Citizens Oversight's Comments on Proposed CA SOS RLA Regulations

Ray Lutz, CitizensOversight.org

2019-12-10 V1
raylutz@citizensoversight.org

Available on the web: https://copswiki.org/Common/M1937

Please see section 5 for a list of key issues and key changes, however, please see the full comment which shall dominate.

A document showing specific changes to the regulations is also available.

1. Introduction

Citizens' Oversight led by Ray Lutz, has been working to understand and improve election audits and the ability of citizens to provide effective oversight of these audits. In the 2016 election, we[1] noticed that some counties, particularly San Diego and Los Angeles, were excluding approximately 40% of the ballots from being included in the 1% Manual Tally Audit, as defined by Election Code 15360. We asked San Diego to include eight additional batches of ballots so as to properly audit the "later" Vote-by-Mail (VBM) ballots[2]. This would have cost San Diego County about $3,200, based on the approximate cost of $400 to audit a single batch. San Diego County refused and instead fought the notion that the later VBM ballots should be included in the audit. After the three-day trial, San Diego County lost and would be required to include those ballots in subsequent elections.

The math requires that including all, or nearly all ballots, in an audit is necessary to prevent the possibility of confirming an incorrect outcome, especially if the ballots belong to an identifiable group and are numerous, as in San Diego where 285,000 later-VBM and provisional ballots were being excluded from the audit.

---

[1] "We" includes the many volunteers who helped to monitor the election audits in California and in other states that conduct audits.

[2] The "Later VBM Ballots" are those that were not fully processed by election night, and comprised about 40% of the ballots in the 2016 election, in 723 batches. Eight additional batches would have satisfied the clear text of the 1% manual tally law, Election Code 15360, which stated that 1% of precincts and Vote-by-mail ballots would be manually tallied.

The County appealed the case. Realizing that we would prevail, San Diego County and the California Association of Clerks and Elections Officials (CACEO) being led by Los Angeles Registrar of Voters (ROV) Dean Logan, covertly modified AB-840, which was initially about signature verification and not related to audits, so as to allow the omission of the later VBM ballots. Their point of view that omitting 40% of the ballots from the audit was a good idea was based on the false notion that including just a portion of the ballots in the audit would allow the results to be extended to the excluded ballots. This change was also unfortunately endorsed by the CA Secretary of State (CA SOS).

AB-840 was approved largely because the legislature did not understand the fact that it would gut the effectiveness of the 1% manual tally audit. Despite the mathematical fact that any audit that conducts sampling must include all or nearly all the ballots in the scope of the random sampling process, the approval of AB-840 allowed reversal of the decision from the lower court, and disallowed attorney fees even though we had won the case based on the law in effect at the time.

This history provides a backdrop to the current actions where the CA SOS is attempting to draft regulations to implement Risk-Limiting Audits (RLAs), while faced with the fact that RLAs are difficult to apply comprehensively. To do so means they are cutting some corners and this comment will provide a counterpoint and alternative direction for auditing our elections so it can be done in a reasonable time, yet also be comprehensive.

2. Background

AB-2125 "Election Results: risk-limiting audits." was passed by the legislature and signed into law on Sept 29, 2018[3]. The law authorizes the use of risk-limiting audits in lieu of the 1% manual tally beginning with the March 3, 2020 statewide primary election, and requires that the Secretary of State adopt regulations to implement and administer risk-limiting audits.

The Secretary of State has drafted proposed regulations regarding risk-limiting audits and has circulated these for comment. The proposed regulations are open for public comment until Dec 10, 2019.

The following link contains the notice from the CA SOS:
https://elections.cdn.sos.ca.gov/ccrov/pdf/2019/october/19110rb.pdf

The following link contains the text of the proposed regulations:
https://admin.cdn.sos.ca.gov/regulations/proposed/elections/audits/audits-proposed-regs.pdf

[3] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB2125

Key Points of AB-2125, the Risk-Limiting Audit Law

2.1. Risk-Limiting Audits may optionally be used starting on March 3, 2020

> 15367 (a) (1) Commencing with the statewide primary election held on March 3, 2020, the elections official conducting an election may conduct a risk-limiting audit in place of the one percent manual tally required by Section 15360 during the official canvass of any election in accordance with the requirements of this article.

2.2. No Contest is excluded from the risk-limit audit law

Election Code Section 15360 defines the existing 1% manual tally. It requires that all contests are audited to some extent.

> 15360 (a)(1)(B)(i) In addition to the 1 percent manual tally, the elections official shall, for each race not included in the initial group of precincts, count one additional precinct. The manual tally shall apply only to the race not previously counted.

SImilarly, AB-2125 specifies that the counties shall conduct a risk-limiting audit on "each contest fully contained within the county's borders, and partial risk-limiting audits for each cross-jurisdictional contest."

> 15367 (2) <u>Participating counties shall conduct a risk-limiting audit on each contest fully contained within the county's borders, and partial risk-limiting audits for each cross-jurisdictional contest.</u> Commencement of the audit and selection of ballots for the audit shall not occur before the reporting of the results to which the contests are being audited. The Secretary of State shall define in regulations how all ballots, including provisional ballots and vote by mail ballots whose status has not yet been resolved, shall be taken into account in the audit to ensure that if a full manual tally of the votes on all validly cast ballots would show an electoral outcome that differs from the reported outcome, there is at most a five percent chance that the audit will not require such a tally. [4]

According to references on the meaning of words, the term "each" and "every" are interchangeable in meaning, where each is used when the items are individually countable whereas every is used for a group. Dictionary.com[5] defines each as follows:

---

[4] Underlining added.

