Three Methods to Check Election Results

Draft 6/25/2021 mailto:admin@votewell.net

This paper is intended to be clear to everyone. Please send questions & comments to clarify it and fix errors.

Contents

Overview

How can officials convince people election results are accurate? The public, or trusted representatives of each group which may doubt results, need to see enough steps to catch and fix problems. Neither insiders nor computers are usually trusted.

Only 31[1] states systematically check accuracy of election tallies, and they omit many contests,[2] omit many ballots,[3] and hide most steps from the public.[4] Some merely run a sample of ballots back through the same machines they used in the election, so most errors will stay the same.

Election systems are complex, to track voter eligibility, ballots and summing all the tallies for thousands of races. Mistakes happen. Billions of dollars and controversial public policies are at stake, so mistakes need to be caught. Similarly we do financial audits to catch financial mistakes. Besides honest mistakes, there are 13,500 arrests for embezzlement per year in the US,[5] usually long-time employees and managers. We need to put the same level of effort into checking elections.

Computer breaches are pervasive, with 67,000 breaches reported in the US in 2018-2020.[6] Large companies averaged 23 cybersecurity incidents per company in 2020: 15 per company caused by careless or negligent employees and contractors, 5 incidents per company from criminal insiders, and 3 from credential theft.[7] In election companies and offices, that level of errors and dishonesty can lead to inaccurate election results.

Election errors are not as closely tracked as embezzlement, but there were at least 200 errors in election machines from 2002-2008, many of which happened repeatedly in different jurisdictions.[8] More errors have happened since then.

Finding and removing errors means checking the entire election, from eligibility and the original voter intent to final tallies.

Overview of Percentage Audits

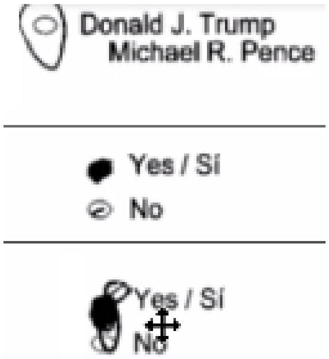
Several states do **Percentage Audits**, where they randomly pick a percentage of precincts or batches of ballots, and hand tally some or all contests in those precincts to see if the computer tally is correct. **Flaws** with this approach include:

1. The sample (usually just one precinct in small counties) is never big enough to have a good chance of catching most errors.
2. Losing candidates rarely are close enough to the auditors to see the ballot markings as they are tallied, so they must trust the insiders doing the work.
3. Audits of early-arriving ballots have to be on or after election day, taking the ballots from storage, since it is generally illegal to hand-tally them before election day. They depend on reliable storage, locks and seals.
4. States recognize hand tallies make mistakes, so they accept discrepancies up to 1%.
5. In some states the percentage audit result is late, or purely informational, and does not lead to changing official result, even if it finds a problem.
6. As noted above, they often cover few contests, hide most steps from the public, and omit major groups of ballots, like mailed ballots.
7. Some states audit by running ballots through scanners again, which does not double-check the scanners' misinterpretation of circled choices, ambiguous choices, fold lines, etc.

Overview of Risk-Limiting Audits

Some statistical and election reform groups[9] support **Risk-Limiting Audits (RLAs)**,[10] which pick a sample size big enough to be 90% or 95% sure of finding problems if they exist. In order to customize sample size and workload during elections, they wait until preliminary results are known, then decide on the sample size and pull paper ballots from storage. They depend on reliable storage, locks and seals.

Stored paper ballots have been subject to tampering for centuries. Blaze, Halderman, Johnston and others show that all **locks** are insecure.[11] Appel, Johnston and others show that all **seals** are insecure.[12] Morrell shows how hard and labor-intensive it is to track the number of ballots which should be in storage.[13] Precinct records are stored even less well than ballots. When Michigan did a thorough review, 11% of precincts had discrepancies in the number of ballots which should have been in storage, including discrepancies of varying sizes in 610 of 1,680 precincts in Wayne County.[14] So *stored* paper ballots are not the final word on voter intent, since there is no way to know when the chain of custody has failed.



Like some percentage audits, RLA advocates believe that the safest way to determine voter intent is for **humans to look** at paper ballots, exactly as the voters filled them out. If samples of paper ballots don't confirm electronic records, RLAs expand the sample to see if the bigger sample agrees.

If an expanded sample still *disagrees* with electronic records, RLA jurisdictions don't expect samples to convince the public of new winners, so they pay for a 100% hand tally of stored paper ballots, and they trust that.

If samples of ballots and electronic records *agree*, they do one independent computer tally of 100% of the computerized election records (not just the sample) to check if this independent tally finds the same winners as the official election tally.

