A Two-Tier Approach

An Accurate, Secure, Transparent, Ballot-Counting Protocol

Lulu Friesdat

INTRODUCTION

Hand counting ballots is not hard. That is the mantra of Virginia Martin, Democratic Commissioner of Columbia County New York, where they do a 100% manual hand-count audit of all contested races on the ballot. "It's not that hard, it doesn't take that long, and it doesn't cost that much."

I have heard her say it over and over again. Sitting next to her on panels, interviewing her for articles, in email exchanges, she says, "It's a blip in our operations."

Her Republican counterpart Commissioner Jason Nastke emphasizes how important these hand counts are to the public. In an article in the local Hudson Valley 360 he says, "Especially in very tight races, which we see over and over and over again, it's important that people in those towns know, 'yes, this is who was truly elected, no fraud or sham, because the board did its job, there's no chance this was a machine error." Martin has put out a document illustrating how many of the County's elections have been decided by one, or a very few number of votes. It is three pages long. City Council races decided by one vote; a Mayor's race decided by 27.

(See TightRaces-HudsonCoNY_Martin attached.)

Because both commissioners are committed to making absolutely sure the votes are counted accurately – and because both maintain a healthy skepticism about relying on electronic voting equipment for their totals – at every election since 2010, when NY state adopted optical scanners as its legally-mandated method of voting, Columbia County has performed 100% hand-count audits.

I. A TWO-TIER SYSTEM

A) Where Can Hand Counts be Done?

This proposal advocates for the use of 100% hand-count audits, as the default method for counting ballots in as many U.S. jurisdictions as possible. What exactly does it mean to say "in as many jurisdictions as possible"? This question has sparked a good deal of debate among those I have asked.

Hand count enthusiasts are loathe to admit that hand counting ballots might not currently be a perfect fit for every electoral landscape. Virginia Martin, for example, says that hand counting scales up. She points out that in jurisdictions with more ballots there is a larger community available to assist with counting. But because the Columbia County template does not involve precinct-based counting – and instead collects the ballots centrally using tight chain of custody procedures – this protocol, if used, could leave large jurisdictions with vast numbers of ballots to count centrally by hand. Los

Angeles County had over 3 million ballots cast in the 2016 presidential election. Counting that many ballots by hand could require more resources, and a more complex skill set, than are currently available.

Another challenge for hand counts, is that some states, California in particular, might have over 70 referendums on the ballot. A manual hand count generally requires a separate pass for each race, and multiple referendums could be daunting to count by hand. Additionally some areas of the country are now using ranked choice voting. In ranked choice voting, candidates who do not have enough votes to win are eliminated, and their votes are transferred to candidates that remain in the race. This adds another layer of complexity to the counting process.

With such a large variance in U.S. Elections – in both the size of jurisdictions and ballot content – a two-tiered approach is preferable to a one-size fits all solution. This proposal recommends creating a "two-tier" system, that gives each county a designation based on its average number of ballots in a four-year period and its standard ballot content. The two suggested designations are:

- **Small/Limited: Small county/municipality with limited ballot content**
- **Large/Complex: Large county municipality and/or complex ballot content**

Jurisdictions would have a protocol, appropriate for their size and content, that ensures an accurate secure transparent count of the votes.

This report:

- Presents tangible guidelines for creating the designations.
- Suggests an appropriate counting protocol of either 100% hand-count audits, or risk-limiting audits for each category and offers comparisons of the two systems.
- Details new advances in how to accurately and securely count ballots.
- Advocates for the adoption of these systems in combination with open-source ballot scanners, and other redundancies, such as releasing photographic ballot images and user-friendly statistical data to the public in a timely manner.
- Offers persuasive evidence that our current counting procedures and the security surrounding them are inadequate in the face of an ever-growing cybersecurity threat.
- Cites, in conclusion, additional reforms that would complement these changes, some of which are pulled from other sources like the Brennan Center for Justice and a letter to Congress from computer and cybersecurity experts.

Current U.S. election protocols are failing us. This report presents substantial evidence that better counting methods are available and urgently need to be implemented to ensure accurate results, and increase voter confidence.

B) Defining a Two-Tier System

1) Voting jurisdictions (counties or municipalities) across the U.S., or in states that adopt this system, will be split into one of two designations:

- Small/Limited: Counties or municipalities with on average 50,000 ballots or less and 10 or fewer referendums.

- Large/Complex: Counties or municipalities with on average more than 50,000 ballots, or more than 10 referendums.

    - Jurisdictions will receive their designation from the Secretary of State's office at least 6 months in advance of an election based on average number of ballots and referendums in the last four years.

2) Counting protocols

- Small/Limited Designation: These counties or municipalities will perform 100% hand-count audits of all contested races.

    - In order to facilitate the smooth adoption of 100% hand-count audits, jurisdictions can phase in their use. The recommended adoption procedure is to count one randomly drawn race by hand in the first election, adding in one more randomly drawn race in each consecutive election for three years, after which time jurisdictions will audit all contested races on the ballot 100% by hand.

- Large/Complex Designation: These counties or municipalities will perform:

    A) A 100% hand-count audit of one randomly drawn race on the ballot.

    B) A 100% hand-count audit of any race on the ballot where the margin of victory is less than 1%.

    C) All remaining races and ballot questions will be audited using a random manual audit of a statistically large enough sample of ballots to determine to a 99% confidence rate that the outcome of all contests on the ballot is correct. This type of audit is often referred to as a risk-limiting audit.

    D) Audits that reveal discrepancies between a machine count and a hand count greater than that allowed by the audit formula must be escalated until resolved by a higher percentage of audited ballots, or a full hand count.

- Large/Complex jurisdictions that wish to do 100% hand-count audits instead of a more narrow risk-limiting protocol may do so for any given race, or for all races.

- In order to follow this system, states must eliminate touch screen (DRE – Direct Record Electronic) voting machines that do not utilize a paper ballot.