[5] https://www.dictionary.com/browse/each?s=t

> every one of two or more considered individually or one by one:
> *each stone in a building; a hallway with a door at each end.*

Thus, it is clear that the risk-limiting law 15367 specifies that no contests would be left out of the audit, just like the 1% manual tally.

This is further underlined by the stated purpose of the provisions added by AB-2125 (underlining added):

> 15365. The purpose of this article is to provide election officials with a method to conduct a comprehensive verification of election outcomes through the post-election audit process.

Clearly, if the method is to provide "comprehensive" verification of election outcomes, it must not exclude contests within that election. We should also add that the key difference between the 1% Manual Tally and the RLA law is that the intent of RLA audits is to verify the outcomes, not just check that a few batches match the computer report. "Verify" implies that the process will be mathematically robust so that there is only a 5% chance that the outcome of each contest is incorrect.

2.3. AB-2125 mentions only Ballot-Polling and Ballot-Comparison audits, and neglects to mention Batch-Comparison risk-limiting audits

Although there are three normally recognized types of risk-limiting audits that use statistical sampling, ballot-polling, ballot-comparison and batch-comparison, AB-2125 does not explicitly mention the batch-comparison audit, which is similar to the 1% manual tally and where procedures are similar to those already in use by counties in California.

> 15367 (3) An elections official is in compliance with this section if the elections official conducts a ballot-level comparison audit, or ballot-polling audit, with a five percent risk limit or a risk-limiting audit with a five percent risk limit using another method for conducting risk-limiting audits as approved by the Secretary of State.

We recommend that any county that considers implementing an RLA should consider using a batch-comparison risk-limiting audit.

Therefore, the regulations should define and allow counties to implement a batch-comparison risk-limiting audit.

2.4. AB-2125 Provides that the Secretary of State establish regulations to implement and administer the risk-limiting audits under the law

The law requires that the regulations establish:

- audit boards,

- criteria for public education on risk-limiting audits,
- procedures to ensure the security of the ballots,
- rules governing cast vote records and other data involved in risk-limiting audits
- calculations and methods to determine when the audit is required to escalate or when it is considered complete.
- procedures and requirements for testing and disclosing algorithms for the selection of ballots to be included
- content of the risk-limiting audit report, to be published with the official canvass of the vote.
- procedures and requirements to ensure that the audit process is observable and verifiable by the public, including providing methods used to select samples and calculate the risk, and verify that the correct ballots were inspected during the audit, and allowing the public to confirm the voter's marks on the ballots.
- that elections officials must provide a 5-day public notice of the time and place of both the risk-limiting audit and the selection of ballots to be used in the audit.

We note that there is no mention that the regulations would include methods for selection of contests to be included because the law already says that "each contest" would be audited, again meaning that every contest would be audited.

2.5. Election Code 15366 Defines "Ballot"

AB-2125 established Election Code section 15366 which defines the term "Ballot" to mean:

- original, voter-verifiable paper ballots
- including voter-marked paper ballots marked manually (hand-marked paper ballots)
- ballot-marking device-marked paper ballots
- VVPAT (voter-verifiable paper audit trail) from DRE (direct recording electronic) machines
- not electronic versions of ballots
- not digital images of ballots
- not paper printouts of ballot images
- not digital cast vote records

One of the goals of this document is to develop the comment that this definition is too restrictive.

In 2012, California adopted regulations that require state agencies to employ a trusted system for maintaining all electronic records created or stored as an official record. The State of California defines a trusted system as, “a combination of techniques, policies, and procedures for which there is no plausible scenario in which a document retrieved from or reproduced by the system could differ substantially from the document that is originally stored.” (Source: California Government Code 12168.7(c))[6]

The CA SOS Electronic Records Guidebook[7] explains that agencies that wish to destroy paper documents and rely solely on electronic versions will need a trusted system in place. A trusted system certifies that electronically stored information (ESI) is an authentic copy of the original document or information.

Given that the CA SOS embraces electronic documents that are created by "trusted systems" to be equal to the paper originals in all facets of commerce, digital images of ballots should be afforded similar stature, if such "trusted system" status could be established. We have developed a draft standard entitled "Securing Digital Ballot Images to Enable Auditing"[8] which has been submitted to the NIST Election Cybersecurity Working group, and is submitted with our comment to become part of this record on the proposed regulations.

Therefore, the term "ballot" should include ballot images that are created with trusted systems.

3. Information about "RLAs"

Everyone wants elections that produce outcomes that reflect the intention of the voters and maintain voter confidence. The CA SOS and election officials gutted the 1% manual tally by passing AB-840 so that it can exclude all later VBM ballots from the audit. Now, "Risk-Limiting Audits" (RLAs) are a possible way forward. These audits are based on statistical sampling and they can limit the risk which occurs due to sampling error by increasing the number of ballots included in the sample. But because of sampling, sometimes a contest that was modified either by an attacker, mistakes or computer error will not be detected even though the true outcome is different from the official results.

Our organization took a particular interest in RLA audits and strove to fully understand them. To this end and with my background in engineering and software development, a Monte Carlo simulator was developed so we could run thousands of fictitious audits on given elections and

---

[6] "Trusted Systems" in the CA SOS Electronic Records Guidebook https://www.sos.ca.gov/archives/records-management-and-appraisal/electronic-records/electronic-records-guidebook/trusted-systems/

[7] https://www.sos.ca.gov/archives/records-management-and-appraisal/electronic-records/electronic-records-guidebook/

[8] https://copswiki.org/Common/M1936 -- "Securing Ballot Images to Enable Audits"

see how they would perform in theory[9]. What we have found is that RLAs, if implemented properly, could audit at least 90% of contests in elections without resulting in a time-consuming and difficult full hand count. But the remaining 10% of contests are the ones we are most interested in -- the ones with close margins of victory.