Versions of RLAs have been done in some states, though without the public visibility which would create voter trust.[15] Maryland decided not to use risk-limiting audits, because of the high sample size and chance of 100% hand tallies when auditing close contests.[16]

Overview of Ballot Image Audits

Ballot Image Audit users agree with RLAs that manual comparisons of paper ballots to electronic records are needed to look for flaws in the electronic records. Humans look at the paper ballots to check the images are good copies. These audits add three other ideas:

- Comparison of paper ballots and images can be done every day during early voting, before early ballots go into storage and leave the public eye.
- Electronic files with digital signatures are more secure than stored paper ballots.
- Electronic files let multiple parties and factions independently re-interpret images, and sum these interpretations, so every faction can check the result.

It is best to compare electronic images to paper ballots every day during early voting, election day and afterwards, as the ballots are scanned, before ballots disappear into storage, where insiders have unsupervised access to them and to chain-of-custody records.

Ballots are typically processed in batches, including a couple hundred mailed ballots per batch, or a ballot box from a polling place. Several steps are needed per batch, with rough time estimates for each team of two people, watched by observers:

- 2 minutes to pull sheets from box and scan (see below to adapt for ballots scanned at precincts)
- 1 minute to print 10 copies of digital signature and give to observers, press and multiple officials. The digital signature does not reveal contents of the images. Images themselves are not distributed or tallied before election day. Simultaneously weigh batch on accurate enough scale to give the number of sheets.[17] Compare to scanner count of images. Any mismatch means a misfeed.
- 1 minute to get 2 random numbers (from dice, lottery balls etc.)
- 3 minutes to count to those 2 random sheets in stack (by hand, machine or scale)
- 2 minutes to electronically project the 2 random images, and use opaque projector to project the corresponding 2 sheets, on screen for public comparison. Observers can photograph all or some of these images to verify later that these are in the digital file when the file is available after election day.
- 1 minute average to close out box or resolve problems (usually zero problems, occasionally will have misfeed or scanner flaw and need 10 minutes to re-scan and re-check or count again to the right ballot)
- 10 minutes total per batch, instead of 2 minutes pure scanning and boxing time

- **For ballots scanned at precincts**: When ballots and results come back to a central location, preliminary results can be released after polls have closed, without waiting to check the scans. Teams to check scans would typically be a second shift, under a second set of supervisors which start work when the ballots arrive at a central location. Jurisdictions with many in-person voters can collect ballot boxes after the morning rush, to handle these during the afternoon, leaving just the evening ballots to handle at night. Scans already made at polls can be checked by comparing random ballot sheets to images, as above. If precinct ballots fell randomly into the box and are hard to compare to the images, it may be faster to rescan at central office, so order of images matches stack of sheets. On election night, this checking needs 10 minutes per batch of 200 ballot sheets, so each team can check 18 batches (3,600 ballot sheets) in 180' = 3 hours. Very large jurisdictions can check a good random sample of batches instead of all.

Versions of ballot image audits have been done in Humboldt County CA, Florida, Maryland, and Vermont, though without checking ballots before they go into storage, and without the full public visibility which would create voter trust.[18]

Sample size needs to be at least **as big a sample** as an RLA would use. Sample sizes are discussed in more detail below in the sections on "Steps in Each Method" and "Sample Size Calculations."

Digital signatures are released immediately for files of ballot images, so copies of the files can be trusted at any later date, as long as the digital signatures match. Bank checks are similarly scanned immediately, and scans are trusted from then on. The paper checks are shredded, though ballots would not be.[19]

Factions which question election results (Trump, Sanders, Stein, Arpaio, etc.) can have their experts tally these files of ballot images in any manner they trust, by hand or machine-aided. They're working from copies of the same file so if they disagree enough to change an outcome, they can discuss the discrepant votes and agree, or take them to a judge.

Comparison of 3 Approaches

- **Human review:** Supporters of ballot image audits, RLAs and most percentage audits agree that human checking of paper ballots is important.
- **Stored ballots:** RLAs and percentage audits depend on stored ballots. Ballot image audits don't.
- **Number of contests audited:** Most RLAs and percentage audits only check 1-2 contests, since significant discrepancies involve 100% hand tallies of *paper ballots*, which are costly. Ballot image audits check all contests, since 100% tallies of *image file*s are inexpensive.
- **Identifying causes of errors**, to fix them for future elections, and distinguish accidents from attacks:
  - Image audits identify scanners' errors separately from erroneous interpretations by election computers, and from erroneous summations, so each can be fixed.
  - RLAs identify erroneous summations separately from erroneous computerized vote records (cast vote records, CVRs).[20] They do not determine which CVR errors came from scanner errors and which came from errors in computer interpretation.
  - Percentage audits report total errors, without identifying the causes.