  Except in some cases where disabled voters need to use a machine to create a paper ballot that expresses their intent, a voter-marked paper ballot is preferable to a voter-verified ballot. From *A Gentle Introduction to Risk-limiting Audits*. "The best audit trail is voter-marked paper ballots. Voter-verifiable paper records (VVPRs) printed by voting machines are not as good. Voters might not actually inspect VVPRs. Printers can jam or run out of paper. VVPRs can be fragile and cumbersome to audit." Voter-marked paper ballots are also a better defense against machine error or manipulation.

- In all jurisdictions, if there are differences between the machine count and the hand count, officials and counters will do their utmost to determine the reasons for those differences, so that the final count accurately reflects the intent of the voters.

- In all jurisdictions, if there are differences between the machine count and the hand count that cannot be reconciled, the hand count will be used for final certification.

3) Audit procedures

- Best practices for 100% hand-count audits will be explored, and then standardized, documented and publicized. Funding must be available to election officials to train teams of hand-counters from each community in these best practices.

- Any audits that are not 100% hand-count audits must be conducted by a neutral outside agency with no known political affiliations or endorsements. Employees at the auditing agencies must pass criminal background checks, and must not have prior or current felony convictions.

- Defining random: From A Gentle Introduction to Risk-Limiting Audits: "Public confidence requires that observers can verify the selection is fair — that all ballots are equally likely to be selected in each draw. This speaks against a number of common methods for selecting samples, including "arbitrary" selection by the election officials; drawing slips of paper, where there is little hope of confirming that each ballot is represented by exactly one slip and that the slips have been adequately mixed; using proprietary software such as Excel; or using any source of putative randomness that cannot readily be checked. Trustworthy methods of generating random numbers often have two features: a physical source of randomness (such as dice rolls) and inputs

from multiple parties (so that even if some parties collude, any non-colluding party could foil an attempt to rig the sample). It can be efficient, effective, and transparent to use a simple mechanical method — such as rolling dice [Cordero et al., 2006] — to generate a "seed" for a well-designed pseudo-random number generator (PRNG)."

4) Required redundancies

- All jurisdictions (small/limited and large/complex) will release photographic ballot images of all ballots to the public within 72 hours of the election and prior to certification. Images will be released in a PNG format. Those ballot images must be verified to be an identical match to the paper ballots, either with unique serialized numbers, or via an alternate method, and must be bundled with an encryption tag that indicates if the images are altered in any way.

- All jurisdictions (small/limited and large/complex) will release detailed, precinct-level results of the election, in a user-friendly format such as CSV, to the public, within 24 hours of the election and prior to certification.

- All jurisdictions will release the cast vote record from each election within 24 hours of the election and prior to certification.

5) Transparent process

- All audits, whether they consist of a 100% hand count, or a more narrow risk-limiting protocol, will be open to the media and the public for close observation, video-taping, live streaming, and photography. This includes audits conducted by both election officials and outside agencies.

- Time and location of audits must be published and well-publicized at least 30 days in advance of the audits.

- Final results of the audits must be published and well-publicized three days before certification.

- Ballots and election records, including cast vote records and photographic ballot images made by voting machines or scanners, must be open to timely affordable public records requests for examination, copying and scanning. Costs for public records requests need to be standardized nationally and capped (with cost of living adjustments) to avoid the price gouging that is currently used as a deterrent to keep citizens from making these requests.

6) Funding mandate

- Sufficient federal funding will be provided to conduct all audits competently.

C) New Advances

We do not have to continue to count ballots the way we always have. There are lots of ways that this process is improving and can be improved further.

1) Readability

The Michigan Election Reform Alliance (MERA) is undertaking a large-scale "human factors" study in order to establish the most accurate, transparent, and verifiable methods of hand counting votes. In particular they are exploring ballot design. Current ballots are designed for machines to process. Ballots that are designed for people to read, could make hand counting easier, and reduce the necessary time and cost involved in hand counts.

2) Projecting the ballot

Wisconsin Election Integrity has conducted audits projecting ballot images on the wall very large so that an entire room can see them. They click count the ballots together 25 ballots at a time. From their report:

"The astounding benefit of slide-show verification, when compared to hand counts of paper ballots, is speed. When two teams of two auditors (four people) counted votes for two candidates in a mayoral primary, they reached agreement on the visual count for both candidates at a rate of 125 ballots every five minutes, so that a reporting unit with 1,000 ballots could be verified in 40 minutes. A hand count of the same precinct would have taken the same number of people at least two hours."

There is an added benefit of transparency, since members of the public can count along with the official teams.

In their next effort they will be using a document projector to project the actual paper ballots rather than photographic ballot images.

3) Releasing photographic ballot images to the public

Most new models of optical scan voting machines make a photographic image of the ballot as it is scanned, and use that image to count the votes. Tagging this image with a unique identifying number that connects it back to a numbered paper ballot can make these images especially useful for citizen review and audits. This can be done without violating voter privacy.

Another way to verify that the photographic ballot image is identical to the paper ballot is to add voter verification into the process. In this protocol, the voter feeds their ballot into the scanner. As the ballot is scanned a photographic image of the ballot is taken and shown privately to the voter. The voter then looks at

the image, verifies that it is identical to their paper ballot, and presses the "cast vote" button. Photographic ballot images can be immediately uploaded to the county's elections website following the close of polls so that candidates and citizens can independently verify the count.

Work on this issue is being led by John Brakey, Ray Lutz, and John Papa among others.

4) Spreadsheets

The Michigan Election Reform Alliance found the use of spreadsheets effective in their hand count audit of Allegan County Michigan.

D) Where to Draw the Line

The demarcation line between small and large jurisdictions suggested here is 50,000 ballots or less and 10 or fewer referendums. Based on my conversations with Martin and other election officials I believe this is an appropriate dividing line. It is possible that further research and discussion would place the divide a little higher or a little lower.

In the 2016 presidential election, Columbia County counted more than 65,000 votes in multiple races on approximately 20,000 ballots. Martin has said that she believes it would be manageable to count multiple races, by hand, on up to about 50,000 ballots. They comfortably counted 7 referendums plus candidate races, by hand, in one election.