We see that there are clearly four key issues with RLAs. To fully explain these issues, we have published the white-paper called "The Four Fatal Flaws of RLAs," which is included with this comment document and fully incorporated as part of this comment[10]. We find these flaws to be so severe that we recommend that election officials continue to implement the 1% manual tally.

But, if they are interested in improving the coverage of that audit, they may want to implement it as a batch-comparison RLA, which will normally require about 14 batches to be audited regardless of the size of the district using them. Thus, in Los Angeles, this could be a big benefit, but in almost all smaller counties, this will be a big increase in the number of batches subject to the manual tally process. This is an estimate and the exact number will depend on the size of precincts and batches.

As a result of our investigation into the auditing landscape, we have concluded that the best way to balance all the issues is to use an independent ballot image audit, which will fully audit the election with single-ballot precision while still auditing some paper ballots using a limited RLA. It will give election officials and the public much higher confidence in the election outcome while avoiding the "full hand count" threat that could occur in any election with margins down to the ballot. We have proposed a method of securing ballot images[11] using the "trusted system" concept which is already embraced by the CA SOS for all other financial transactions and legal documents. Our proposal has been submitted to the Election Cybersecurity working group of NIST, the National Institute of Standards and Technology.

Maryland utilized ballot image audits and has compared them with batch-comparison and ballot-comparison audits, and they find that there are distinct advantages to performing ballot image audits[12]. A number of other jurisdictions, including Leon County, FL and Wakulla County, FL have used ballot image audits.

4. Comments on the Proposed Regulations

To make it easy to process these comments, we not only provide our comments in narrative and persuasive form here, but we have also generated a set of proposed changes to the regulations.

---

[9] White Paper: Election Audit Strategy and BRAWL -- Balanced Risk Audit with Workload Limitation -- https://copswiki.org/Common/M1879

[10] Four Fatal Flaws of RLA Audits -- https://copswiki.org/Common/M1938

[11] Securing Digital Ballot Images to Enable Auditing -- https://copswiki.org/Common/M1936

[12] Powerpoint Presentation by the State of Maryland comparing auditing methods. https://copswiki.org/w/pub/Common/M1915/Maryland%20Clear%20Ballot%202018.pptx

4.1 -- 20111 Definitions

4.1.1 Add Definition for "Batch-Comparison Risk-Limiting Audit"

The regulations should define the "Batch-Comparison Risk-Limiting Audit". The text is proposed as follows:

> (m) "Batch-Comparison Risk-Limiting Audit" shall mean an audit where batches, such as precincts or mixed-precinct VBM batches, are drawn randomly and weighted by Maximum Error Bound. Each batch is tallied similar to the 1% manual tally, and all ballots shall be included in the scope of the batches that can be chosen. The number of batches required are determined by statistical calculations, assuming a maximum vote change per batch of 40%.

As it turns out, if an attack which altered the outcome could be hidden in as few as 20% of the precincts in the election, auditing 14 random batches would be sufficient to reduce the sampling risk to less than 5%, assuming all batches have equal size.

4.1.2 Add Definition of Ballot Image Audit

We suggest that due to the risk that an RLA may become infeasible to complete within the certification period, election officials be given the option to amend their audit using a ballot image audit. Also, we do not support the notion that not all contests will be included. However, we understand the desire of the SOS and elections officials to limit the workload to complete these audits. We have concluded that doing ballot image auditing is a viable approach to improve the coverage of the audit while still performing a limited RLA of selected important contests.

> (n) "Ballot Image Audit" shall mean an optional additional audit that can be combined with an RLA so as to avoid a full-hand count and more fully cover contests not included in the RLA in the selection process. In this process, images of all ballots are exhaustively re-tabulated down to precision of a single ballot by an independent third party. Such an audit does not replace the RLA but can be used to allow election officials to review and recount the ballots by an independent third party auditing service should the sampling process fail to sufficiently limit the sampling risk.

With Ballot Image Audits, the most common hacking and error scenarios are detectable with 0% sampling risk even without image validation. For example, if the tabulation were to be modified, if voter intent was incorrectly evaluated, or if there are common systemic machine errors after the images are created and secured, these are all detected by a ballot image audit without image validation. The single weakness that would require that paper be inspected is if the

images are modified after scanning in but prior to securing them. This risk step is identified as C2 in the companion comprehensive risk analysis paper[13] and is mitigated by image validation.

4.2 -- 20112 Audit Types

4.2.1 "Audit Tool"

This section includes text regarding the use of an "audit tool"

> An elections official conducting a risk-limiting audit shall use an RLA software tool provided by the Secretary of State...

This should not be included in this section on audit types.

Furthermore, we object to the use of any DRE-like auditing software which provides for the direct entry of the vote into the software, and not providing a paper audit trail which can be verified by the auditing team and the public. Instead, the auditing team should tally the vote directly to paper forms, which can be easily scanned to produce a record of the tally of the vote from the sampled ballots. These can be later reviewed by the public to verify the audit. The tally sheets used in audits should be standardized by the CA SOS. Citizens Oversight has developed a proposed draft standard: "Uniform Audit Tally Sheets."[14]

4.2.2 Additional Definitions

The secretary of state should include additional definitions, as follows:

4.2.2.1 Batch-Comparison Risk-Limiting Audit Definition

> (c) A batch-comparison audit where precincts or mixed-precinct batches are hand-tallied and compared with the computer report with a five-percent risk limit, based on a maximum expected vote change per batch of 40%, or assuming that as few as 20% of the batches could be affected in any attack.

