From: Merlin Klotz
To: SoS Rulemaking
Subject: Requested and additional election rules comments
Date: Monday, July 17, 2017 1:44:32 PM
Attachments: DC Election Statistical Review APPENDIX.PDF
Linderman Response 7-17.docx
Memo - SOS (005).docx

Attached find:

1. Requested calculations of statistical confidence of current process.
2. Response to Dr. Linderman comments
3. Consideration of Current Election Process and Berkley Theory Threat Assessment

Current protocol complies with statutory definition of Risk Limiting Audit. Consideration of the entire protocol enhances the statistical probability that the election produced the correct results on all races as compared to the Berkley theory focused on a single element with regard to a single race.

The benefits of the entire Colorado model including Central Scan extend to operational efficiencies and confidence in the outcome. Imposition of the Berkley theory on the current model adds cost and statutory time line challenges without any increased statistical confidence benefit.

I ask that the Secretary of State delete proposed Rule 25 and all related changes as unnecessary and counterproductive.

Merlin Klotz

Review of Douglas County Elections Process

Appendix

Ken Horton

July 12, 2017

Introduction

The purpose of this paper is to provide some mathematical detail to the methodology provided in the previously submitted "Review of Douglas County Elections Process."

Validation

In the original paper, we determined sample sizes required to gain 95% and 99% confidence in the result of our election. To do this, we used the hypergeometric distribution. For example, assume 200,000 votes were cast in an election and the VS told us that a candidate garnered 51% of the votes (102,000 for and 98,000 against). Now, assume the system was inaccurate and that the candidate gained no more than half of the votes (100,000 for and 100,000 against). Under this assumption, we know that in the 200,000 total ballots, there are at least 2,000 incorrectly read ballots. If we randomly select 500 ballots from the 200,000 total, then X, the number of incorrectly read ballots in our sample, follows a hypergeometric distribution:

$$X \sim \mathsf{Hyper}(m, n, k)$$

where m is the number of incorrectly read ballots (2,000), n is the number of correctly read ballots (198,000), and k is the number of ballots we select in our random sample (500). The probability of getting x incorrectly read ballots in our sample of size k is given by:

$$P(X = x) = \frac{\binom{m}{x}\binom{n}{k-x}}{\binom{m+n}{k}}$$

When we select a random sample, we want to be quite confident that if enough incorrectly read ballots exist to sway an election, we will select at least one in our random sample. So we are looking for the probability that $X \geq 1$:

$$P(X \geq 1) = 1 - P(X = 0) = 1 - \frac{\binom{2000}{0}\binom{198000}{500}}{\binom{200000}{500}}$$

This probability is 0.9935 (calculated using the free software package `R`). If we increase our sample size to 1000, this probability becomes >0.9999.

Verification of Reported Margin of Victory

In order to verify our reported margin of victory, we consider the traditional method of calculating margin of error in polling. Our goal now is to use a random sample to verify the reported vote result (as opposed to simply validating the accuracy of the voting system). If we select a random sample of $n = 500$ ballots, and record x, the observed number of votes won by the winning candidate, we can calculate a lower bound for the true percentage of votes won. Based solely on this sample, we can be $(1 - \alpha) * 100\%$ confident that the actual percentage of votes gained is greater than:

$$\frac{x}{n} - z_\alpha * \sqrt{\frac{x/n * (1 - x/n)}{n}}$$

where z_α is 1.64 for 95% confidence and 2.33 for 99% confidence. If this lower bound is less than or equal to 0.5, then it's feasible that the reported winner did not gain 50% of the votes. In this case, our sample does not verify the result of the election. Assume 200,000 votes were cast in an election with we determined that the winning candidate garnered 55% of the votes. Ostensibly, a random sample of size 500 would look somewhat proportional to our population. However, sometimes, by luck, we will draw random samples that our unusual. The question now is what is the probability that a random sample of size 500 will verify the result of our election? This question is answered with simulation.

We simulate a large number (say 50,000) of random samples of size 500. For each of these 50,000 random samples, we calculate a lower bound according to the equation above. Next, we determine the percentage of those lower bounds that were above 0.5. This represents an empirical probability that a random sample of size 500 would verify the result of the election. In the example stated in this section, 72.20% of the random samples resulted in lower bounds greater than 0.5. Thus, the probability of a random sample of size 500 verifying the election result is 72.20%. In order to get to 95% probability, we would need to take a larger sample ($n = 1092$).

DOUGLAS COUNTY
COLORADO

Merlin Klotz, Clerk & Recorder

301 Wilcox Street ♦ Castle Rock, Colorado 80104 ♦ (303) 660-7469 ♦ douglas.co.us/clerk

Dear Dr. Linderman,

I note your comments regarding Douglas County and myself. I've long been aware that when one is losing a debate the tactic is normally to divert the discussion away from the issue at hand. Beyond that, your comments reveal your lack of understanding of the implicit controls in the Colorado central scan process.

