

Subject: Comments on January DRAFT

From: "Harvie Branscomb"

To: voting.systems.task.force, coloradovoter, "joseph richey", "Angie Layton", "Kathryn Wallace", "Margit Johansson", "Richard Coolidge", scott.gessler, "Teak Simonton"

Date: 03/01/2011 07:19 PM

To the Voting Systems Task Force

The attached is my commentary on the January DRAFT document from the San Francisco Voting Systems Task Force entitled:

"Draft Recommendations on Voting Systems for the City and County of San Francisco" (visit <http://www.sfgov2.org/Modules/ShowDocument.aspx?documentid=155>)

Thank you very much for initiating and requesting broad public comment on a well intended and appropriately future looking document. It is a document that election jurisdictions across the country may benefit from.

Harvie Branscomb comments on San Francisco DRAFT recommendations

Edited 2/17/2011 and 3/1/2011

Submitted for consideration to: voting.systems.task.force@sfgov.org

regarding the following DRAFT:

<http://www.sfgov2.org/Modules/ShowDocument.aspx?documentid=155>

The draft makes clear that this report is not only to advise on immediate acquisition but in fact to expose intentions for future potential purchases over the long term. Clearly this document is not intended to be limited by the capabilities of existing equipment. The benefits obtained from this document will likely accrue to the public around the USA. Therefore I extend a strong compliment to the authors for this undertaking. It is essential that voting systems providers and writers of statutes become aware of and design for improvements that are not in the market today. In recognition of the potential importance of this document, I have contributed some very specific comments on portions of the text. Where I have quoted from the DRAFT document "Draft for Public Comment – January 2011" I have used strikeout to indicate suggested deletions and yellow highlight to indicate suggested additions.

Page 8 line 24... **Voting system reliability-susceptibility to external interference.**

The section is not about reliability- it is about susceptibility to intentional external interference.

Reliability is one of several quality criteria for voting systems about which little information seems to have been gathered beyond some original certification tests. Reliability more appropriately refers to the property that any selected individual instance of a system will perform as it is designed, or that any two such systems will act alike, or that any one such system will act consistently. Reliability is very different from accuracy and it is also different from susceptibility. All are important.

Note that the report makes statements about accuracy and confidence in the paragraph about what amounts to susceptibility. If the document really intends to talk about accuracy, it should be noted that if systems are in any way unreliable, they cannot be "accurate". If the systems are in any way susceptible, they may still remain accurate as long as that susceptibility isn't exploited.

Page 9 line 21 missing the word "is"

19 confirms the machine result. If a discrepancy remains after a second count, the audit team fills 20 out a Manual Tally Incident Report, which **is** reviewed by supervisors in charge of the canvass.

The procedure described is an interesting one- first a hand count for voter intent and then upon finding a discrepancy, a second a hand count intended to match the machine's capability to interpret. What isn't mentioned is that any discrepancy between the first and second hand counts is likely to represent a weakness of the voting system that deserves to be mitigated, particularly in a close election. Data about these discrepancies, once they are able to refer to individual ballots, are extremely valuable for improving the accuracy of vote counting equipment and procedures.

Page 10 - line 3. The conclusion "is not a risk limiting audit" may be correct but it isn't a very useful conclusion. If the audit seeks to replicate a perfectly operating machine, it will fail to give advice as to the correct outcome, as long as voter intent remains the standard for election accuracy. Note that there are relatively common means of expressing clear voter intent by marking paper ballots that cannot be interpreted by any known machine algorithm. In these cases, the voter intent must be evaluated by human cognition. The audit is often the only opportunity for this to occur. If the audit is limited by procedure to checking the machine's reliability, it will not fully serve to verify or add confidence to the outcome of the election. Therefore it is essential to place confidence in hand counts that attend to voter intent, and to back this up with excellent procedures.

Line 14: If such an audit is done in a manner that allows reconciliation of any discrepancies at the ballot level- comparing the actual ballot marks to the cast vote record, (even if the original discrepancies are detected in precinct and/or batch aggregated results) then the root cause of the discrepancy can be reported and used in a process to incrementally improve the accuracy of the election system. This is highly desirable and tends to offset an inherent tolerance of discrepancies that may be associated with a risk limiting audit of the typical not-very-narrow victory-margin contest.

Page 11 line 5: The finding regarding the Humboldt project is interesting but in the scope of possible audit alternatives, very incomplete and therefore unsatisfying. The Humboldt project exemplifies one of several approaches that involve access to cast vote records and photographic records of ballots or indeed ballots themselves that may have benefit whether these records are accessible by election officials alone, or alternatively the public at large.

Line 12: the finding is again true, but less than conclusive or informative - considering the broad definition of "risk-limiting audit" used in this document.

Page 11 - line 30: Existing pdf export formats and even some Excel formats used for exporting data can be extremely difficult to parse.