All three approaches are "software independent," meaning they can find and often bypass errors caused by misbehavior in election software.[21] Software independence does not mean the audits detect human misbehavior; it just refers to software misbehavior. Images, verified before ballots go into storage, add protection against human interference with stored ballots, so they are also "storage independent," meaning the audits bypass flawed storage. Other human misbehavior in elections is generally limited by having multiple independent eyes on each step.

Unreliable Locks

Since 1850, people have known how to create a master key from any key in a building, such as a borrowed restroom key.[22] Attackers who cannot find key blanks can 3D-print them from a photo of the lock.[23]

"Roger Johnston... has conducted vulnerability assessments on more than a thousand physical security and nuclear safeguard devices, systems, and programs. It’s his opinion that all security technologies and devices can be defeated—usually 'fairly easily'... "The typical security manufacturer isn’t likely to have good insider threat security, so product tampering at the source is a risk...Then [the security device] will sit on loading docks, and then sit again, sometimes for months, somewhere at the end user, and only then is it installed"[24]

Insiders go in with keys: Cuyahoga County, OH (Cleveland) election workers entered storage rooms in advance and secretly went through the ballots to make public audits appear problem-free. In court these staff "*countered that the board had always done things that way - with the knowledge of its attorney,*"[25] There are no statistics on how often criminals enter rooms undetected, but law enforcement often does so, so ability to enter rooms undetected is widespread at least in law enforcement and former law enforcement.[26]

Ballot drop boxes are the first line of defense, with ineffective locks.[27]

Access to locked courthouses: A report on staff of the company Coalfire, testing courthouse security, found "many of the alarm systems they’d encountered in the past weren’t properly armed and never actually dialed out to responders... Coalfire staffer had easily gotten into a courthouse during daylight hours by impersonating a state IT worker. Then he'd simply sat down and plugged a computer into the network... They snaked a tiny boroscope camera under doors to check for alarms or security guards. They picked old-fashioned pin-and-tumbler locks on doors and desk drawers with simple lock picking tools, finding key cards in drawers and using them to get past other internal doors in the building. They used DeMercurio’s cutting board shim trick and a tool that slides under a door and reaches up to hook its inside handle... “They just said ‘We’re obviously insecure, and now we’re going to make sure we never test again,’”" [28]

Lockpicking is widely taught and practiced.[29] Different techniques apply to electronic locks.[30]

Summary records of the number of voters at each precinct, seal logs, etc. are stored even less securely than ballots.

Unreliable Seals

Election security expert Professor Appel of Princeton points out that when seals are missing or broken, nothing usually can be done. "An attacker who simply cuts, removes, or destroys tamper-indicating seals (without doing anything else) can attempt to call the legitimacy of the election into question... I demonstrated for the judge the complete removal and replacement of all seals with no visible evidence of tampering... 'To the court’s untrained eye, most of the seals appeared unaltered with a few showing minimal damage.' [Opinion 2010, p. 52]... corrupt election officials may hire corrupt seal inspectors... or deliberately fail to train them... Consider an audit or recount of a ballot box, days or weeks after an election... The tamper evident seals are inspected and removed—but by whom"[31]

Johnston and Warner write "no seal is unspoofable (just as no lock is undefeatable)... The optimal choice of a seal depends on the details of your security goals, threats, and adversaries and your personnel... amateurs can attack seals in a way that leaves little (and sometimes no) evidence... Sometimes the consternation and delays that a suspicious seal creates for superiors... make front-line employees reluctant to raise their concerns."[32]