Conversations with other election officials, give the impression that they would find counting large numbers of ballots by hand very challenging. In Dane County Wisconsin they hand counted one race on over 300,000 ballots during the Wisconsin recount. It took them fourteen days working fourteen hours a day, and county clerk Scott McDonell was not a fan, saying, "Humans are the ones that make mistakes. We were constantly having to start over."

The difference between Martin's comfort and McDonnell's struggle with hand counting is note worthy. Martin may have a better understanding than most of why this is. She says that the first time they did the hand counting it was difficult, stressful and very lengthy. But over the years, as they have become familiar with the process, it is now completed faster, and with very few problems. Over time it became clear that some of the people that they brought in to count were simply better at counting than others – they had more of a facility for it. Her office made a habit of hiring those individuals and now they have a well-trained post-election team that quickly and efficiently conducts the count. She says there's no need to start over if effective counting systems are in place. Currently, across the country, most hand counting is a rare event, likely conducted during a stressful and contentious recount. So most counties never experience the comfort level that Martin and Nastke have achieved in Columbia County. If jurisdictions were to begin regularly counting ballots by hand, we would regain this skill as a nation.

E) Benefits of 100% Hand-Count Audits

There are three easily identifiable benefits of doing 100% hand-count audits, in combination with risk-limiting audits.

1) Transparency and confidence

   The first benefit is transparency and confidence. A full hand-count audit does not rely on complicated statistical formulas, technology or software. Almost any member of the general public who has basic counting skills can observe the process, and either feel confident that the counting is being done correctly, or have objections based on a transparent process that they can readily understand.

Further benefits are:

2) Baseline of comparison

   Hand-counted jurisdictions will provide a baseline of comparison for counties that utilize other methods of tallying the votes. With many counties conducting full hand counts, it will be easier to identify counties with anomalous results; and if there is concern about the accuracy of the results, those areas can be targeted by candidates for recounts.

3) Training of hand counters

   Teams of hand counters will be trained across the country. As counties become more familiar with hand counting, the number and types of races that they are comfortable counting by hand could expand.

Using full manual recounts *where possible*, can give both the public and candidates maximum confidence that the tabulations have correctly determined the voters' intent in *all jurisdictions*.

II. COMPARING AUDITING SYSTEMS

A) Why Not Do Risk-Limiting Audits Everywhere?

We could, and it would be better than what we're doing now. This report fully supports the adoption of risk-limiting audits, because they are the best method currently available to efficiently and affordably check the accuracy of vote totals in large and complex jurisdictions.

But there are drawbacks inherent in the complexity of statistically derived audits; furthermore, risk-limiting audits are in preliminary stages, and may have both implementation and security issues that need to be worked out. Because of those issues, which are detailed below, this report favors adopting risk-limiting audits in conjunction with 100% hand-count audits as described in section I. B) above.

Any audit procedure is only as strong as its weakest link. Here are a few of the weaknesses in the current risk-limiting audit protocol.

1) Complexity

Although the protocol uses terms like "super-simple" the formulas are difficult for anyone without at least some advanced mathematics training to follow. This is one formula used in the "super-simple" ballot-level comparison audit, from *A Gentle Introduction to Risk-Limiting Audits*.

"The rule depends on the "diluted margin" m, the smallest reported margin (in votes), divided by the number of ballots cast… Suppose the audit has inspected n ballots. Let u1 and o1 be the number of 1-vote understatements and overstatements among those n ballots, respectively; similarly, let u2 and o2 be the number of 2-vote understatements and overstatements. The audit can stop when

$$n \geq \frac{4.8 + 1.4(o_1 + 5o_2 - 0.6u_1 - 4.4u_2)}{m}.$$

."

A tool set has been developed to help election officials plug in the necessary numbers for any given audit. But the tool set requires understanding what will likely be a new set of vocabulary terms, or new usage of terms, for most people including: diluted margin, pairwise margin, understatement, overstatement, pseudo-random sample, ballot manifest, and human interpretation of the ballot. Here are some sample instructions from the tool kit:

"Contest 3 has an understatement of 2 votes only if the contest has only two candidates. If there are two or more losers in the contest (and only one winner), this contest has an understatement of only one vote, because only one pairwise

margin was understated by two votes; the others were overstated by one vote. Similarly, if there are two or more winners in the contest and only one loser, this contest has an understatement of only one vote. If there are at least two winners and at least two losers, there is no understatement in this contest, because at least one pairwise margin was not affected at all by the discrepancy. Regardless, the ballot has an overstatement of 2 votes, because the ballot has an overstatement of 2 votes in contest 2."

Many election officials will struggle to follow this. That does not mean it cannot be implemented. Many jurisdictions will get the guidance that they need and perform the audits as intended. But what are the possible dangers of implementing a process that those responsible for conducting may not understand?

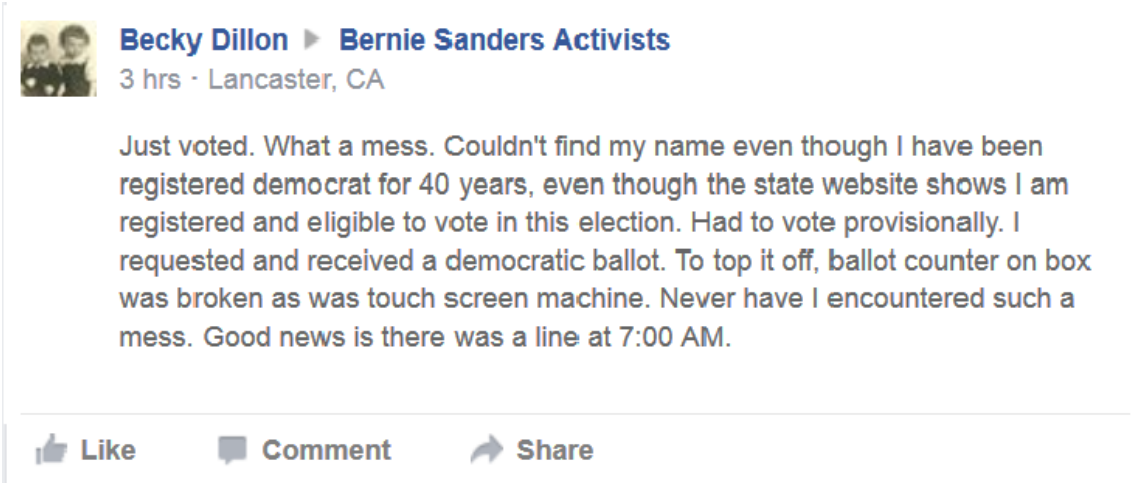
- They may do it incorrectly, thinking they are doing it right.
- They may know they are doing it wrong, but not want to ask questions for fear of looking stupid.
- They may pretend to implement the process, but not actually do it.

