Andrea Gyger

From:	Harvie Branscomb [redacted]
Sent:	Friday, June 06, 2014 4:50 PM
To:	SoS Rulemaking
Cc:	[redacted]
Subject:	rulemaking comments- conditions for use
Follow Up Flag:	Follow up
Flag Status:	Flagged

Amendments to Rule 20.5.2, regarding internal controls for the Voting System: 6

20.5.2 In addition to the access controls discussed in Rule 20.4,

Add after section (H) No one may transfer any portion of the election database or election related code to or from the developer or any other party during the course of the election including by transfer through flash memory, CD or DVD or any other media. This does not include reports and logs. [yes this has happened for the purpose of unlocking integrity locks built into the system]

--

Amendments to Rule 20.11.2: 17

20.11.2 Anonymity. The designated election official must implement measures to 18 protect the anonymity of voters choosing to vote on DREs. 19

(a) Measures to protect anonymity include: 20

(1) The county may not MAKE [not keep] any record indicating the order in which 21 people voted on the DRE, or which VVPAT record is associated 22 with the voter.

[note that these rules will help prevent problems I have encountered with anonymity violations but are not nearly sufficient to solve the anonymity problems.

There are many other solutions that need to be applied. For example, the holding back of about 10 ballots from each ballot style until all other ballots have arrived (8 days post) will insure that incremental vote counts will not expose personal voter intent.

Duplication can also be a source of anonymity violation. The requirement to match originals with duplicates by numbering them is a source of a violation if the duplication was doen to remove identifying material. In this case the duplicate should not be numbered.

Another case is when a certain ballot style is duplicated to remove some contest votes. In this case the best way to prevent the duplicate from being identifiable is to create a secondary ballot that contains vote marks to be subtracted from the vote totals. These special subtraction ballots need not be done in an identifiable way, but must be kept separate and whether or not counted by machine, subtracted from the vote totals rather than added. This way the original ballot can be included with the remaining ballots and remain anonymous.

SOS should provide rules to ensure that ballots are sorted and shuffled as soon as possible after the identifying attributes are removed. In fact sorting can be done while the envelopes are in place.

Sorting makes sure that any batch will not contain unique ballot styles that would interfere with anonymity. Counties with envelope sorters should be required or encouraged to sort by ballot style before batching. Some do.

--

20.17.3 ACCESS LOGS.

Logs of all kinds must be enabled- access, audit, system and all other logs. Often these logs are not activated and ignored. Electronic logs should be printed or otherwise made available so that any exceptions on them are noticed.

--

20.17.6 OPTICAL SCANNERS AS DEFINED IN RULE 21.1.13: 24

(A) WHEN ISSUING BALLOTS, THE COUNTY MUST PROVIDE...

Secrecy sleeves must be used for the purpose intended. Envelipes must be removed from secrecy sleeves at a location or at a point in time that is substantially removed from the location or time that the ballot is removed from the secrecy sleeve. Two different teams of at least two election judges should be used for the two separate actions and these teams must not be in direct communication. Ballot envelopes should be in substantial batches (at least 10) when envelope opening is performed and likewise for secrecy sleeve opening. Preferably the batches are recreated and shuffled while the ballot is in the secrecy sleeve.

--

(E) THE COUNTY MUST PROGRAM EACH OPTICAL SCANNER TO REQUIRE AN 3 OVERRIDE KEY FOR BALLOTS THAT ARE REJECTED BY THE SCANNER.

It is unwise to use an override function because one does not know how many errors are going to be affected or what mistakes will be made furing the override condition- the judges assume there is one error but there may be others unrecognized. The override turns off the sensitivity to all conditions that would have led to a rejection regardless of whether the election judges are aware of them or not .

There are much safer ways to handle this- such as (best) hand counting the rejected ballots, or (next best) put rejected ballots into Hart Ballot now or similar where all defects are potentially revealed to the operators by showing images of the ballot or (less best) duplication of rejected ballots before scanning again. Override is a very poor policy and it definitely leads to mistakes.