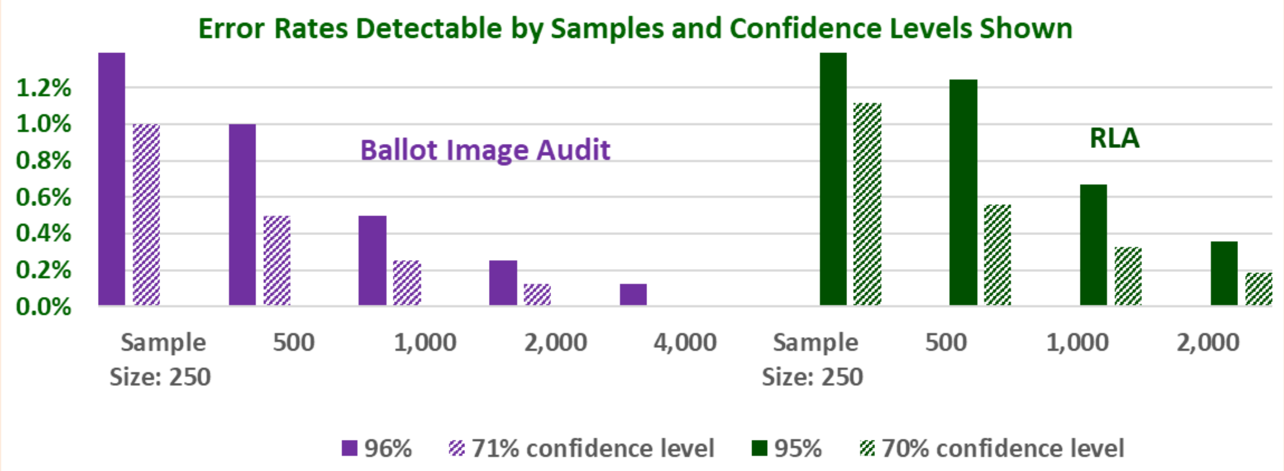
Two Methods to Check Election Results

Risk-Limiting Audits and Ballot Image Audits

BALLOT IMAGE AUDIT **(includes examining adequate sample of ballots)**	**RISK-LIMITING AUDIT (RLA)** **(includes examining adequate sample of ballots)**
Summary of Each Method	
Ballot image audits Select sample size with good, known, chance of catching errors. Immediately after scanning each batch of ballots, select sample ballots and compare to the scanned images of those ballots. *This step finds errors in scanners, which can be fixed immediately. It verifies image files.* For ballots which are scanned at polling places, checking happens when ballots and images are returned to the main processing office. There are several solutions if ballots fall randomly into polling place ballot boxes, including central scanning or having the scanner number ballots after they leave	**Risk-limiting audits (RLA)** Select sample size with good, known, chance of catching errors in 1-2 contests. After provisional ballots are tallied, weeks after election day, select sample ballots and compare 1-2 contests on these ballots to computer records (cast vote records, CVRs).[35] Tally these same 1-2 contests on all CVRs (not just sample).[36] So far this has just been done by the Secretary of State in Colorado, but people trusted by each faction should do tallies independently, so voters trust results. *This step finds errors in software summing the results.*

the voter's hand.[33] Tally all contests,[34] from all images (not just sample). People trusted by each faction should do tallies independently, so voters trust results. *This step finds errors in the software which interprets scans and sums the results.* If winner differs from official result, change official result in any or all contests.	If winner differs from official result or is very close, do 100% hand tally, of these 1-2 contests only. When RLAs were developed a decade ago, ballot images were uncommon, and verifying them against paper ballots was even less common, so the option of tallying 100% of images instead of paper ballots was not addressed.
Human interpretation of marks on ballots is important in both approaches. Examples of ballot marks are on page 8. Some are clear to humans. Some can lead to long discussions in a public process.	
For sample ballots, humans check if images are clear. This should be public. No time is needed to interpret marks. People just check image quality.[37] For the entire file of clear images, parties can hand-interpret at their own expense. More often, computer programs from multiple independent parties will agree on unambiguous images. Humans can spend time in public on ambiguous votes: overvotes, marks outside ovals, etc.	Humans interpret marks on sample ballots in RLAs. This should be public, and can take time when marks are ambiguous. For 100% hand tallies, most of the time is spent manually going through ***un***ambiguous ballots. Usually ambiguous marks are referred to separate staff, and this needs to be public.
Strengths: Paper ballots are examined as soon as they arrive, before anyone can change them in storage. Discrepancies in all contests are found and fixed Independent experts, trusted by each faction, can tally images, by hand or by machine, to find errors and their causes. If people want to examine stored ballots later, the digitally signed images give evidence whether chain of custody was secure, and give backup if needed. **Weaknesses**: Staff manually examine more ballots than needed, if all contests have wide margins.	**Strengths**: Fewer ballots need to be examined on contests with wide winning margins. **Weaknesses**: Paper ballots sit in storage before examination.[38] Insiders can and have breached storage. Law enforcement, and therefore former law enforcement, have skills in covert entry.[39] Breaches might be detected by checking digitally signed ballot images. Sample primarily designed for 1-2 contests. May need 100% hand tally, which is hard and costly to do accurately, and accuracy is rarely measured.
Steps in Each Method	
Before election: Choose **sample size**, affordable for each jurisdiction. When errors affect 1% of ballots, a sample of 500 ballots has 96% chance that it will find errors in 2 or more batches. When errors affect half a percent of ballots, the same sample of 500 has **70%** chance that it will find errors in 2 or more batches.[40] A sample of 250 would not be enough. There is little reason to be stricter, since the alternative of hand counts has this much error when it has been measured.[41] It is possible hand counts could be more accurate by using more staff and constant re-checking, but the scale and cost involved have not been demonstrated. If the public would trust a bigger sample in a bigger jurisdiction, in spite of the statistics, a useful option is to sample at least one ballot from every batch. A large place with 2,000 batches would have a 96% chance of catching errors which affect a quarter	***Before election:*** Choose how many contests to audit (usually just 1). ***Before or after election:*** Decide on an upper limit for audit **sample sizes**, affordable in each jurisdiction (usually done,[42] and sometimes recommended,[43] but not part of theory). If decision-makers do choose an upper limit, then the contests selected for auditing will be contests won by wide enough margins to keep samples under the limit. Colorado has picked contests for its RLAs with samples up to 358 per county in the 2020 general election, 868 in the 2020 primary, 313 in 2019 local elections, 381 in the 2018 general, 351 in the 2018 primary). The graph for RLAs uses Dr. Stark's tools.[44] The apparent differences in error-detection ability between RLAs and ballot image audits are not significant and are artifacts of the calculations. 70%