4.2.2.2 Batch Image Audit Definition

> (d) A ballot image audit may be used to augment the risk-limiting audits, particularly when the margin of victory is less than 2% for ballot-comparison audit, and less than 10% for a ballot-polling audit, and the number of ballots required in the statistical sampling procedure will become infeasible to complete within the canvass period.

---

[13] Comprehensive Risk Estimation in Election Audits -- https://copswiki.org/Common/M1913

[14] https://copswiki.org/Common/M1939 -- "Uniform Audit Tally Sheets"

4.3 -- 20113 Audit Initiation

This section introduces the notion of two types of audit,

- A single-phase audit, which is conducted only after all ballots have been cast and tabulated
- A two-phase audit that can be started before all the ballots have been tabulated.

The issues we have with this approach is covered in the section on Reg. Section 20122, where the two-phase audit is further defined.

4.4 -- 20114 Selection of Contests

4.4.1 Objection to Auditing Only Three Contests

This section provides that only up to three contests will be audited within each county. We object to this section because:

- It is not legal. The notion that only three contests will be audited is in violation of election code section 15367 (2):

  > Participating counties shall conduct a risk-limiting audit on each contest fully contained within the county's borders, and partial risk-limiting audits for each cross-jurisdictional contest.

  As well as other reasons as specified in section 2.2 of this document. Also, please see "The Four Fatal Flaws of RLAs" document, Fatal Flaw #2.

- This provision selects the contests randomly, with no attention to the consequence of the contests. What happens in practice is that contests which are of low or no consequence, such as advisory contests, contests with only one candidate, and judicial yes/no contests, will be selected instead of very consequential contests, such as the presidential contest, congressional seats, mayoral races, etc.
- This provision selects contests without any attention to the margin. Of course, contests with close margins should be audited rather than contests that are landslides.
- If only a few contests are selected, it renders the 5% risk limit to be moot, because the risk of selecting a contest which has not been attacked dominates. For example, if there are 10 contests with equal consequence, choosing just one results in a 90% risk, and 10% confidence. If a 5% risk limit based on the sampling error is then applied, then this decreases the confidence by 5% of 10%, or 9.5%, and thus a 90.5 confidence. This method flies in the face of the intention to result in a risk-limit of 5%.

4.4.2 Prudent Reduction of Contests for RLA Audit

We understand the desire to reduce the workload required for performing RLA audits. In the current proposed regulations, three contests are chosen for the RLA, and there is no consideration to any other in terms of whether sufficient ballots have been sampled to reduce the risk to any given level. Then, for contests that do not have any ballots at all included in the sampled ballots, one batch is manually tallied according to the rules of the 1% manual tally audit, per Election Code 15360.

This is not a comprehensive implementation of RLA audits and has no rigorous statistical support. But we understand the desire of the SOS to want to limit the scope of the audit to limit the workload required.

We can support reduction in the scope of the audit and to turn to an auditing method that does not explode into a full-hand count if the margin is very tight. Our recommendation is to use a Ballot Image Audit (BIA) performed by an independent third party where all ballots are retabulated based on the ballot images, and where the ballot images are produced within the "trusted system" paradigm already endorsed by the CA SOS, and secured using the best in cybersecurity technologies.

Then, a limited RLA audit can be performed on random contests but weighted by consequence and margin. auditing the hand-marked paper ballots with a limited RLA will detect a compromised vendor if the contest selected for audit happens to be the one subjected to the RLA audit.

In this case, we support the use of just a few contests selected using a weighted random selection technique. The contests should be weighted as follows:

- First, according to consequence. All contests that have no opposition (one candidate) or advisory contests with no immediate consequence should be eliminated from review, including advisory judicial (yes/no) contests. Consequence can be estimated by weighting contests according to campaign funding levels.
- Second, according to margin, where tighter margins have a higher weight.

4.5 --20115. Audit Board Selection

This provision provides for the selection of audit boards to perform the audit. We support the general notion of this provision and it should be used for all audits, including the 1% manual tally audit.

4.5.1 -- "Multiple Audit Boards" is not clear

The provision says that the election official can appoint multiple audit boards, and that "only one audit board shall evaluate each ballot." But there is no limit to the size of an audit board. And it may be very time consuming if there is a manual hand count.

So we believe this should be rewritten to provide that the audit board provides oversight and adjudicates voter intent in cases where there is a dispute. Other workers can perform hand tallying and data entry.

4.5.2 -- Agreement should include agreement to be video recorded

The Audit Board may be video recorded; therefore, the agreement should include a statement that they can be video recorded in their public role.

4.6 -- 20116. Public Education on Risk-Limiting Audits

We request that the CA SOS specifically address how they are planning to resolve the issues broached in the document, "The Four Fatal Flaws of RLA audits."

4.7 -- 20117. Ballot Manifest and Ballot Handling

4.7.1 Does not sufficiently define how the manifest is created

This section proposes that a ballot manifest be generated "independent of the voting system." We submit that this provision makes ballot manifest creation very difficult and that it is essentially infeasible to actually comply with the notion of complete independence, but it also depends on what the definition of "voting system" is.

Therefore, the method for creating the manifest must be defined.

For example, in an audit that requires that each ballot be identified with a unique identifier so it can be accessed, this could be applied typically by the scanner outfitted with an imprinter so the physical ballot can be imprinted. That means the number as provided in the manifest is actually supplied by the scanner. Is that part of the voting system? It seems that it is, and therefore, there is dependence on the voting system.