Requiring all scanners to have the override function is of course even worse. Please delete and rework this requirement so that errors do not creep into our election results unawares.

--

“Provisional ballots must be processed separately from non-conditional ballots - system subcomponents are unable to functionally differentiate and correctly process to Colorado specific requirements”

[this should say provisional envelopes must be kept separate. Once provisional ballots are released for counting they should be mixed in and not identifiable as such, else an anonymity violation usually occurs.]

--

(this portion from ESS but applies to all vendors sections:]

Software Condition 1(c) is deleted as unnecessary and redundant. The security and audit concerns addressed by this condition are currently covered by Section 1-7-514, C.R.S., and Election Rules 11.3-11.5, and 11.8, and proposed Election Rules 20.2-20.5, 20.7, 20.9, 20.11, and 20.13.

If this means that election night methods to create subtallies for each memory card are to be dispenses with, this is an outrageous misunderstanding of 1-7-514. The law requires and the audit technically to be meaningful requires a comparison of hand counts during the audit to the election night subtallies that are demonstrably added together to reach the published totals and match the outcomes. All of this must be checked, but in the relatively new rules the election night comparison is dispensed with, unfortunately. The good thing is that responsible conties ignore these rules and do the right thing with an audit of election night tally.

--

Sorry I ran out of time for comments at this point. The audit rules need serious reconsideration in light of best practices that are now well agreed to and published. CEIMN has published best practices for audits that Colorado would do well to examine and follow- even before the 2017 expected risk limiting audit.

Harvie Branscomb 6/6/2014

--
Harvie Branscomb
http://www.electionquality.com
[redacted]

Andrea Gyger

From:	Harvie Branscomb [redacted]
Sent:	Friday, June 06, 2014 5:19 PM
To:	SoS Rulemaking
Cc:	[redacted]
Subject:	One general comment as a post script to the rulemaking public comment opportunity
Follow Up Flag:	Follow up
Flag Status:	Flagged

To the rulemakers at SOS:

In my ten years of watching Colorado elections very closely I have seen our 4 vendors' systems put to the certification test by the SOS and all of them substantially fail. At that point the legislature over a two year process grandfathered in all of the systems in use in 2008 regardless of whether they were included in the certification test at all or whether they failed substantial portions of the tests (e.g. 30%).

The saving grace and hoped for remedy from blanket acceptance that ended the story of the Conroy v. Dennis case was embedded in the conditions for use that were quietly patched together and released without public comment. Among them were some guidelines for conducting audits that were not well thought out and some workarounds for physical problems.
Unfortunately the current rules that we are told replace these conditions for use are insufficient to provide technical credibility to our current election systems in front of a technically aware audience.
As much as one might wish it were true, the conduct of an election without complaint is not verification of accuracy.

The conduct of an election with substantial complaint also seems to provide nothing to resist the urge to claim credibility and manufacture confidence that is not based on verified facts and rational accountability. Broomfield 2013 is the most recent example.

Colorado continues to brag about its election system but the systems in place are not set up to reveal their flaws, and recognized flaws are quietly (and exasperatingly) worked around in the field, usually with a very compliant and agreeable set of friendly election judges around a very overworked DEO of whom none are likely to spread complaints or share their stories outside a very small and friendly club.

So very few of us know most of what is known to be wrong with our election systems. Perhaps even fewer understand how little the law and rules help us achieve accurate, reliable, secure, accessible, transparent, accountable elections. But there are some who do.

Broomfield proves that Colorado's system for sharing information about elections is defective. There is a chance that Broomfield's contractor with instructions from Broomfield will share a fraction of what was learned there, but history suggests that we will learn little or nothing from Broomfield even as it provided a great deal of information about flaws in election equipment, election procedure, election rules and election law.

The format of the pdf provided with this pre-rulemaking discovery was very difficult to respond to. I hope that it will be easier to handle in the future. I regret the loss of the conditions for use in principle, but the fact of the conditions were such that they were either insufficient or ignored.

Harvie Branscomb 6/6/2014

--
Harvie Branscomb
http://www.electionquality.com
[redacted]