percent of voters, and 70% chance for errors which affect an eighth of a percent of voters. A spreadsheet calculates all options.	is not recommended, but can happen when an RLA sample is designed for one contest, and results are reported for other, closer contests.



During election processing: Election computer scans each batch of ballots, then: • If a batch's image count differs from ballot count,[45] rescan batch to cure multifeed.[46] • Give copy of this file of images, to independent auditors or public.[47] File gets digital signature[48] to identify true copies. • Select 1 or more random ballots from each batch.[49] Compare to images just created by scanner, publicly. If image does not match ballot, fix the problem, re-scan & re-compare. • If desired, can set aside sampled paper ballots for re-study later. Safe deposit box with dual locks is a start, though imperfect.	***During election processing:*** Store paper ballots, although seals, locks & security cameras[50] are imperfect (pp.2-3).
After election results are tallied: Public or independent auditors tally images. Compare to published tallies, for all contests. Resolve any disagreements by finding which subtotals disagree (precinct, batch, date, etc.) then which specific ballots gave different tallies, and looking at them jointly. The digital signature ensures everyone's image files are exact copies, so ballots are always in the same order in the files, even though ballots came in randomly from voters, so can't be identified with voters. So independent auditors can tally and compare the first 20, next 20 or last 50 images in any batch with discrepancies, to pinpoint which image(s) they tallied differently. If parties disagree when looking at the same images, a judge can decide.	***After election results are tallied:*** Check all locks, seals, records, procedures. Digitally signed ballot images help test chain of custody Select a contest. *Ballot Comparison Audit* Give machine interpretation of each ballot (Cast Vote Record, CVR) to independent auditors or public. Select a random sample of paper ballots. Compare chosen contest on each ballot to its public CVR. If contest doesn't match, expand sample, potentially to 100% hand-tally of selected contest, even though hand tally averages 0.5% to 1% error.[51] Independent auditors compare tally of CVRs to published tallies, for sampled contest(s).[52] If multiple independent auditors interpret ballots or tally CVRs differently, they need to pinpoint discrepancies. A judge decides if necessary.

<table>
<tr><th colspan="2"><b>Recovery from Errors</b>
(Most errors happen by accident. Catching accidents and recovering from them is the first requirement. Catching them will also catch and recover from intentional errors, i.e. hacks)</th></tr>
<tr><td>For ballots which are scanned at polling places, checking happens when ballots and images are returned to the main processing office.
For ballots which are centrally scanned, such as mailed ballots, checking can happen on a flow basis as they are scanned, even before election day. Checking does not involve seeing totals. It only requires looking at a few individual ballots, such as staff see anyway, in adjudication or on top of a batch going through a scanner. Image files are not released to public before election day, but checksums can be, and image files can go to independent auditors who put them in dual-locked safe deposit box.
If multifeed, <b>rescan batch</b> or at least misfed ballots.
If any batch has scanner error (white or black lines, dirt, etc.), <b>rescan batch</b> with cleaner scanner. Double-check batches before and after this one.
If random error is detected in <b>2</b> or more batches, need to <b>rescan and retest all batches.</b> This will also remove uncaught random errors in the other batches. 2-batch cutoff can be changed, but it gives 96% chance of catching errors affecting 1% of ballots and 70% chance for errors affecting 0.5% of ballots. This step can be done as soon as 2 errors are found.
Rescanning does depend on chain of custody for paper ballots up to the time of rescanning, but the digitally signed image files provide a good test of ballot security. Even though some images are imperfect, they were good enough to pass inspection when they were first scanned, so they will usually identify any effort to sabotage the stored ballots.
If no errors are found, the images are confirmed without needing to trust the chain of custody.</td>
<td>About half of multifeeds are missed by the samples, since they are only found when the nth ballot found by counting in a storage box doesn't match the ballot image, which the scanner created. On average the nth ballot is half way through the box.
If mismatches are detected in any batch, expand sample, potentially to <b>100% hand-tally</b> of selected contest. RLA does not accept re-scanning as an option.
If locks, security or seals are broken or bypassable, on ballots, or on the paper records showing number of ballots voted, there is <b>no recovery.</b>
If the number of ballots differs[53] much from records of number of voters, there is <b>no recovery.</b></td></tr>
</table>