2) Corruption

Not only will many election officials not understand the process, members of the public will also find it challenging. What are the dangers inherent in that situation?

- Election officials could take advantage of an audit process that is not widely understood to "game" the audit. That is exactly what happened in the 2004 Cuyahoga recount. "The board staff rigged the sample count … the precincts actually were secretly selected in advance."

Both traditional media and social media reports indicate that U.S. elections are increasingly occurring in an environment of corruption. The 2016 elections witnessed 120,000 voters purged from the rolls in heavily Hispanic districts in New York; missing DMV registrations in North Carolina; party registrations being changed without a voters' knowledge or intent, voters being sent incorrect ballots, a shortage of ballots, polling places being closed, discouragingly long lines, and disturbingly large disparities between initial exit polls and official results.



Becky Dillon, a CA voter forced to vote via provisional ballot, June 7, 2016

Because of this broad context of corruption, it is particularly important that rigorous audit procedures be successfully conducted in a transparent process that is understood by the public. Although risk-limiting audits are a step in the right direction, they do not currently meet this bar.

3) Security

Because risk-limiting audits are complex and highly technical, the likelihood is that the details of implementation will be fleshed out, not by individual counties or states, but more broadly by a third-party company. This is what is happening in Colorado. In 2009, Colorado passed legislation mandating the adoption of risk-limiting audits. Colorado has now hired a company called Free and Fair to develop software for the audits and provide support for their implementation.

Free and Fair is building a "computer tool" to relieve election officials of as much of the pain of these audits as possible. According to their GitHub, a random selection of ballots for the audit will be automatically generated based on the random seed provided "using the SHA-256-based pseudo-random number generator." The process also incorporates the contest margins and other parameters. Ballot manifests and cast vote records are uploaded to a server. There is a state-wide dashboard to view the information centrally. As the audits are performed, the dashboard is updated, along with any formatting or content issues. The public will have access to "appropriate data."

Stephanie Singer, the project lead said in a phone interview that once the ballot selections are made, election officials examine the chosen ballots and then enter those results into a computer program that generates a cast vote record file of the audit. A cast vote record file is a global document, typically in spreadsheet format, used to view all votes cast in a particular election. The comparison of that cast vote record file with the cast vote record file of the initial election results

determines if the initial results are considered accurate, or if the audit needs to escalate, possibly to a full hand count.

Based on information available online and conversations with Singer, it looks like many of the protocols being developed by Free and Fair will utilize an internet connection. This could leave the audits vulnerable to a malware attack. According to their GitHub, Free and Fair has a comprehensive set of validation and testing practices in place. But it is beyond the scope of this report to evaluate them. Singer says that white hat hackers are welcome to test the Free and Fair security setup, keeping in mind that the system will be not be finalized until sometime in September.

The most efficient form of risk-limiting audit, relies on the cast vote record file to determine which ballots to compare. One question is whether that document could be corrupted or manipulated. Duncan Buell, a professor of computer science and engineering at the University of South Carolina, says, "Something like this could be hacked." Buell, who spent fifteen years doing computer analysis for the intelligence community, said there are ways to encrypt spreadsheets, but was not sure how effective that would be. Free and Fair seems to be a new breed of company, working in a very different, more transparent paradigm than traditional voting machine vendors. However, the distrust engendered by the poor security and secrecy of legacy voting machine vendors runs deep. Buell said, "as the recent Chicago breach shows, not even the big name vendors can be trusted to do the right thing."

Because it is unknown who will eventually be contracted and/or subcontracted to support the implementation of risk-limiting audits, it is important that strong security and transparency be part of their procedural mandate. Someone with the skill set sophisticated enough to hack an election will have the comparable skills necessary to hack an audit process to match.

4) Transparency

One primary protection against the audit being manipulated is transparency, but as with the security issues, it is currently unclear if there will be sufficient transparency for the public to truly check that the results of the audit match the original count. In order to do this, the public needs access to the original cast vote record that is being compared to the audit. Colorado election officials may determine that the cast vote record cannot be released because they believe to do so could violate the privacy of some Colorado voters. If the cast vote record is not released, Stark says, "a hash or other cryptographic commitment is made that proves the CVRs (cast vote records) used in the audit are the CVRs that the voting equipment exported." Advocates for election transparency will likely be uncomfortable with this. They will point out that, in this scenario, the public is once again asked to "trust" that the results are accurate.

B) Critiques of 100% Hand-Count Audits

Even supporters of hand counts, like Philip Stark, a professor of statistics at the University of Berkeley, do not believe that 100% hand counts are always the best tool for the job. Stark, who has been the primary developer and proponent of risk-limiting audits is concerned about the amount of time required for full hand counts. He says, "A ballot-level RLA [risk-limiting audit] tends to be more efficient."