I would remind you that the issue was and remains whether Colorado should abandon an audit protocol that assures 99+% probability of not certifying an incorrect outcome on all races with a 1% differential to favor one that only achieves 90% to 95% probability of not certifying an incorrect outcome on a single race with a 5% differential.

You should be aware that the statutory definition of "*Risk Limiting Audit*" is not mutually exclusive to your definition of RLA:

> *CRS: 1-7-515 (5) (b) "Risk-limiting audit" means an audit protocol that makes use of statistical methods and is designed to limit to acceptable levels the risk of certifying a preliminary election outcome that constitutes an incorrect outcome.*

I will give the Berkley theory credit for providing benefit in jurisdictions (116,990 out of 178,217 precincts) who still rely on polling place elections, each with a single ballot style and no structural security. However, this is Colorado and the state and security of election process here is advanced from many others. In an all-mail ballot/central scan process, the definition of risk limiting audit is not best met with the Berkley theory as the entirety of the process can be secured, precluding a need to rely on a single element of the process for confidence in the outcome.

I would offer that it is not the Douglas County voting hardware that is obsolete, as you allege, but rather the Berkley theory that is obsolete with respect to Colorado. It is a theory that once was applicable but is no longer relevant in states with uniform, advanced, central scan election processes. As you noted in *Risk-Limiting Post-Election Audits: Why and How*, **"Some jurisdictions' heavy use of vote-by-mail ballots can complicate batch-level audits."** (Lindeman, et al)

The premise of why the Berkley theory is necessary is that **"Computer software cannot be guaranteed to be perfect or secure, so voting systems should be software independent:"** (Lindeman and Stark, *A Gentle Introduction to Risk-limiting Audits*, pg. 1)." From this it may be deducted that Apollo 11 landed men on the moon purely by accident. Or, it may be deducted that the software code inspected, certified and installed by the SOS office on our equipment has imbedded bugs that perform mischievous acts then self-erase from the code. As for "being secure", that is precisely why the entire protocol must be considered in evaluating the veracity of an election rather than just a single element. In jurisdictions that lack the security and controls that are standard in Colorado, the Berkley theory may add some degree of confidence.

However, since you believe that the Douglas county “problem” is obsolete equipment I offer you a challenge. Bring on your best techies and alter the outcome in a mock election including PLAT, LAT, PELAT in our facility under the current Colorado rules and protocol without being detected. Yes, that means you are not authorized to step foot in the count room.

Merlin Klotz

DOUGLAS COUNTY
COLORADO

Office of the Clerk and Recorder

www.douglas.co.us/clerk/Elections

Mr. Merlin Klotz

MEMORANDUM FOR Colorado Secretary of State

Subject: Colorado Voting Process & the Berkley Theory

Introduction:

The memorandum will challenge a couple of assumptions regarding the Berkley Theory and review a nominal Threat Assessment for the Colorado Elections Process (CEP).

I. Assumptions

A. <u>Assumption of Fallacy in the Colorado SOS Audit Process (CSAP)</u>

1. The burden of proof is on the affirmative in the statement that the CEP has security challenges. Additionally, the burden of proof is on the affirmative to show that the Berkley Theory is effective and efficient in dealing with any proven security issues. As the existence of any specific security issue has yet to be established for the CEP, it follows that the Berkley Theory cannot yet be established as the preferred solution. Finally, there are multiple and multifaceted security procedures and protocols required state-wide to secure the CEP and ensure that any issues are noted and corrected.

2. <u>Personnel</u>: Personnel are trained and maintain appropriate chain-of-custody procedures when dealing with cast ballots from the time of receipt through the entire process.

3. <u>Physical</u>: For example, the Ballot Tabulation System (BTS) in Douglas County (DC) is kept in the basement of the Elections Facility behind four locked doors. This area is open only to DC Elections staff. All others entering the area are under escort of the same. The area is under 24-hour camera surveillance and real-time monitoring when the building is closed. CEP rules establish surveillance and access standards.

4. <u>Virtual</u>: The BTS is networked on a closed system. For someone to achieve unauthorized electronic entry into the BTS, he or she would have to be physically in the Tabulation Room, the likelihood of which is mitigated by the physical security measures noted above.

B. The Berkley Theory

1. The Berkley Theory doesn't address a number of theoretical issues as it only reviews a portion of the CEP. The relevance of the existence of homogeneity at n sample of N set is not readily apparent to the security and accuracy of the CEP. Nor is the purported ability to randomly select n sample, which matches N set in proportional outcome.

