Connecticut Citizen Election Audit

Connecticut Election Cybersecurity Task Force **Luther@CTElectionAudit.org**
May 17, 2018 **334 Hollister Way West, Glastonbury, CT 06033**

Secretary Merrill, Deputy Bates and members of the Task Force, my name is Luther Weeks, Executive Director of the Connecticut Citizen Election Audit (Citizen Audit), a computer scientist, and a Certified Moderator. I appreciate the task force approach to determining the best use of the new Federal funding, along with this opportunity to provide recommendations.

Since 2007, the Citizen Audit has organized citizens across Connecticut to observe and independently report on eighteen statewide post-election audits. We have observed over 700 local post-election audit counting sessions. I have personally observed over 140 local counting sessions. I am a contributor to *The Principles and Best Practices for Post-Election Audits*[1], as the moderator of the State Audit Working Group, I contributed to Colorado's rules for implementing its first-in-the-nation risk-limiting audit, and to the text of Rhode Island's risk-limiting audit law passed in 2017.

From the video of the first meeting of the Task Force, I applaud the attention to the cybersecurity of Connecticut's election systems and was heartened by learning about the current protections and proposed additional internal audits of Connecticut's voter registration database. It bothers me when national reports question our registration system's security based on it being "more than 10 years old", while we all know it and the platform it runs on are constantly updated for bug fixes and security.

On the other hand, I must point out that even though our optical scanners are appropriately not attached to the internet, they are still vulnerable. Many of us remember computer viruses that proliferated without connectivity. As far as I know, all security experts recognize that STUXNET represents a successful nation-state attack on an unconnected proprietary system. (Even though we do not say for certain the identity of the attacking nation state(s).)

The remainder of my remarks will address the role and value of paper ballots and post-election audits, along with how a portion of this Federal money can be used to enhance their value.

Enhancing post-election audits was explicitly included as an appropriate use of funds in the Federal legislation. Protection of paper ballots is a necessary component of trustworthy post-election audits. In Connecticut, we could use all the Federal funds to protect paper ballots, just to approach the reasonable protections in several, perhaps the majority, of other states. I am not expecting that. Instead, **I recommend initial steps that will cost, less than one-half a million dollars and outline a more comprehensive, yet efficient plan for the long run that might best protect Connecticut elections and ultimately our democracy.** As Secretary Merrill noted in the previous task force meeting, some of these recommendations will require changes in the law, while others could be accomplished by enforceable directives issued by the Secretary.

Why are post-election audits and paper ballots a critical component of protecting our elections? In the 1970's, I was an early database administrator. My supervisor at the time said summarized it well, **"data protection involves prevention, detection, and recovery". Cybersecurity and other measures protecting voting equipment and voting systems are primarily prevention measures and to a lesser degree detection measures. No matter how much effort we put into cybersecurity, software testing, and hardware maintenance there will always be a significant level of**

[1] http://www.electionaudits.org/principles

vulnerability: Cyber vulnerability, direct attack, potential for software bugs, human errors, or hardware failures.

Paper ballots, sufficient post-election audits, and recounts provide a primary means of detecting cyber, software, human, and hardware failures. They also provide a means of recovery. They provide for, so called, *software independent* verification of election results, resulting in justified public confidence. I agree with Secretary Merrill that public confidence is important. I emphasize that the goal should be *justified public confidence.*

For post-election audits and recounts to be trusted requires strong paper ballot security and a credible chain-of-custody. Audits must also be transparent and publicly verifiable. The independent Citizen Audit[2] reports show our ballot security is woefully inadequate, falling far short of any reasonable standards for any critical documents, let alone voted ballots. For instance, the report for the November 2016 post-election audit report, consistent with previous reports concludes[3]:

> **After ten years of optical scanner use, the laws have not been updated to recognize that polling place voting with optical scanners involves paper ballots. Most officials interpret the law to imply that polling place ballots are required only to be sealed only until the 14th day after the election, yet the audits do not start until the 15th day after the election.** We note that **the adherence to prescribed chain-of-custody and ballot security procedures varies widely among audited districts.**
>
> Ballots are not uniformly maintained in secure facilities, and access to these storage facilities is not reliably logged or recorded, even though the law requires two individuals to be present when these facilities are accessed. In many towns, each registrar could have undetected lone access to the sealed ballots for extended periods. In many towns, several other individuals also have such access. The lack of uniform security of the ballots diminishes confidence in the integrity of the ballots. This diminishes confidence in the integrity of election results.

I suggest reading the November 2017 and previous Citizen Audit reports for selected quotes from citizen observers detailing their reasons for chain-of-custody concerns.

Later the report details that **in 29% of audits, observers had chain-of-custody concerns** and, as volunteered by election officials[4]:

> **In 48% of towns surveyed** in this audit, a single individual can access the ballot storage. In other towns, even though policies require more than one person to access ballots**, there are few or no protections in place to prevent a single person from accessing the ballots.**[5] This is a serious problem, since single individuals could change the ballots and be undetected. At minimum it destroys the credibility of audits and elections.