His concerns extend further to the transparency of the count. In an email, he said, "Full hand counts are effectively impossible to observe closely enough to ensure they are accurate. Typically, there are teams of 3-4 people at different tables. The ballots are only visible to one or two of them. The ballots are not held up for public inspection. Observers typically have to keep a distance from the ballots, and that makes it impossible for the general public to see what's going on. Counting to large numbers – hundreds – is error-prone. The picket-fence style of tallying is extremely error prone. And because people know what the tally of each batch is "supposed" to be, they may tend to make the hand count agree with the machine count."

This has not been my experience. I have observed large-scale hand counting in Brown County Wisconsin, watched footage of hand counters from elections in New Hampshire, and interviewed dozens of people involved in hand counts over the course of a decade. I have been struck at how conscientious they are; the focus and dedication they bring to the task at hand; and their ability to determine precisely the intent of each voter.

As a journalist in Brown County, I was given complete access to observe and film the process. I was able to film ballots close up, and follow in detail what problems were discovered and how they were resolved. Watching the video, you can see that at one table they could not get the number of ballots to reconcile with the number of voters who signed in. The group counts repeatedly until they find a stack of 10 ballots that had been miscounted as a stack of nine. They were then able to reconcile the numbers. As an observer, I followed the process with no trouble, and it gave me strong confidence that this group of individuals was successfully determining how many people voted, and what their votes were. I had much less confidence in the results determined by running a large portion of the ballots through a scanner.

In Brown County there were observers representing each candidate. Some were watching the process closely and taking notes, or speaking with officials. Interviews indicated they were comfortable with their level of access and had confidence in the process overall.

I have also filmed hand counts that did not give me confidence, as I discuss in III. C. That is why the proposal calls for best practices for 100% hand-count audits to be explored, standardized, documented and publicized – and for funding to be provided to train teams of hand-counters from each community in those best practices (I. B-3, B-6). Better ballot designs and new hand-counting techniques such as slide show auditing, and the use of spreadsheets (I. C) can also address some of Stark's concerns.

C) What are the Comparative Costs between RLAs and hand-count audits?

Virginia Martin has estimated the cost of hand counts in Columbia County at 14 cents per vote counted, or a little more than 1% of their operating budget. Costs for risk-limiting audits are that are currently available are from the pilot program that was run in California from 2011 – 2013 (see appendix H of that report.) In two of three races that this report compared, the risk-limiting audit was considerably more costly than the estimate for a 100% manual hand count. But these estimates are not conclusive. The risk-limiting audits shown here were conducted by Professor Stark personally assisting county election officials, or those officials following a set of instructions. The cost of software-supported risk-limiting audits coordinated by a third party company such as Free and Fair may be quite different.

The final report from the California pilot program also says that much of the current cost of risk-limiting audits is associated with scanning the ballots. This is because those counties' current voting systems are unable to produce the cast vote record file necessary for one type of audit. The ballots are scanned to create that file. If off-the-shelf scanners with open source software capable of creating a cast vote record file are adopted – risk-limiting audit costs of individual counties could come down. Newer voting machines from traditional manufacturers are also capable of creating cast vote record files.

The costs of hand counts could also come down, as new techniques like slide show auditing and easy to count ballots are adopted; making those protocols faster and more efficient as well.

So, at the moment there is not enough data to say if there will eventually be a clear financial advantage to risk-limiting audits over 100% hand counts. The current data that is available does not indicate that.

County	Date	Number of Votes	Number of Races	Cost of RLA	Est Cost of Full Manual Audit	Manual Audit more expensive	RLA more expensive
Humboldt Co CA	2011	6288	3	1,964.41	2640.96	676.55	
Merced Co CA	2011	7321	2	3816.47	2049.88		1766.59
Ventura Co CA	2011	17376	1	5,201.78	2432.64		2769.14

III. CURRENT U.S. COUNTING PROTOCOLS ARE INADEQUATE

A) Many Elections Are Won by Only a Few Votes

As mentioned earlier, a surprisingly large number of contests are won by a very narrow margin. Here are the races from Columbia County that were won by less than 30 votes in 2015. The town name is on the left, followed by the race and the margin of victory.

Ghent: Council by 15
Greenport Supervisor by 21
Hudson and Wards 1-5: Mayor by 27
Hudson and Wards 1-5: 5th Ward Alderman by 8
Taghkanic: Council by 1

(See TightRaces-HudsonCoNY_Martin attached.)

B) Are Voting Machines Making Mistakes?

With such close elections, we want to be confident that whatever system we are using is counting every single vote. Unfortunately that is not currently the case. Many of the optical scan systems in use will not read votes if the mark is too light, if the voter does not fill in the circle exactly, or if the mark goes outside the circle. The machines can also be programmed to read ballots incorrectly, or lose calibration.

In 2012, the Election Assistance Commission found that an optical scanner in use in multiple states, the ES&S DS200 had numerous problems including:

- Random screen-freezes that prevented ballots from being fed.
- Failure to log errors in a file that would let election officials know about problems.
- Skewing of ballots as they're fed into the machine, making votes cast in some parts of the ballot unreadable.

"Jane Platten, the Cuyahoga County elections director, said the county had to switch to shorter ballot pages to fix the problems … Later fixes offered by ES&S also led to system freezes, so the county went back to the previous, flawed software as 'the devil we know,' she said."

In Racine County Wisconsin, during the 2016 presidential recount, I filmed a volunteer named Liz Whitlock, who was stunned at how inaccurate the entire process was. She and her team used clickers to count the votes as the ballots were scanned with an Optech 3P Eagle machine. They registered a difference between their click count and

the scanner results of almost 5%. If that error rate were applied across the entire state, it could produce a difference of 140,000 votes. Trump won the state by 22,000 votes. The clerk in Racine County refused to count any ballots by hand, even after this error rate was revealed.

Wisconsin Election Integrity, a group of volunteer citizens who monitor Wisconsin's elections, compiled all of the vote changes that were recorded during the recount. Even with only a small number of counties recounting the votes by hand, counties changed their reported totals by over 17,000 votes. To reiterate, this was a state that was won by 22,000 votes. Sixty-four percent of all precincts reported different totals. According to the report, "In a few precincts, vote totals were altered by more than 20%."