Handling Scanning Errors:

If mechanical or software errors (or hacks) affect at least 1% of ballots, the sample is big enough to detect the errors in at least two batches. So the review will lead to rescanning all batches. They can't just rescan batches which detect random problems, since that would leave unfixed problems in other batches.

Errors can include red pens when Dominion scanners suppress red, or pens which reflect badly so their marks are missed by scanners. When the sample detects these, staff need to find a scanner or settings to read the ballots correctly.

If mechanical or software errors (or hacks) *consistently* affect for example the 1st or 65th ballot in many batches, the sample will detect them at least a couple of times, so the 2-batch cutoff forces all batches to be correctly rescanned.

If a subtle hack changes for example a state senate contest to Democrat in every image which follows a Green vote (or to Republican after Libertarian votes), it will be caught rarely, but at least twice. The pattern will not be obvious, to people who aren't reading the previous ballot. The only fix is correctly re-scanning all batches.

Scanning errors lead to 100% hand tally:

The same types of errors listed at left will similarly be found by an adequate RLA sample. If they affect the chosen contest(s) they will be fixed by a 100% hand tally.

If they affect other contests, they will not necessarily be found or fixed.

Other Causes of Error

A. Programming mistakes – Election computers are complex, updated every year. All big computer systems have many bugs.[54] Bugs can shift winners as much as hacks can, and many hacks look like bugs. So bugs need to be taken seriously. Recovering from bugs solves many hacks.

B. Undetected[55] and unfixed[56] backdoors and other hacks – These are pervasive, from multiple adversaries.

C. Insiders at election system manufacturers, and their suppliers, and at election offices – for their own motives, and if they are bribed or blackmailed by people who want a contract or land use approval or other goal.

D. Vulnerability to insider fraud is shown by the 13,500 arrests[57] for embezzlement per year in US businesses. 85% involved a manager,[58] and most were long-time employees. In election companies and offices the same level of dishonesty can lead to election fraud instead of embezzlement.

E. Foreigners who want a policy outcome at one or more levels of government or want to destabilize by defeating incumbents. They can reach air-gapped machines through updates, and when memory devices go back and forth, to transfer results for public release on the internet.

F. Criminal gangs who want to choose prosecutors, sheriffs or judges.

G. Picking polling place locks, when machines sit unguarded the night before an election.

Other Types of Risk Limiting Audit:

Steps above are for Ballot Comparison RLA, where individual ballots are directly compared to their corresponding CVR. There are two other types of RLA, which have slightly different steps. Both still depend on stored ballots.

Different Steps for ***Ballot Polling Audit***

These ignore the CVRs, and need bigger samples:

Select a random sample of paper ballots. Tally them.

Compare to published tallies. If they don't match, expand sample, potentially to 100% hand-tally of selected contest.

Different Steps for ***Batch Comparison Audit***

These ignore CVRs, and take sample of batches, not of individual ballots. The total ballots tallied are many more, but the work is easier to supervise and do accurately, taking whole batches at a time:

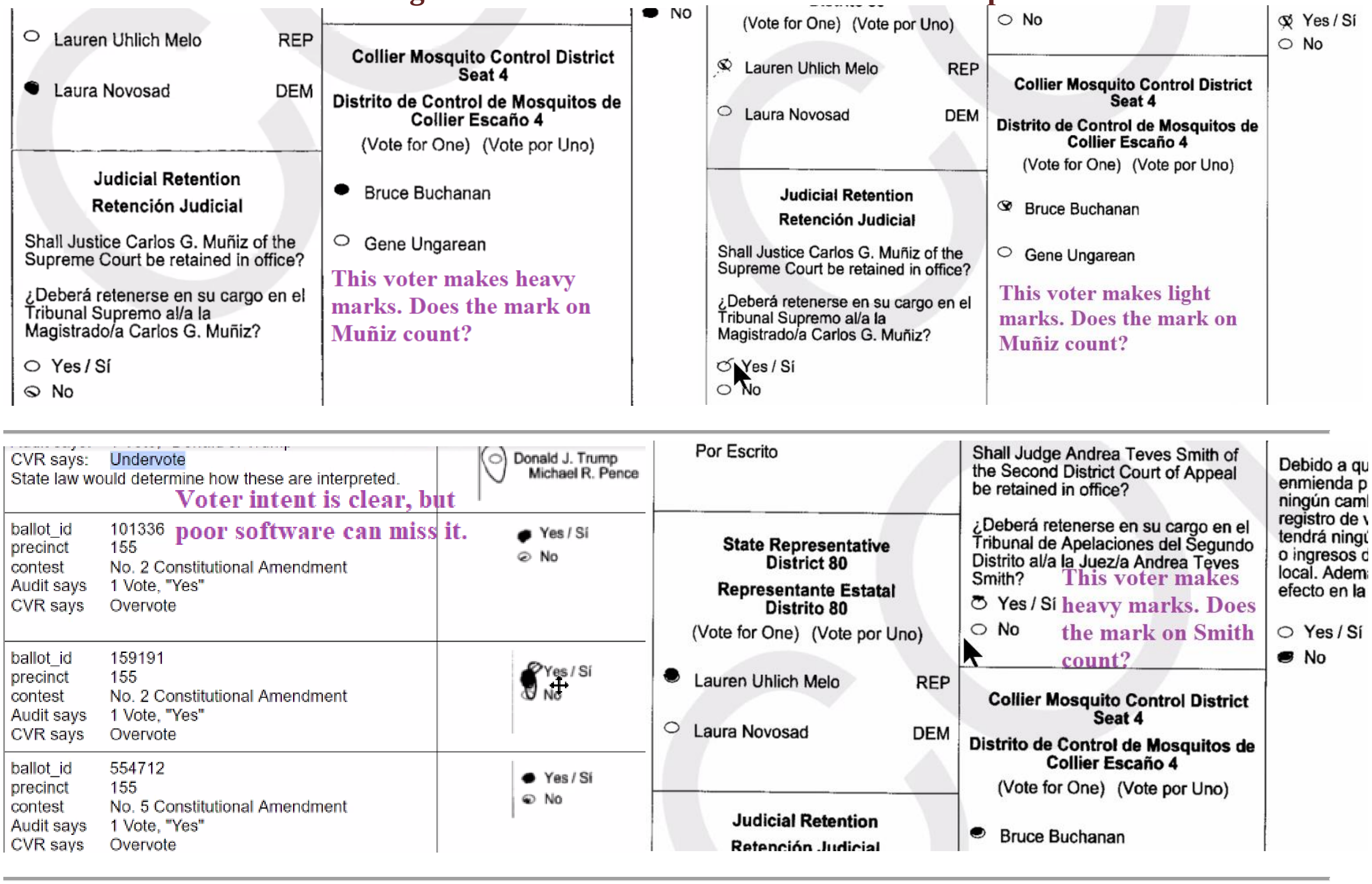
Publish machine tally of each batch.

Select a random sample of batches. Tally chosen contest in each batch. Compare to published tallies of those batches. If they don't match, expand sample of batches, potentially to 100% hand-tally of selected contest in remaining batches.

Other Aspects of Elections

Elections are complex, and all other aspects need regular monitoring, reporting and improvement: long lines, initial voter registration, list maintenance, impersonation, adding/changing/losing ballots before scanning, confusing ballots and instructions. *Comment on two other papers, on auditing eligibility and ballot-marking devices.*