Is the concept here that all ballots will have to be hand-counted because we do not rely on the count supplied by the voting system?

In essence, we do not believe the concept that the ballot manifest has to be independent is feasible, nor does it provide any benefits. Instead, the audit should rely on a second phase, which is reconciliation with the Poll Lists, which we can define as the list of all voters who voted

at polling places and returned VBM ballots. Then, the counts in the Cast Vote Record are sufficient to serve as a ballot manifest.

4.7.2 Manifest Format not available for review.

Paragraph (b) says " The format for the ballot manifest shall be in the format required by the RLA software tool in the California Post-Election Risk-Limiting Audit Ballot Manifest Format document dated October 15, 2019, which the Secretary of State shall post on its website."

We performed a search for "Ballot Manifest Format" and found no document posted on the CA SOS website, so we cannot review or comment on the format.

4.8 -- 20118. Chain of Custody

4.8.1 Should define procedures here and be subject to public review.

This provision provides that "the election official shall establish written procedures to ensure security, confidentiality, and integrity of the ballots, cast vote records, or any other data collected, stored or otherwise used pursuant to this section."

We object to the CA SOS delegating these important procedures with only 5 days notice to the public. The availability of information to verify and validate the audit is a very important issue which we believe should be set by the law or CA SOS regulations and be subject to public comment and discussion. All data that is produced in the course of processing the election is public information unless explicitly restricted by law.

4.8.2 Security seal procedures must be standardized.

Tamper evident seals are only as good as the procedures used and the associated documents kept with follow-up if evidence of tampering is noticed. ISO 17712:2013 "Freight containers — Mechanical seals" is an international standard which sets standards for tamper evidence and strength when the seal itself is to provide resistance to tampering.

Since only tamper-evidence is the type of seal being specified, additional procedures are required, such as:

Ordering:

1. Ordering security seals, should always be the responsibility of one designated person in a district.

2. All orders for security seals should come from one centralized location in a district.

3. Seal manufacturers should ship security seals to one specific location in the district.

4. Security seals should be laser marked with a marking and number series unique to the district that uses the seals.

5. Utilizing color coding or location coding is an ideal method to identify different districts.

Security seal inventory:

Security seals should always be kept in a secure area where only authorized personnel will have access. This will prevent fraudulent use of security seals. A log book of “seal release” must be kept.

OUTBOUND SECURITY SEAL LOG BOOK

Maintain one log book for outbound seal recording and a separate log book for inbound seal recording.

The outbound security seal log book should contain the following information:

1. Date and time of seal application.

2. Container number.

3. Name of the authorized person applying the seal.

APPLICATION OF THE SEAL

1. All seals must be applied according to the instructions of the manufacturer, and a designated employee must check the seal application.

2. To insure a correct seal application, always check the seal application by pulling the box flap or seal locking mechanism

ENTRY PROCEDURES

A. As containers are received by the elections staff, a staff member will record the following information.

1. Container number.

2. The seal’s number, color and coding.

3. The person who is delivering the container's identity.

4. Date and time.

UNINTENDED BREAKAGE OF SECURITY SEALS

A. Should it be necessary to break a seal before its arrival at the final destination, the following information should be recorded:

1. The name of the person breaking the seal.

2. The reason for breaking the seal.

3. The time and date the seal was broken.

4. The serial number of the broken seal.

5. The serial number of the replacement seal.

6. The names of the witnesses to the breaking of the seal.

REMOVAL OF SEAL AND MAINTAINING INBOUND LOG BOOK

A. To insure the integrity of a security seal prior to its removal, be sure to check the seal for signs of tampering, and pull the seal to verify that it is still locked.

B. Follow the below checklist:

1. Only designated employees should remove seals.

2. Record the seal marking, color- and numbering in the inbound security seal log. Always verify that the seal corresponds with the seal information of the shipping document.

3. Before removing the seal, look for signs of tampering!

4. Pull the seal to insure that the seal is properly locked, and THEN remove it.

5. Any suspicion of tampering should immediately be reported to the security manager. Also be sure to provide a full description of the issue in the inbound security seal log. Do not throw the seal away, as it may be needed for further investigation.

6. All shipments received with a compromised seal must be registered in the inbound security seal log. It may be required to replace compromised seals with new seals.

7. If pilferage or theft has taken place, an investigation must immediately begin.

ADDITIONAL PROCEDURES

A. In addition to monitoring the seals and their application, other steps may be taken to increase the effectiveness of the security seal program:

1. Insure that the containers are designed so ballots and other materials can only be accessed by removing the security seal.

2. Make use of different colors and markings on security seals, and also use different types of seals to indicate ballots from different locations, types of materials, etc.

3. Change the colors and markings of seals, and dispose of previous types and colors of seals for each election or each year. This will prevent fraudulent use of old seals.

4.9 -- 20119. Data Publication Prior to Audit

4.9.1 Should publish to posting service with trusted timestamps and without overwriting

This section speaks of publishing information to the election official's website. Unfortunately, such websites are normally not equipped with trusted timestamps such that the data cannot be changed by a compromised employee and the date forged to create an earlier date, thereby covering up a failing audit or evidence of an internal attack. Also, a sophisticated attacker could modify the data on the website without detection.

Instead, election officials should post to a third-party posting service website like Sharefile.com which provides trusted timestamps that cannot be back-dated. No files should be overwritten, but each update should provide a new file.

4.9.2 Cast Vote Records are Public Information and contain no user-identifiable information, and should be similarly posted.