Page 12 line 8: It is not correct that each ballot must be marked with a unique identifier (whether or not this identifier is accessible to the voter). Some election audit systems that depend on individual ballots use the order in which the ballots are stacked as the means to pair ballots with their photographic image counterparts or their respective cast vote records. If this method is used, it is essential that the order not be the same as the order in which public records show the voters casting their votes (by whatever means).

Page 12 - line 15: As stated above, there are additional benefits to be obtained from attention to single ballots, other than lower levels of effort for "stronger confidence". Real feedback on ballot interpretation errors are easily obtained from the single ballot methods, and this feedback if directed appropriately can help improve the election system accuracy (for all elections using the same equipment or procedures).

Page 13 - line 10: A-Tallies of the results: including under votes and over votes from each precinct...

line 12: B-Text files of ~~cast ballot records~~ cast vote records, which are currently (and also confusingly) called "ballot image files":

"Cast vote records" is the syntax used on page 7 line 16.

Page 13 line 22: (2) the referenced paper makes the assumption that hand counting is an established accurate means for interpreting and accumulating vote counts good enough for both audit and for dependable certified results. And this ought to be the case. However, in at least one state where election audits have been used since at least 2006, Colorado, there is now a very low confidence in the accuracy of hand counts on the part of election officials including officials within the Dept. of State Division of Elections. This widespread lack of confidence among officials is likely caused by the very circumstances of and procedures used in election auditing where discrepancies found are often, if not almost always, attributed to human hand count error. The frequent if not consistent discovery of "hand count error" in audits where there is a continuous comparison to a machine count simply degrades confidence in and ability to perform accurate hand counts. Hand counts that are done for audit purposes can easily slide in accuracy because of the relatively harmless effect of conducting, poorly, a hand count while auditing. The worst side effect is some extra reconciliation and perhaps some more but equally inaccurate hand counting. The "risk limiting" aspect of the proposed audits actually might over the long term serve to further relax the necessity for accuracy in hand counts, except in rare close margin situations where the outcome will in fact change upon execution of a full hand count. When a contest outcome will actually depend on execution of an accurate hand count, election officials may no longer be prepared to stand behind the accuracy of these hand counts. This is a conundrum that requires attention in planning for future audits.

Page 13 - line 28- (4) The recommendation to make public the ballots or photographic images of ballots does raise issues that require full airing and resolution of the underlying public policy issues in a venue where the benefits can and will be measured and compared against the possible risks, and means to mitigate the possible risks considered and implemented.

Page 14 - line2 Recommendation 7 (public access) implies that recommendation 4-(academic access) is significantly more protective of data. One deduces from this that there should be at least three perimeters/levels of election data protection- the innermost level of access is allowed to accredited election officials (judges, watchers, etc); a mid-level allowed to "academics"; and an outermost for the public. The distinction being made between "academics" and "public" is a bit hard to grasp but may have some value in a transition towards more accessibility by the public. Election laws have long made the distinction between "election officials" and the "public". Modern methods of records retention and distribution have made it technically feasible to at least partially remove this legal and practical barrier. The question remains whether good public policy encourages the removal of this distinction between official and public or official academic and public for most cases of election records (all that are anonymous). In order to retain confidence in the effective anonymity of the ballots and privacy of the votes, before removing this legal barrier, the public must become aware of the benefits of transparency and the significance of any un-mitigated risks associated with it.

Page 14- line 4: The phrases "limit conflicts of interest, protect voter privacy, and discourage vote-selling." are appropriate descriptions of the subjects for this conversation- and there is

perhaps one other- “discourage attempts by members of the public to prove that their vote was incorrectly tabulated”.

Page 14 - Line 7- The announcement of an acquisition preference is highly desirable and those of us in smaller states are happy that anyone in California is providing useful advice to developers of voting systems. The description here is insufficient to guide the development of the optimal system, and might be misleading. The printing of a unique identifier mentioned here isn't necessary, and at least in some forms it is I believe contrary to California law, e.g. if the printed number is visible to the voter. A number that isn't accessible to the voter could be useful and would presumably be legal, but isn't necessary either. Here are a list of potential “acquisition preferences” that might be expressed:

- a) Exportability of a cast vote record (“ballot image record”)
- b) Exportability of a photographic scanned image of the ballot (conceivably only for election official use)
- c) Ability to add a watermark including a unique human and machine readable identifier onto a ballot after the ballot is cast, to be included in any cast vote record and photographic scanned image, if any
- d) Access via EML to all election data (except the scanned image in b) – but this is already covered by recommendation (10)

Page 14 - Line 14-15:

11-Announce an acquisition preference for voting systems that allow individual voters to verify their cast votes after the election and independently check the vote tally.