A recent MIT/Harvard/UW paper confirmed the number of votes changed in the Wisconsin presidential recount at over 17,000. They estimated that ***1 in every 170*** votes had originally been miscounted.

Whitlock, the volunteer who was observing was particularly upset about a process used to address the surprisingly frequent problem that there are more ballots than people who signed in to vote. She described what happens, saying, "They spread out the ballots on the table, and they pull 20 ballots randomly, to get rid of." A representative from Wisconsin Election Integrity confirmed that this process is part of the Wisconsin election code (s.7.51(2)(c - e).

Whitlock's experience comparing the scanner's performance to a click count, and the Wisconsin Election Integrity confirmation that overall there were numerous changes in the recount both demonstrate that current vote-counting protocols are not accurate. Karen McKim, a member of the Wisconsin Election Integrity Action Team, said that in at least two other counties that performed manual verification during or after the recount (Marinette and Outagamie) electronic miscounts similar to those suspected in Racine County were confirmed.

(Racine County WI video.)

C) Aren't We Doing Audits Now?

Most states are not currently conducting audits that are robust enough that they would detect a serious mistake or a manipulation of the election results. A recent Politico article on risk-limiting audits quoted computer science professor J. Alex Halderman as saying that currently, only two states — Colorado and New Mexico — "conduct audits that are robust enough to detect cyberattacks," The article goes on to say that "so far, the two states have conducted them only sporadically."

New York State has a mandatory 3% audit that takes place following each election. I filmed that audit in Brooklyn following the 2016 New York general election. What I saw was not encouraging. Although election officials were friendly and allowed me to view all

parts of the process, there did not seem to be any of the standard hand-counting protocols in place that ensure that ballots are counted correctly. Multiple parties did not view each ballot, multiple parties did not watch the count as it was written down. Each table had individuals counting stacks of ballots and writing down hash marks basically with no supervision. The election official had the results of the machine count, so she knew what the hand count numbers needed to match. There was no sense that the audit was anything but perfunctory. This is not the type of hand-count audit that would actually alert election officials to the existence of a problem with the results, if there was one.

(Video of 2016 Brooklyn New York 3% audits will be available online.)

At a congressional briefing in May, Susan Greenhalgh, a spokeswoman for the election watchdog group Verified Voting, confirmed that there are problems with audits that are currently in use. She said, "Not all audits are created equal… it's really important … that we're doing the types of audits where the voter verified paper ballot … is compared to the tally that's created by the software… Most of the country is not performing those types of audits right now."

What is required is a rigorous, transparent procedure, conducted with trans-partisan oversight and secure chain of custody that tests whether the machine results are accurate. This can be done by either meticulously examining each vote and comparing that count to the machine count, or by demonstrating to a high statistical degree of confidence, such as 99%, that the results of the machine count are correct.

D) Do We Really Have a Problem with Election Security?

Yes. We do. Computer security experts have hacked every voting system in use. They have written papers, run hacking demonstrations, appeared in documentaries, testified before congress and hacked actual elections, all to communicate one concept as clearly as possible: our current election systems are not secure.

At the same congressional briefing in May, J. Alex Halderman, a professor of computer science at the University of Michigan said, "There are 52 different models… over the last ten years, many many different models, both of the DRE style and the optical scan style machines have been brought into the laboratory. And in every single case where a machine has been subjected to rigorous independent security review, it's been shown to suffer from vulnerabilities that would allow the spread of vote-stealing malware."

(video of Halderman/Feldman AccuVote TS hack)

Cybersecurity expert James Scott, a senior fellow at the Institute for Critical Infrastructure Technology, added some hair-raising specifics. In less than 10 minutes of testimony Scott detailed almost every nightmare election hacking scenario imaginable. Many of them were depicted, not as potential threats to worry about in the future, but as events that are happening on the dark web currently or whose implementation is imminent.

"We were asked by HPE [Hewlett Packard Enterprise] to figure out how you would break a local and national election… This is the tool kit that we would have used… On one click… This is what's downloaded into your system and then will migrate laterally throughout your network: Remote access Trojan … a key-logger to record keystrokes; a screen-grabber so you can take screen shots of what's on the screen; a camera and microphone capture tool, so you can listen to what's happening in the office… code-injection mechanisms; social media spread and activation tool..."

Scott listed one type of attack that has been researched by Black Box Voting previously. He confirmed that votes can be changed fractionally via malicious software, and that this is an especially effective and plausible way to manipulate vote totals.

> "The payload that most of these guys are interested in would be a tabulation manipulation feature using fractionalization and decimalization, which weighs [weights] the vote. So what you can do if you're trying to back into a victory for your particular candidate ... it gives every vote a certain weight – and that way it looks completely legitimate. And this is going to be a huge problem down the road."

He describes the actual changing of the votes as the simplest part of the process.

"The malware that would go into the actual voting machine is much easier… The easiest way to do that is to gain spear phishing … access to the manufacturer's update. So you would get the admin credentials, move laterally throughout the network, find out where the payloads of information are, sit there and just basically wait; until using the rest of this payload, you'll be able to see when they're getting ready to update the latest software for all of their voting machines. And then what you do is you just let the manufacturer distribute the payload."

E) Is it About the Russians?

Possibly. But our elections security is so poor it could be hacked by anyone. It could be hacked by the Russians, the Iranians, the Chinese, the North Koreans, the Democratic Party, the Republican Party, your nephew or my niece. Our systems are particularly susceptible to insider rigging. Much of the software has "backdoors" or other vulnerabilities that can allow almost anyone with brief access to the system to install programs that could change votes.

The Fulton County "Rare Error"

On April 18th, Georgia held a special election in the sixth congressional district. Eighteen candidates threw their hat in the ring. In the initial returns, the Democratic candidate Jon Ossoff was leading the race, maintaining totals above 50% - the level needed to win

outright and prevent a run-off. Then a voting machine in Fulton County experienced a "rare error."