It is essential for the oversight of audits that cast-vote records information be provided. These records must be provided down to the ballot, if a ballot-comparison audit is performed. It is not feasible to provide effective oversight nor to verify an audit unless the complete set of cast vote records is provided such that the votes in each record can be added up to produce the posted grand totals. These files MUST be posted to a public website, as described above, to provide any confidence in the audit. If they are not posted, then it would be a simple matter to substitute a different and matching cast vote record for the one supposedly selected in the random selection.

The provision quotes Elections Code Section 2194(a), is regarding information related to voter registration information. Since there is no voter registration information in the cast vote record, there is no basis to not release this information to the public based on this code section.

4.9.3 Information to be posted should be enumerated.

The following information should be posted to a posting service with trusted timestamps:

- The semi-final, unofficial, or official summary results of each contest showing the total number of votes for each candidate or contest option

- The same as above additionally broken down by precinct and batch.
- For ballot-comparison risk-limiting audits, the complete set of cast-vote records, broken down by ballot.
- For ballot image audits, the complete set of ballot images, as produced by the Election Management system, and preferably in PDF/A format, with the same ballot ids as is shown in the cast vote record, and the CVR file with the additional field showing the style number of the ballot. Ballot images should be placed in ZIP archives with sizes about 5GB or less.
- The ballot manifest, if it is not part of the CVR file.
- An Election Information File, which provides correspondence between the contest names as used in the semi-final, unofficial, or official summary results, those used in the Cast Vote Record file, and those used on the ballot itself, and those used in any ballot marking device summaries, and similarly for contest options. Also included in this file is the exact text in any Yes/No question type contests, which is normally available by reviewing the sample ballot. The Election Information File is useful to correlate and correct for small deviations in the names used within the data file and names used on the ballot.

4.10 -- 20120. Random Seed

4.10.1 Open to Video Recording

The generation of the random seed is specified in a public meeting. Such a meeting must be held in a place which is not subject to any additional security, registration or restrictions of the public, and video recording must be explicitly allowed. Live streaming of the meeting is also allowed.

4.10.2 Random Number Generator (RNG)

The random number generator that will be used should be announced when the random seed is announced so any member of the public can verify the generated random numbers provided by any software that may be utilized. The code for the RNG will be posted and made available.

4.10.3 Posted Data will be Confirmed Prior to Generation of the Seed

During the meeting and prior to generation of the seed, election officials will publish the secure hash message digests using NIST standardized SHA-256 or better hash generation algorithms, publish these to the secure-posting service, and provide printouts to anyone attending the seed generation ceremony.

4.11 -- 20123. Ballot Retrieval and Manual Examination

4.11.1 Ballot Retrieval is Critical and Public Oversight is essential

Ballot sampling in ballot-level RLAs that access random ballots from a secure storage area is a critical step as RLAs can be easily "fixed" or defeated by compromised workers. Assuming election staff has modified the election results to "flip" an election between two ballot options A and B, where A is the actual winner but B has been awarded the win through an attack on the tabulation, then compromised workers can defeat the audit very easily by biasing the choice of ballots chosen for audit.

In a ballot-polling RLA, they need only choose ballots that have votes for B over those for A. In a ballot-comparison audit, they need only choose ballots for records that have not been changed.

So verifying that the ballot is indeed the one that has been indicated by the random number generator is important, and the public must be allowed to observe this process.

4.11.2 Paper tally sheets should be used

This section includes the following:

> (d) The audit board shall record the voters' choices in every contest on every ballot card selected for audit, including contests not subject to an RLA or partial RLA. Those choices shall be entered into the RLA tool.

First, we must object again that a subset of contests are selected for audit. Second, we must again assert that the marks on the ballot should be entered into a paper tally sheet either prior to using any DRE-like software recording tool, or concurrently. A proposed standard for uniform tally sheets and how they should be used has been proposed[15] which is incorporated and attached to this comment.

The use of paper tally sheets respects the need for "software independence" of election systems, and this is even more important for auditing software.

The other benefit of using tally sheets is that the practice is similar to the process already being used in the 1% manual tally audit, and the amount of data that may need to be entered into any software tool can be reduced by at least 20x (for ballot-polling audit) or 100x (for batch-comparison audit).

4.11.3 Extending to all contests not included in the RLA samples

The regulations provide that only three contests be included in the RLA, chosen at random in any county. We believe this does not fulfill the intent of the risk-limiting audit law, as already

---

[15] https://copswiki.org/Common/M1939 "Uniform Audit Tally Sheets"

described, as it says that the audit should be comprehensive. Section 20123 (g) implies that all contests are nevertheless supposed to be covered by the audit by subjecting them to batch-comparison auditing as defined in the 1% manual tally audit section 15360, where contests not covered by the 1% manual tally would be tallied in at least one precinct.

> (g) If there is any contest in the jurisdiction not contained on any of the ballots selected for the audit, the elections official shall select one or more precincts at random from precincts that contain the contest and manually tabulate the votes in that contest in those precincts, pursuant to Elections Code section 15360. The manual tabulation shall apply only to the contests not previously included in RLA.

This is problematic for several reasons, as follows:

1. The trigger to move to a batch-comparison audit of one batch for contests not included is based on whether the contest is "not contained on any of the ballots selected for the audit." Apparently, by this provision, if even one ballot is included in the ballots sampled, that is enough to say the contest is audited. One ballot is not enough to claim that the contest is "included in the RLA."

2. Being "included in the RLA", as mentioned in the last line of this paragraph must mean more than just sampled and marks tallied. The whole idea of a risk-limiting audit is that sufficient samples would be collected such that the samples effectively can predict the outcome of the election. If ballots are sampled but are not compared with the official result, and if no calculation is performed to see if the risk limit was met, then the contest is arguably not "included in the audit."