2. The Berkley Theory may be a moot process. When the CEP was Voter Support & Polling Center (VSPC)-based, it was a much more vulnerable process with thousands of pieces of equipment, hundreds of Elections Judges and temporary workers, and a very short timeline. These factors combined to increase the personnel, physical, and virtual vulnerability of the CEP to malicious interference. The current mail-ballot-based CEP is significantly less vulnerable. The existent points of vulnerability include the following:

a) Personnel: Election Judges and temporary workers are still used but in far fewer numbers than previously.

b) Physical: 95%-99% of ballots are returned by mail or drop box and are handled by fewer people and with more secure processes than before.

c) Virtual: CEP software for Voter Registration is controlled and maintained by the SOS, and the SCORE databases are compared against other State databases for information accuracy. The CEP tabulation software is controlled and certified by the SOS and controlled and maintained in secure facilities by county elections offices on intranets unconnected to anything outside of the room.

3. The Berkley Theory may be internally problematic as well as not applicable to the CEP. One nationally recognized Election Equipment Vendor noted that "There's something funny about the formula to compute sample size - it's a constant called Lamda that appears in an exponent. I've asked several times where it comes from and Mark Lindeman (who is routinely cited as an RLA expert) told me that he didn't know but 'it seems to work.' I may be wrong about this but the lack of transparency in the math is astounding" (12 Jul 17email to Merlin Klotz).

II. Threat Assessment

Background. Threat & Vulnerability Assessments are designed to manifest credible threats and vulnerabilities allowing for effective and efficient actions to correct and mitigate negative effects to mission operations. Threats to the CEP fall into the three categories noted above, i.e., Personnel, Physical, Virtual. Threats in these categories can be divided into credible and non-credible. Vulnerabilities are points in the CEP that are open to affect by the threats. Risk is calculated as a function of a credible and relevant threat to a specific vulnerability.

A. Threat Assessment – The Review of Potential Actors and Actions to Produce a Malicious or Negative Effect on Mission Operations

1. The term credible threat means a threat that is "real and immediate, not conjectural or hypothetical." Kegler v. United States DOJ, 436 F. Supp. 2d 1204, 1212 (D. Wyo. 2006) (Retrieved from https://definitions.uslegal.com/c/credible-threat/). To be credible, a threat must meet capability, temporal, and probability criteria.

a) Capability: Does the threat have the capability to negatively impact the target or its operations?

b) Temporal: Does the threat have the ability to negatively impact the target or its operations in a timely fashion?

c) Probability: What is the likelihood of the threat manifesting?

Failing to meet any of these criteria (with a probability factor lower than X) means that the threat is not a credible one. For example, if a group in Ukraine makes statements that they will intimidate voters in Colorado and prevent them from voting, relevant questions would be by what manner (physical or virtual), is the selected capability extant with the group, can that capability be deployed in time to affect the election, and what is the likelihood of an individual voter in Colorado filling out a ballot they got in the mail being vulnerable to such intimidation tactics?

2. Threats:

a) Personnel: The personnel in the SOS and county elections offices pose a potential vice a credible threat to the CEP as the likelihood of their taking malicious action is below X.

b) Physical: There are a range of potential physical threats to the CEP and its components. The credibility of such a threat is low as the probability of such an event is below X.

c) Virtual: There are two main sections of the CEP electronic system. They are SCORE and the BTS. SCORE is theoretically vulnerable to hacking as it is connected to the internet. The BTS is not as it is on an intranet contained in the Tabulation Room.

B. Vulnerability Assessment – The Review of the Susceptibility of Operational Components to a Threat

1. CEP is operated by individuals who have access to CEP processes, procedures, and materials.

2. CEP Facilities are under guard, cameras, the response of armed Quick Reaction Forces (QRF), and other measures.

3. Some CEP Systems are connected to the internet.

C. Risk – The Calculation of a Specific Vulnerability to a Given Credible Threat

1. Personnel: Accessed personnel can conduct malicious activities in a variety of methods.

2. Physical: CEP Facilities can be attacked in a variety of methods.

3. Virtual: Hacking, phishing, spear-phishing, and a variety of malicious methods can affect the CEP Systems.

D. Mitigation – Measures Taken to Lower Risk vis-à-vis a Specific Vulnerability

1. Personnel: Background checks are done on individuals to determine any potential threat posed by looking for previous and related malicious conduct.

2. Physical: CEP Facilities are required to be secured, have camera surveillance, and other security measures to mitigate the effectiveness of any physical attack. Counts of Ballots are maintained through the process from intake through count.

3. Virtual: SCORE is protected with a variety of industry software security protocols and administrative tools. The data is further protected by an organizational requirement to cross-check SCORE with other State and County databases to ensure accuracy of data. The BTS is completely isolated and cannot be reached virtually. It can only be manipulated from the room it is in, the access to which is limited as noted above.

E. Assessment Recommendation:

1. A Threat and Vulnerability Assessment should be run on the CEP to determine what problems are or are not extant. Then and only then can effective and efficient measures be designed and taken to mitigate those threats and lower true risk.

2. Resources should be leveraged and actions taken only on threats deemed to be credible. To expend time, resources, and energy on theoretical or potential threats and absorbs capacity, which then cannot be leveraged to address the credible threat.

3. The Berkley Theory may have the net effect of making the CEP less rather than more safe and secure.

Brett Merr
Douglas County Elections Deputy