This wording suggests that a voter would be expected to be able to identify their own cast vote record. That seems too close to being able to prove the identity of their cast vote record- which produces an untenable situation in which voters may attempt to fraudulently claim their vote was mis-interpreted. Voters might even deliberately smudge the marks on their ballots in a close contest in order to be able to appear in court to make claims about what their voter intent was in a tight race. The better way to frame the above “preference” is this: “Announce an acquisition preference for voting systems that allow individual anonymous votes on individual contests to be verified by observation of the corresponding marks on paper ballots or their digital representations. In addition all the digital interpretations (cast vote records) should be available for independent accumulation to obtain a check on the vote tally.” Whether this verification takes place in public or not is a matter for a well informed public policy decision.

[In regards to the remaining sections, I have simply proposed strikeouts and alternative texts.]

Page 15 Line 18. The phrase “secret ballots” is an unfortunate choice of words and tend to be misleading. It appears in this huge sentence (that deserves to be subdivided):

Balloting Systems and Services: As the phrase is used in this Report and titles this subsection, refers to those technologies employed for the following uses of ~~secret ballots~~ anonymous ballots in a public election: producing ballots prior to an election, or on-demand during an election; delivering a ballot to a voter, either in person, or remotely for absentee voters; marking a ballot, whether manually marking a paper ballot, or digitally marking an electronic ballot, or using digital means to indicate ballot choices that are then represented on a printed ballot; presenting a ballot to be counted, whether remotely or in- person, or presented physically or digitally; and the actual counting of ballots.

[Recommend that, in general, the phrase “secret ballots” ought to be replaced by “anonymous ballots”]

Page 15 lines 30-34

“Under and over votes are reported to allow a cross check against the number of ballot pages for each contest.” Some CCOS devices retain “and could, potentially, export” ballot images and/or individual records of each counted ballot. Some CCOS devices reject ballots with ambiguous marks, while others provide a user interface for election officials to interpret the voter's intent and indicate how an ambiguous mark should be realized and recorded as a vote or non-vote. “All devices require the interaction and interception by resolution teams in order to accurately interpret voter marks and none of the devices at present can determine automatically which ballots require this review”.

p. 16 lines 1,2:

Some DREs include a printer that produces a physical copy of the ballot selections or a Voter Verified Paper Audit Trail (VVPAT). DRE are particularly time consuming, costly, and difficult to test, as it is almost impossible to test vote on a DRE with 100% accuracy. Reconciliation of any discrepancy is impossible without a video recording of the gesture of the test voter, taken from the perspective of the test voters’ eyes (parallax errors become significant here for touch screen technologies).

p.22 line 16-18:

2.2.6. CCOS devices should provide a user interface for election officials to locate all ambiguous ballot marks (not just under votes) and interpret them as needed, with full logging of every interpretation, said logs to be publicly available and entries in the log should be traceable by some means to the original paper ballot for auditing purposes.

P23 line 24: missing word “so” or “in order that”

P24 line 5: missing phrase “are used” and perhaps “from”- this line needs work

Line 9: trust that the **physical and** digital chain of custody has not been broken nor that any event has occurred that

Lines 11-14:

there are opportunities for fraud or error. The ~~difference between~~ **potential for discrepancies between** physical ballots and electronic version of the ballot data ~~it is~~ **such** that without proper system security ~~the~~ opportunities for fraud and error can be much greater in volume **and scope** and more precise in their intended impact and be harder to detect.

P24 line 27 (proposed additional comment). **It should be considered that often efforts to obtain the benefits of security stand as obstacles to transparency and the benefits to be obtained from easy access to data. Implementations of security must be designed with the public's clear interest in access to election data in mind.**

P25 line 28- here is an unfortunate reference to “ballot secrecy” in the TTBR that is mentioned above. This really ought to have been referred to “**ballot anonymity**”.

Although this phrase is in a quote from the TTBR, it merits a disclaimer- ballots are not inherently “secret”. It is the process of voting- the “ballot” when used as a verb- that deserves privacy. The ballot presumably (and as intended, practically) becomes anonymous upon separation from the voter.

P29 lines 2-3:

create a secure or trustworthy system. It is well settled that a perfectly secure system is an impossible goal because all software is **and all actions of personnel are** potentially fallible.

P29 lines 17-18:

Manual audits ~~remove the need to~~ **help mitigate total dependence on or** trust in the correctness and integrity of software.

P30 lines 31-32:

3. Digital images **of adequate spatial resolution and pixel depth** of each counted ballot, with a cast-vote record for each for which are made 31 available for examination

P31 lines 10-12:

7.2. Election management system features and reporting system features for recording and publishing both components of and results of logic and accuracy testing (e.g., **actions taken in testing of DRE**, test decks and test count results)

P31 line 26 (additional feature)

13. Logic and accuracy testing sufficient to insure conformance of each instance of hardware and software to a consistent test specification- to make sure that all instances are reliable.

P32 lines 12-13:

delivery, implementation, and use of the voting system. The goal is to achieve an accurate, verifiable, accessible, secure, cost effective, reliable, trustworthy, and maintainable system.

End of commentary.

Harvie Branscomb is a Canvass Board Member for Eagle County Colorado, and a Board Member of Coloradans For Voting Integrity (<http://cfvi.us>)