What exactly caused that "rare error"? Georgia votes on 15-year-old touch screen machines with no paper trail. Data is transferred on and off them with memory cards. An incorrect memory card was inserted in a Fulton County machine. This caused it to malfunction and for several hours, election officials struggled to gain control of it. Following that error, county officials reported that Ossoff's totals had fallen below 50% and that he would need to compete in the run-off. He eventually lost that run-off to Republican Karen Handel, who received only 19.8 percent of the vote in the first round.

Following the election, Voter GA, an elections research and advocacy group wrote a report identifying two "critical" security flaws that would make it simple for anyone with a modicum of knowledge about the system to change the election results. Neither the software, nor the central databases used in the election, are programmed to recognize or sound an alarm if foreign data is introduced into the program. The VoterGA report concludes that someone with access to the machines could inject foreign data "into live election results for totaling and publishing." Because the machines used in Georgia, the AccuVote TS do not have a paper trail, there is no way to check those election results against the voters' intent.

Douglas Jones, a computer science professor at the University of Iowa said that if he was a hacker he would change the results by creating exactly the type of scenario that unfolded on election night. "I would slip the wrong memory cartridge in and cause them to have to back track, and while they were backtracking and fumbling and rescanning cartridges, I would slip in a ringer." Garland Favorito one of the report's authors went further, adding, "In my professional opinion these machines were designed with deliberate backdoors for tampering."

I wrote about this story previously, and some of the information here is drawn from that reporting.

Nineteen states use the AccuVote TSx – a model that is almost identical to the one used in Georgia. But the AccuVote is not the only machine, currently in use in the U.S. with serious security issues. Every system currently in use is vulnerable to a vote-stealing malware attack. The Institute for Critical Infrastructure Technology released a report called, "Hacking Elections is Easy." The report includes topics like

- The shocking ease of hacking all aspects of virtually any voting machine's "black box" technology.

- A few simple tactics that can "fix" any local, state or national campaign in just days or even hours.

Very few states have any meaningful protections in place for the vote-counting equipment, the voter registration databases or the other electronic systems that surround our elections.

F) Is it Possible that U.S. Elections Are Already Being Hacked?

Yes. It is.

Continuing with our narrative about Georgia's sixth congressional district special election, the race was held in two installments. The events of the first round were outlined above. The second round took place on June 20th. A lawsuit was filed to demand hand-counted paper ballots be used in the election, stating among other issues that the machines in questions were no longer certified. The court ruled that there was an "absence of evidence (e.g., voter testimony, malfunction, unexplained deviations, skewed results, historical data, national research, etc.)" and the election was allowed to proceed on the touch screen machines. Paper ballots run through scanners were used for absentee voting as usual. The certified results declared Handel the winner 52% - 48%.

I published a second article detailing some of the oddities of the election results.

- Ossoff won the paper mail-in vote 64% - 36% (a 28% lead)
- Ossoff won electronic early voting 51% - 49% (a 2% lead)
- Ossoff lost the electronic Election Day voting 58% - 42% (a 16% loss)
- There is a difference of 44% between the paper mail-in returns and the electronic day of election returns.

  (Excel sheet attached: GA6-2017-results-comparison_Friesdat)

The mail-in results themselves have oddities:

- In the previous 3 elections Republicans had outperformed Democrats in the mail-in vote on average by more than double (69% - 31%). But in both rounds of the GA special election Democrats outperformed Republicans by surprisingly large margins (77% - 23% in the first round and 64% - 36% in the second round).

  (Excel sheet attached: GA6-2017-mail-in-comparison_Simon)

There were no major revelations about either candidate – nor were there any last minute surprises in the race to help explain such massive shifts in the votes. Given the extreme vulnerabilities of the voting equipment in Georgia, and many other security issues that are beyond the scope of this paper to detail, it is essential to face the possibility that the voting equipment and/or vote-by-mail protocols were used to deliver inaccurate results.

Because there are no paper records for the majority of the votes cast in the election and because the state does not require post-election audits, there is very little information that can be used to determine whether the results reflect the intent of the voters.

Following the election, a second lawsuit was filed seeking to invalidate the results.

That lawsuit describes how a security researcher, Logan Lamb, discovered that all of the confidential materials from the election center website had been left exposed on the internet where they could be downloaded by anyone. These documents included, "passwords to access the central server for the election, and the code that was to be used to run the election… everything a bad actor (such as a hacker) would need in order to interfere with the election." In an interview Lamb said that, based on the version of Drupal the server was running, he believed the material had been exposed online for three to four years.

The lawsuit further details how during the period that the website was exposed, training videos were also on the website, instructing election officials to download files from the website, "put those files on a memory card, and insert that card into their local county voting systems." This is exactly the type of scenario that cybersecurity expert James Scott described where election results could potentially be manipulated by distributing malware through standard update procedures.

That lawsuit is pending.

G) Is the Security Environment Getting Worse?

Yes. Almost all of our major institutions and many corporations have been successfully hacked.

IRS Commissioner John Koskinen told *Fortune* magazine, "We are basically attacked or at least probed over a million times a day." The U.S. Army and Navy, the Pentagon, and NASA were all successfully penetrated by a hacker named Gary McKinnon. The *Guardian* quoted McKinnon as saying he could scan "65,000 machines in less than nine minutes." This was between 1999 and 2002; hackers have developed considerably more sophisticated tools since then.

Banks and corporations are also defending against constant attacks on their data and financial resources. In February 2016, CNN reported that hackers stole cash from 100 banks and rigged ATMs to spew cash in "one of the largest bank heists ever," totaling approximately $1 billion in stolen funds. Other financial institutions that have been successfully attacked include JPMorgan Chase, Citigroup, the Federal Reserve Bank of New York, and security analysts working for Bank of America. The hacker collective Anonymous has, by themselves, hacked the Church of Scientology, Hidden Wiki, San Francisco BART, the Department of Justice, and the World Trade Organization. Major corporate attacks include the Target data breach that exposed the financial information of 40 million customers, the Sony email scandal, and Adrian Lamo's attack on The New York Times, which was apparently so easy that according to geek.com, Lamo "created an entry in the [New York Times] Op-Ed database for himself."

