to cease use of automated signature verification and notify the Secretary of State if the device fails an audit. It is not clear what would constitute “failing the audit” in this language, nor what will happen to the ballot envelopes processed by the failing device. Those ballot envelopes processed by a system that then fails its audit should be re-examined to ensure they were appropriately processed. A definition for “failing the audit” should be established and incorporated here.

**7.7.7 (c):** After first requiring that the system must be operated on a dedicated and secure network, the devices are allowed to be connected to the county network for maintenance and support, albeit with a requirement to be secured behind the county's firewall. Even if not connected during an election, malicious code could be introduced as a Trojan horse, left to hide until an actual election, and firewalls can be breached. To maintain the security of the system, requiring an air-gap would be preferable.

**10.19:** There is reference to recounting ballots by machine, and recounting by hand. It would be more useful to reference machine counting as "retabulation" rather than "recounting" because the methodology does not differ. As noted in a state by state database of recount rules on the site [www.CEIMN.org](http://www.CEIMN.org), they use "recount" as the term of art describing a manual count, not feeding ballots into a machine, whether the same one as originally used or a different one. We recommend the same protocol.

**11.4.2:** This section discusses affixing seals to equipment that has completed the L&A test. As is sometimes the case with seal protocols, however, there's no mention here of what happens if between the L&A test and the deployment of the equipment on Election Day, the seals appear to have been disturbed or broken. There is language that seems to fit in 20.13, but it should be at least referenced here.

**11.4.3, E and F:** CRS 1-7-514 indicates that the audit should compare manual tallies of the selected ballots with the "corresponding ballot tallies recorded directly by each such device in the original election tally." The rules here do not conform to that statutory requirement, in that a new count is conducted of a subset of ballots counted in the original tally. If the original tally were obtained on election night by counting sets of ballots in smaller batches, this would allow rules to be established that do not call for a recount prior to conducting the audit, and the audit could be carried out on the original count, as required by statute. We understand that these rules have existed in their current form for some time; however, we continue to believe that they are not in compliance with the requirements of Colorado law.

**11.8:** This section limits the purchase of accessible voting systems exclusively to those certified to 2002 federal standards. We understand that this standard is mandated by statute and that the Secretary can only require by rule that voting systems meet standards promulgated after January 1, 2008, which is problematic as no new standards have been adopted since that date. However, there are 2005 certification standards. While the Secretary may not be authorized to adopt such standards by rule, we believe the Secretary of State should encourage counties to purchase equipment that meets the highest standards, assuming those are, at a minimum, compliant with the 2002 federal standards.

**16.2:** No language is incorporated here, nor in any other section we could find, that would explain that electronic return of a voted ballot is only for use when another more secure means of return such as postal mail (or expedited return via express services made available through the MOVE Act) is unavailable. There's nothing here that would provide instruction to the UOCAVA voter nor to local election officials that sending a voted ballot via mail is extremely insecure. There's no mention of the provision that enables this method of return only in those rare circumstances when mail isn't available.

This section must establish a determination of what constitutes that emergency circumstance. Some states spell out this restriction by indicating that electronic return is allowed only for those in hazardous duty circumstances, combat situations, for example. Colorado adheres to the MOVE Act provisions of a 45-day window of opportunity for UOCAVA voting, and a voter can get their ballot instantaneously via electronic delivery, and Colorado accepts UOCAVA ballots up to 8 days post-Election Day if they were sent by Election Day. Thus the circumstances in which electronic return of voted ballots should occur should be minimal.

Return of the physical ballot marked by the voter should be encouraged. The election official should provide guidance that encourages the more secure means of return, including the expedited return provided for by the MOVE Act, which enables voters to track their ballots. Otherwise these regulations disregard clear language in statute that was designed to make elections and voting more secure.

**20.4:** There is no protocol noted here for what happens if a seal is broken or out of place. That gap should be closed. It appears to be covered in **20.13** but that should be referenced here. It otherwise appears as if there is no protocol.