3. The batch-comparison method as defined in the Election Code 15360 can be very good but Election management systems (EMSs) have a hard time creating a report of every batch for VBM batches that are not sorted by precinct. So this additional batch from a precinct would not provide sufficient coverage of various types of ballots including early and later VBM ballots, unless those VBM ballots are also sorted by precinct.

4. Tallying one batch of ballots can catch many simple mistakes, such as incorrectly programming the x,y coordinates on ballots of a given style, or swapping the candidate names of the results, which effectively swaps all the votes between those candidates across all precincts and batches. But the 1% manual tally does not have any specified means for escalation if sufficient deviations are found that do not rise to that level.

Choosing only one precinct for any contest not included on the ballots that were chosen in the audit is not a mathematically sound approach to extend the audit to additional contests, nor is it a sound approach to extend the audit to the contests that ARE included on the ballots chosen.

Furthermore, this last-minute "hack" to try to make the RLA regulations cover all contests does not explain how the additional precincts are chosen "at random."

4.11.4 Procedures do not describe extension of the audit to other contest not explicitly selected

Given that only three contests are selected for audit, how are contests properly treated if they are not one of the big three? The section above discusses how contests are apparently considered to be "included in the RLA", if at least one ballot is sampled with that contest on it. One sample will never be enough to determine whether the outcome is correct, even though an error on one ballot can find certain systemic errors. But in terms of the definition of an RLA, which is to confirm the "outcome" of the election, it will be required that hundreds or thousands of ballots be individually sampled, depending on the margin.

To audit the election comprehensively using a risk-limiting audit, the typical procedure would be to choose the contest which has the most breadth and includes the most ballots in its scope, and also the tightest margin. Thus, any contest that is jurisdiction-wide (or larger) can be used as the contest that will set the margin. If the contest is not jurisdiction-wide, it can be handled one of two ways, depending on how well the ballots are organized. It may be possible to identify the precincts or batches that do contain the contest of interest and sample that.

The following procedure could be used to perform a comprehensive risk-limiting audit:

1. First consider jurisdiction-wide contests, such as any state-wide or county-wide contests. Select the one with the tightest margin of victory. This will determine the maximum number of samples required to confirm the election.

2. Randomly select samples across the entire jurisdiction. Tally all contests on the ballots chosen.

3. Continue to pull samples until the risk limit is met for the tightest district-wide contest. Calculate the risk for the other district-wide contests. They should also be confirmed by this count of ballots unless there is an indication of a serious issue.

4. Now consider the other contests that were included on the ballots that were chosen, and contests that were not sampled at all.

5. Calculate the risk for each contest. For those that exceed the risk limit, consider only the subset of precincts that are included in those contests, and pull additional samples from only those precincts until the risk limit is met for all contests. This is typically performed in tranches, where an estimate is made regarding the number of ballots to be drawn from the subset of precincts, and that entire number is drawn at once, and they are evaluated and included in the calculation of the risk. After the first tranche, some of the contests will likely be confirmed within the risk limit, and this will likely reduce the number of precincts that are included in subsequent sampling rounds.

You will note that the procedure above requires that the ballots be sufficiently organized to allow ballots to be sampled from a reduced set of ballots that do not include ballots from contests that

are already confirmed. In a ballot-polling audit, this may be feasible only if the ballots are actually sorted into precincts or into groups of precincts that will allow more focused sampling.

If the district is performing a ballot-comparison audit, it should be feasible to exactly identify which ballot includes the contests of interest, and confine the random selection to those ballots.

If the SOS still wishes to conduct a non-comprehensive audit which is not risk-limiting except for some contests, a contest should be considered to be "included in the RLA" if it meets some level of limited risk, perhaps 2x the risk of the officially included contests (10%). Those can be considered "mostly confirmed," so that tallying an additional precinct is not allowed. Then, for all contests that were not "mostly confirmed," including those that had no ballots included at all, they would be included in the subsequent batch-comparison audit.

For those districts that have organized their ballots so they can be pulled and compared in a ballot-comparison audit, they may find it easier to pull ballots from targeted precincts to comply with the risk limit.

4.11.5 Completion Deadline

This section includes the final paragraph:

> (h) The RLA shall be completed no later than the business day before the canvass deadline.

Given the fact that RLA audits may require full manual hand counts of ballots, this deadline may need to have an emergency relief valve in case the audit is not feasible to complete in the allotted time. There are two options we can offer to help with the fact that the audit may not be possible to complete in a reasonable period of time if the margins are very close:

1. Allow certification of part of the election with a tentative certification on those contests that are still being hand-counted.

2. Provide for ballot image audits, so that the images can be quickly retabulated to provide a full review of the election by an independent third-party service, while also including an RLA to some extent to validate the ballot images. If an RLA is performed on a contest, then it will also validate the images of that contest, because the machine interpretation is based on those images.

4.12 -- 20124. Public Observation and Verification of Audit

One of the most important flaws of risk-limiting audits as described in the document "The Four Fatal Flaws of RLA Audits" is the complexity of the audit process and the fact that the auditing team may innocently fix up the audit to produce "clean" results rather than accurately report an

election that has some discrepancies, even if those discrepancies do not rise to the level to overturn the election.

4.12.1 Include the option of using a Batch-Comparison RLA

The risk inherent in the audit process itself can be minimized by using a process that is as simple as possible. For this reason, we recommend that districts consider the batch-comparison RLA instead of the ballot-polling and ballot-comparison methods. This audit process has a few other benefits, as follows:

1. The ballot-comparison audit requires a cast-vote record file that breaks down the computer results for every individual ballot. The ballots must be individually identified so they can be retrieved. In the batch-comparison audit, the computer report does not need to be broken down to the ballot level. It can be more easily be generated from existing equipment.