If anyone believed that elections were somehow exempt from the risk of hacking, the recent DEF CON 25 exploits ended that perception.

The hacking convention featured a "Voting Village" where members of the hacking

community were able to try their hand at penetrating voting equipment. Hackers took complete control of a Diebold e-poll book similar to one currently used in dozens of states, and a WINVote electronic machine no longer in use. Participants bypassed the security screen on the iVotronic by holding the vote button down, while inserting the PEB (Personal Electronic Ballot) card. Then they Googled the password to find out it was svcsvc. The iVotronic is in use in 18 states.

The Sequoia AVC Edge (in use in 13 states) and the AccuVote TSx were dismantled to find that the software on both was completely unencrypted. One novice hacker Ryan Quasney said he thought he could write a program to manipulate votes in under two months. He said somebody with more experience could probably do it in about a week. (Machine usages according to Verified Voting.)

(Video: DEF CON hackers crack voting equipment)

IV. ADDITIONAL PROTOCOLS

A) What Other Changes Are Needed for Our Voting Systems?

This report focuses on establishing transparent audit procedures that will ensure accurate results in U.S. elections and increase public confidence.

There are a number of other improvements to our election systems that are either necessary for audits to take place, or are important in their own right. Many of these have been recommended in other reports, or developed by researchers active in the election integrity community. This report seeks to consolidate the suggestions in one location, for ease of review.

1) Eliminate direct record electronic machines (Recommended by multiple reports)

    - The use of Direct Record Electronic voting machines with no paper trail must be eliminated. These are in use in approximately 20 - 25% of jurisdictions spread out across 15 states.

2) Replace old voting machines with new, auditable systems (Brennan Center)

    - New systems must have voter-verified, preferably voter-marked, paper ballots.

    - The Brennan Center for Justice estimated that in 2016, 43 states were using voting machines that were at least 10 years old. Georgia is using machines that are 15 years old.

3) New systems must create photographic ballot images that are released to the public

4) Open source software

- When ballot-scanning software is used, procedures must be in place that assure that the software used is authentic and exactly the same as the software that was reviewed and tested. It should be at a minimum, disclosed source, with a strong preference towards nonproprietary, open source software. As with other software, it must be tested periodically and updated to address any security issues that are revealed.

5) Recount access

- Candidates must have access to 100% manual recounts without going to court. Recounts need to be affordable, and costs need to be standardized nationally and capped (with cost of living adjustments) to avoid the price gouging that is currently used as a deterrent to keep candidates from requesting recounts.

6) Secure chain of custody procedures

- All counties must have strict chain of custody procedures that require bi or trans-partisan oversight throughout the election process: including oversight of the ballots – both blank and marked, poll books or electronic sign in equipment, voting machines and all component parts of the election. Security must include seals being used and checked; chain of custody paperwork being checked and signed, and ballot and equipment storage facilities that require bi or trans-partisan participation to unlock.

  (See ColumbiaCoNY_ChainOfCustody_Martin document)

6) Secure the voter registration databases

- Electronic poll books and voter registration databases as well as all associated hardware and software must have stringent security protocols. The Brennan Center for Justice recommends completing a full assessment of threats to voter registration systems.

7) Improve overall physical and cybersecurity protcols

- Physical security and security against internet-related vulnerabilities for voting equipment must be strengthened; including improved ability to detect attacks. (Recommended in a letter to Congress by computer and cybersecurity experts.)

- The Brennan Center for Justice recommends upgrading and replacing IT infrastructure, including databases.

8) Security protocols for early voting must be examined and strengthened

9) Security protocols for vote by mail must be examined and strengthened

B) How Soon Do We Need to Act?

Immediately.

At the congressional briefing where cybersecurity expert James Scott spoke, he listed one hack he is particularly worried about: "Access as a service is when a hacker gains access and then they sell for a fee … they keep that backdoor open. So the malicious actor is able to go in and out, and manipulate." He warned: "Access as a service *will* be available for state tabulators by the next presidential election."

Legislators will be in session this fall drafting legislation for the 2018 sessions. It is imperative that we have language drafted and ready for them to implement, so that we can have meaningful audits in place for the 2018 elections.

CONCLUSION

There is currently no single more important task for the U.S. elections community, than to get meaningful audits in place prior to the 2018 elections. 2016 demonstrated an atmosphere of corruption, followed by plummeting confidence levels in election procedures and outcomes. In 2016, only about half of registered voters were very confident that their vote would be counted accurately in the upcoming election. Nine out of ten Americans said they "lack confidence in the country's political system."

The security protocols protecting voting equipment are almost non-existent. They have been demonstrated – by both academics, and actual hackers – to be easily penetrated in every circumstance where they have been tested. The situation is similarly grim for the surrounding systems such as voter registration databases and epolling books. Meanwhile, cybersecurity threats are increasing daily.

There has been a significant divide in the election integrity community about whether to advocate for the 100% hand-counting of paper ballots or to support more targeted risk-limiting audits. Both have advantages and drawbacks.

Based on ongoing dialogue with a broad spectrum of reformers, election officials, and academics, this report presents a moderated position that seeks to utilize each auditing system in the most appropriate locales. Although more work needs to be done to identify and standardize best practices of both procedures, either method can ensure secure and accurate election results. Implemented in concert, in a variety of jurisdictions, both methods will benefit by comparison to the other. Both methods must be implemented using a transparent process open to scrutiny by the public and the media.

In addition, the report advocates for the rapid adoption of new advances, such as releasing photographic ballot images and other detailed election data in all jurisdictions.

Providing these materials to the public in a timely and affordable way, prior to certification, will assist in restoring confidence in our results; and ensure that they are an accurate reflection of the voters' intent.

The proposal is written in detail, citing best practices where possible, with the intent that aspects of it can be translated into legislation.