In many cases, any single individual in the registrars' offices could access voted ballots for hours, undetected. In some cases, janitors and firemen as well. We do not formally access the physical security, yet it is often insufficient to protect ballots from anyone with access to town hall.

I suggest reading the November 2017 and previous Citizen Audit reports for selected quotes from citizen observers detailing their reasons for chain-of-custody concerns.

[2] http://www.CTElectionAudit.org
[3] http://ctelectionaudit.org/2018/ObservationReport2017Nov.pdf Page 11
[4] http://ctelectionaudit.org/2018/ObservationReport2017Nov.pdf Page 18
[5] Numbered tamper-evident seals are a useful protection, but without extensive procedures for their verification and other strong ballot protections, at best they provide a few seconds of protection from possible compromise. For more information, see: http://www.cs.princeton.edu/~appel/voting/SealsOnVotingMachines.pdf and http://www.cs.princeton.edu/~appel/voting/Johnston-AnalysisOfNJSe_als.pdf

Connecticut currently has an insufficient post-election audit. Insufficient because it only audits 5% of polling-place cast, machine counted ballots, exempting all centrally counted absentee ballots, Election Day Registration ballots, and originally hand-counted ballots from the audit – providing a formula for attacking the election by fraudulent counting or programming in areas that will not be audited**. Insufficient because many of the local counting sessions are poorly conducted, with most differences in counts attributed to human counting error and left uninvestigated – a phenomenon that is, as far as I can tell, unique to Connecticut**. Without reliable results and recounting, there is no basis to determine when a difference is a human error or an original count error. On the other hand, officials in other municipalities consistently do an effective job of auditing – some errors in certified results have been correctly identified -- yet are not used to correct the certified results.

Fortunately, there is a straight-forward remedy close at hand. The UConn VoTeR Center in conjunction with the Secretary's Office have developed an independent, electronic system to rescan and recount the ballots, called the *Audit Station*. So far, the Audit Station has been used on a pilot basis for some of the selected post-election audit districts. **Unfortunately, the Audit Station has not been used in a way that meets requirements for software independence or that would satisfy most election integrity activists, leading scientists, and security experts** associated with post-election auditing[6,7].

The good news is that the Audit Station could easily be enhanced to fully support the requirements of *Electronically Assisted Post-Election Audits* that would **satisfy most experts**[8]. UConn has prototyped the necessary enhancements to the Audit Station. Sufficient procedures are straight-forward. They would cost about the same as the current insufficient procedures, while providing even less aggravation and challenges for officials. Nine sets of hardware for the Audit Station – one for each region - have been purchased, while most of that equipment stays idle.

Another advantage of the Audit Station is that it audits all contests, not just three races as required in the current manual audit.

My written testimony details Citizen Audit recommendations for ballot security and audits. Once again, I emphasize that audits and protected paper ballots are necessary for detection and recovery from every type of attack, breakdown, and error.

Thank you

<u>Minimal Recommendations for Ballot Security</u>

- Change the law (in the interim enforceable directives) to recognize polling-place voted ballots; require all ballots be kept under tamper-evident seals[9] for at least 90 days in approved containers, except when required for legal purposes; require all ballot storage access require two unique keys and locks; that one key be kept by the municipal clerk and the other be kept by the registrars and their deputies; that any access require two individual of opposing parties from the registrars office, with the clerks office verifying what ballots were taken or returned; and that the clerks maintain a permanent record of what was accessed/returned, by whom, and for what purpose.
- Require that a copy of the log be made available at each post-election audit counting session.
- Implement seal protocols and training in the proper sealing and unsealing inspection of tamper-evident seals.

[6] https://www.stat.berkeley.edu/~stark/Preprints/retabNotAudit13.pdf
[7] http://ctelectionaudit.org/2018/ObservationReport2017Nov.pdf Pages 37-40
[8] https://www.stat.berkeley.edu/~stark/Preprints/retabulation13.htm

- Implement independent post-election *Process-Audits* that, among other things, verify the existence of the ballot access logs and asses the security of the storage, seals, and locks.

Minimal Recommendations for Post-Election Audits

- Complete the enhancements necessary to the Audit Station to support Electronically Assisted Post-Election Audits.
- Develop and mandate the procedures necessary to support Electronically Assisted Post-Election Audits.
- Deploy and use the existing Audit Station hardware for all post-election audits. E.g.
  - After each election and primary train and staff three teams of three individuals and three sets of the hardware to conduct the audits in conjunction with local election officials. (Many municipalities have several "scanner technicians" employed on election day and for several days before each election. Many would be ideal candidates with the availability and the skills needed for such short-term assignments. This would be very similar to the current program where a few registrars are employed to conduct Moderator Certification Training.)
  - Two machines would be used by each team on each of several days to conduct audits, with the third machine as backup.
  - For instance, teams could spend three days at a location in each region. With nine regions each team would handle three regions, three days each. Registrars with districts selected for audit could sign-up on a first come, first served basis on any day, in any region.
- Expand the audit to make ballots eligible for selection for the audit: Polling-place scanned, absentee, EDR and originally hand-counted.
- Enhance the Audit Station and Election Night Reporting system to add audit results to the Election Night Reporting system such that the public can view and download the detailed results.