**21.5.3:** This section calls for independent analysis of voting systems including penetration testing, etc. before certification. The vendor is required to provide the report. What determines if the tests were adequately conducted? This section should contain a clause that requires the test report to have been reviewed by the Colorado CIO's office. The CIO examines the SCORE system and conducts penetration testing on a variety of Colorado information systems. It's an in-house resource with expertise that could be brought to bear for voting systems. At a minimum they should review any penetration testing reports, as well as security plans that the counties have to prepare.

**21.5.8:** This section references the audit logs the voting system should be capable of recording and maintaining. An audit log should be a real-time, immutable, append-only log. This means that it shouldn't be possible to log anything other than in real time; that it should not be possible to erase or modify the information that has been logged; it should only be possible to append information. These requirements are not described here. There should be a means for protecting the audit log from accidental destruction as well. The system should use open file formats and be publicly disclosable. (This document prepared for the CA Secretary of State in 2010 by election technology expert Dr. David Wagner, UC Berkeley provides clear insights into what should be logged beyond the minimum, and may be useful. See p. 14 in particular.)

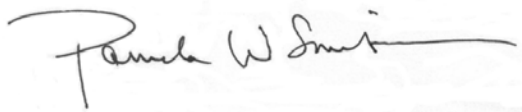
We also want to take this opportunity to address some issues that are not addressed in the rules, but that warrant the attention of administrators, advocates and lawmakers. We do not find any information here about new hybrid systems like an online ballot marking wizard system in use already in Colorado. Such systems present the ballot information to the voter, and generate audit trail information, and as such should be considered every bit as much in need of testing and certification as any other voting system device. Other systems which should be examined for functionality include ballot on demand printers and election night reporting systems if used.

An online ballot delivery and marking system presents a blank ballot for a voter. The vendor must be required to demonstrate how their system will ensure that the voter is receiving the correct ballot style presented with all the right candidate information, and tests should confirm such functional capabilities, just as they would for a polling place ballot marking device or voting machine. Further, there's no information about whether the voter is presented the opportunity to mark his/her ballot online. If so, there are myriad security and privacy implications that pertain, even if the voter prints the ballot after having marked it online and mails the physical ballot back. That voter's information is being rendered by a remote server that is typically not under the control of any election official, in order to set the information up for printing (or, capture in a PDF that can then be directly emailed without the voter ever having printed it). If there is a choice to just email it back, then this is really a fully electronic voting system (i.e. Internet voting system), with no voter-verifiable paper audit trail, and with the added hazard of traveling over public networks -- which locally cast or mailed ballots don't do. Before Colorado makes this leap, we urge robust public disclosure and debate about the known security risks at stake.

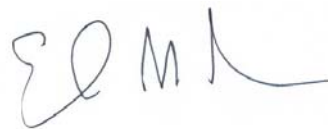
The more secure scenario for systems that provide a blank ballot to a voter is one where the voter marks the ballot manually after having printed it, or that s/he marks it via a resident program rather than an online system, and then prints it after having marked it on a client-side resident program (e.g. a fillable PDF can be presented to the voter which s/he then downloads and marks, and prints). This requirement was passed in California recently, preventing the use of online ballot marking wizards that have never been put to any federal scrutiny. Indeed, no federal standards have been put forward for such systems, and the use of such systems without having any way to secure them is very concerning. In California, in addition to the requirement that the ballots only be delivered blank to the voter with no online marking capability, any such system must be examined by the State before it is approved for use. Colorado should add such a requirement.

Thank you for the opportunity to comment on these proposed rules. If you would like additional information about any of the comments above, please feel free to contact us.

Sincerely,



Pamela Smith  
Verified Voting Foundation  
2777 Jefferson Street, Suite E-F  
Carlsbad, CA 92008  
(760) 434-VOTE w | (760) 613-0172 c



Elena Nunez  
Executive Director  
Colorado Common Cause  
620 16<sup>th</sup> St., Suite 300  
Denver, CO 80202  
(303) 292-2163 w | (720) 339-3273 c