2. Voting equipment used in precincts, such as from ES&S, Dominion, and Hart, shuffle the ballots in memory and do not keep the paper ballots in order, and thus, if a ballot-comparison audit is to be performed, these ballots must be rescanned with equipment that will usually imprint a number on the ballot and maintain their order and correspondence with the cast-vote record file. This is not an issue with a batch-comparison audit.

3. Counties are used to performing the 1% manual tally, and a batch-comparison RLA is not that much different. The main differences would be:

    a. All batches and precincts must be included in the audit, and would not be subject to the exclusions allowed after the passage of AB-840.

    b. The batches and precincts should be chosen, not with linear random sampling, but sampling related to the "Maximum Error Bound" which is a combination of the size of the batch or precinct and also the margin of victory in that batch for the contests under consideration.

    c. The number of batches tallied will depend on the margins of the contests.

4. Generally, this will benefit very large districts like Los Angeles, where instead of tallying 45 precincts or so, they could tally only around 14, under the assumption that the attack would have to modify at least 20% of the precincts. As with all RLA audits, the number of batches required for audit will grow substantially when the margin gets very close.

5. But for smaller districts, it would likely be infeasible to move to RLA audits, using any method.

6. The risk limit is slightly more complex to calculate because it depends on how the hacks are characterized. Most simplistic equations do not adequately limit how much a given

batch or precinct may be modified, and as a result, the risk limit is overly conservative, meaning that a 10% risk limit in a batch-comparison audit is similar to a 5% risk limit in ballot-sampled audits.

4.12.2 Include as much data as possible in the report

The main strategy for allowing verification of really any sort of audit, including the RLA audits, is to include as much information and data as possible in the report. This will be covered in the following section.

4.13 -- 20125. Certification of Contest Results and Reporting of Audit Results

4.13.1 Standardized Audit Report

We propose that the districts use a uniform audit report file format, which can be in a machine-readable but also directly printable .xlsx format. Allowing the audit report to be directly printable eliminates some transcription errors that can otherwise occur.

A proposed Uniform Audit Report Format is being reviewed by the election integrity community at this address: https://copswiki.org/Common/M1940. This proposed audit report format is hereby fully included in our comment on the SOS regulations.

5 Conclusion

5.1 Key issues

1. Audit is not "Comprehensive" and the method is not mathematically sound.
    a. Only three contests are randomly chosen for the audit, one-state wide and two not state-wide and either fully or partially contained in the county. There was no mention of choosing only a few contests in AB-2125.
    b. Random choice of contests is uniform, with no weighting for consequence or margin.
    c. There is no "expansion" to other contests defined, no risk calcs for other contests, but all marks are tallied.
    d. Any contests that are not tallied with at least one ballot must have a batch tallied using 1% Manual Tally rules, with no risk calculations nor tallying.
    e. This method does not result in a "comprehensive" RLA which is specified in the law developed by AB-2125.
2. Relies on DRE-like entry software with no way to verify. Paper tally sheets should be used and we have drafted a proposed uniform standard.

3. Defines only ballot-polling and ballot-comparison audits, but not batch-comparison RLA. I think there is a fear people would start to see the 1% manual tally as a crippled batch-comparison audit (which it is).
4. The method of determining the manifest is not clearly defined.
5. We believe the Poll List (List of all ballots cast at precincts and VBM ballots) should be published to allow for consistency checks.
6. A uniform audit report format should be used. We have proposed such a format which is both human-readable and computer parseable.

5.2 Requested Corrections

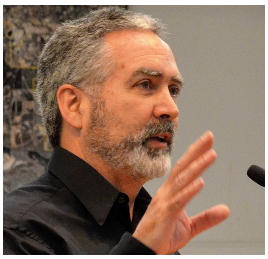
1. The RLA should be comprehensive and include all contests to be "legal."
2. If contests are to be selected randomly, the selection must be weighted by importance, so that high-consequence and close-margin contests are more-likely chosen.
3. Risk calculations should be performed for all contests, and no contest should fall below some given risk level, say 20%.
4. Batch-Comparison RLA should be defined and offered as an option.
5. Ballot-Image Audit should be defined and offered as a solution for an RLA that is expanding to a full hand count. The SOS should support the work to allow scanners to be considered "Trusted Systems" per the definitions already embraced by the SOS.
6. Uniform Paper Tally Sheets should be adopted and required for data entry, either initially or concurrently with any entry into DRE-like "software tool."
7. A Uniform Audit Report format should be adopted which is both human and machine readable.
8. Chain of Custody standards should be improved, per the suggested wording provided.
9. Cast-vote records should be made public and posted to a posting service with trusted timestamps.
10. "Ballot" definition should be extended to electronic scan of the ballot when created by "trusted systems."

5.3 Hearing Requested

Because of the complexity of this issue, we request a hearing on these regulations.

==========

About Ray Lutz



Ray Lutz holds a Master’s degree in electronic and computer engineering and has significant industry and standards experience in document processing equipment, including printers, scanners, facsimile, imaging, etc. Also was involved in a test-strategy development group for testing VLSI (very large scale integrated) circuits, and ran a quality assurance department in a manufacturing setting. Founded Citizens Oversight in 2006 and has been involved in election integrity oversight, particularly of election audits, and mainly with respect to those audits in California.

Contact Information:
raylutz@citizensoversight.org