Yet all this is not enough. In the long-run to provide justified credibility in ballot security and in our elections. I would suggest:

A Comprehensive Safe and Efficient System for the Long-Run, Including *Risk-Limiting Audits*[10]

The major barrier in Connecticut to trusted ballot security is the cost associated with sufficient facilities and staffing in each of 169 municipalities. Larger jurisdictions in other states have vaults with guards and electronic surveillance for voted ballots. Some have video surveillance and archived recording of all activities in such vaults and election administration areas prior to and for several weeks after elections. Some smaller jurisdictions use metal ballot transfer cases with two unique keys on each case. Leaving the polling place in the custody of opposing individuals and held by different entities.

The major barriers Connecticut has to Risk-Limiting Audits are scanners that do not produce, so called, *Cast Vote Records*, need for efficient Risk-Limiting Audits, polling place scanning, and the distributed nature of ballots and records in 169 municipalities.

[10] One definition of Risk-Limiting-Audits from a law in California: *"Risk-limiting audit" means a manual tally employing a statistical method that ensures a large, predetermined minimum chance of requiring a full manual tally whenever a full manual tally would show an electoral outcome that differs from the outcome reported by the vote tabulating device for the audited contest. A risk-limiting audit shall begin with a hand tally of the votes in one or more audit units and shall continue to hand tally votes in additional audit units until there is strong statistical evidence that the electoral outcome is correct. In the event that counting additional audit units does not provide strong statistical evidence that the electoral outcome is correct, the audit shall continue until there has been a full manual tally to determine the correct electoral outcome of the audited contest."*

The following is an outline of a comprehensive, efficient solution that would also facilitate more uniform recanvasses (Connecticut's name for our machine recounts.) and, as a side benefit, facilitate public observation.

- Build/acquire regional ballot storage facilities that can be guarded and remotely surveilled. (Each of nine regions seems too many, perhaps three to five locations). They could be additions to town halls with compensation to the host town; former town halls with vaults; or former bank buildings.
- Perhaps State Police or other secure means used to collect and deliver voted ballots on election night.
- All ballots rescanned by the Audit Station.
- Risk-Limiting Audits and recanvasses conducted at those facilities.
- Adjust the election calendar, recanvass, and audit laws to hold comprehensive audits sooner, so that audits can be used, when appropriate, to trigger full recanvasses in cases where the audits indicate that the incorrect winner my have been initial reported[11]. Consider replacing recanvasses with robust adversarial recounts. Where risk-limiting audits are used, eliminate close-vote recounts and, when necessary, have risk-limiting audits trigger recounts.

Some Details About Risk-Limiting Audits and Process Audits

At this point Risk-Limiting Audits seem to have reached buzzword status. Yet, most people are not exactly sure what they are, how they work, and very few have seen a risk-limiting audit in action. Know these things:

- Risk-Limiting Audits have the potential to create justified confidence in election results, while reducing the costs associated with conventional audits and recounts.
- Only one state, Colorado, has implemented comprehensive risk-limiting audits. After several prototypes, Colorado has done risk-limiting audits once, in November 2017. It was an extensive cooperative effort between officials, scientists, activists, and a third-party vendor. It needs improvement in several area – everyone involved is working on that.
- In 2017, Rhode Island passed a Risk-Limiting Audit law in record time, with broad legislative support, yet the work of planning and implementation remains.
- Risk-Limiting Audits are not simple to implement and understand. They are not one-size-fits-all. There are multiple methods. There are unique challenges in each state, based on the diversity of state election equipment and election administration procedures. The cooperation and support across the board in Colorado was exemplary. Rhode Island on the surface may seem like Connecticut, yet at this point it is much more ideally positioned to facilitate Risk-Limiting Audits.
- Risk-Limiting Audits alone are insufficient to insure or demonstrate election integrity. They, like many existing audits, provide assurance that counting and totaling of ballots was accurate enough to determine the correct winner. Independent, so called, Process-Audits, are needed to assure, among other things, that the voted ballots were securely preserved, that the voter registration database is accurate, that voter registration procedures were sufficient and followed, that polling place operations were conducted correctly, the check-in process was accurate, and that voters were served – even that the post-election audits were properly conducted and reported.

[11] Current Connecticut law requires that recanvasses must be completed within eight days of the election, while audits cannot start until fifteen days after an election. This can cause unnecessary recanvass or prevent close-vote recanvasses, while audits are too late to effect certification. We should not consider this as beyond change. Other states vary considerably from this calendar. E.g. Minnesota law requires that audits must be completed within five days after each election, while their more robust close-vote recounts cannot commence until two weeks after an election.