Ambiguous Marks on Ballots for Humans to Interpret


○ Lauren Uhlich Melo REP
● Laura Novosad DEM
Judicial Retention
Retención Judicial
Shall Justice Carlos G. Muñiz of the Supreme Court be retained in office?
¿Deberá retenerse en su cargo en el Tribunal Supremo al/a la Magistrado/a Carlos G. Muñiz?
○ Yes / Sí
No
Collier Mosquito Control District Seat 4
Distrito de Control de Mosquitos de Collier Escaño 4
(Vote for One) (Vote por Uno)
● Bruce Buchanan
○ Gene Ungarean
No
(Vote for One) (Vote por Uno)
Lauren Uhlich Melo REP
○ Laura Novosad DEM
Judicial Retention
Retención Judicial
Shall Justice Carlos G. Muñiz of the Supreme Court be retained in office?
¿Deberá retenerse en su cargo en el Tribunal Supremo al/a la Magistrado/a Carlos G. Muñiz?
Yes / Sí
○ No
○ No
Collier Mosquito Control District Seat 4
Distrito de Control de Mosquitos de Collier Escaño 4
(Vote for One) (Vote por Uno)
Bruce Buchanan
○ Gene Ungarean
Yes / Sí
○ No
Donald J. Trump
Michael R. Pence
● Yes / Sí
No
Yes / Sí
No
● Yes / Sí
No
Por Escrito
State Representative District 80
Representante Estatal Distrito 80
(Vote for One) (Vote por Uno)
● Lauren Uhlich Melo REP
○ Laura Novosad DEM
Judicial Retention
Retención Judicial
Shall Judge Andrea Teves Smith of the Second District Court of Appeal be retained in office?
¿Deberá retenerse en su cargo en el Tribunal de Apelaciones del Segundo Distrito al/a la Jueza/a Andrea Teves Smith?
Yes / Sí
○ No
Collier Mosquito Control District Seat 4
Distrito de Control de Mosquitos de Collier Escaño 4
(Vote for One) (Vote por Uno)
● Bruce Buchanan
Debido a qu
enmienda p
ningún caml
registro de v
tendrá ningú
o ingresos d
local. Adem
efecto en la
○ Yes / Sí
● No

This voter makes heavy marks. Does the mark on Muñiz count?

This voter makes light marks. Does the mark on Muñiz count?

CVR says: Undervote
State law would determine how these are interpreted.

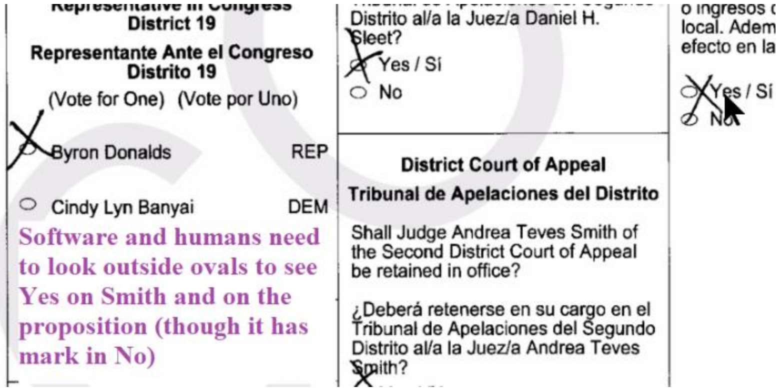
Voter intent is clear, but poor software can miss it.

ballot_id 101336
precinct 155
contest No. 2 Constitutional Amendment
Audit says 1 Vote, "Yes"
CVR says Overvote

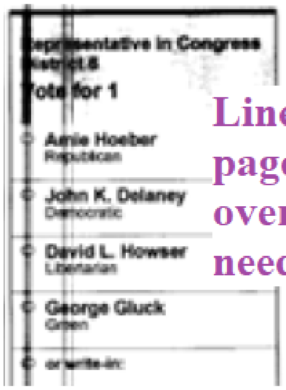
ballot_id 159191
precinct 155
contest No. 2 Constitutional Amendment
Audit says 1 Vote, "Yes"
CVR says Overvote

ballot_id 554712
precinct 155
contest No. 5 Constitutional Amendment
Audit says 1 Vote, "Yes"
CVR says Overvote

This voter makes heavy marks. Does the mark on Smith count?


Representative in Congress
District 19
Representante Ante el Congreso
Distrito 19
(Vote for One) (Vote por Uno)
Byron Donalds REP
Cindy Lyn Banyai DEM
Distrito al/a la Juez/a Daniel H.
Sleet?
Yes / Sí
No
District Court of Appeal
Tribunal de Apelaciones del Distrito
Shall Judge Andrea Teves Smith of the Second District Court of Appeal be retained in office?
¿Deberá retenerse en su cargo en el Tribunal de Apelaciones del Segundo Distrito al/a la Juez/a Andrea Teves Smith?
o ingresos
local. Adem
efecto en la
Yes / Sí
No

Software and humans need to look outside ovals to see Yes on Smith and on the proposition (though it has mark in No)



Lines down page create overvotes and need new scan

Errors in Hand Counts

Ansolabehere and Reeves (2004). "Using Recounts to Measure the Accuracy of Vote Tabulations: Evidence from New Hampshire Elections 1946-2002" CALTECH/MIT Voting Technology Project. They treated careful recounts as accurate, and any difference in the initial hand count for a candidate in each town was treated as error. Average error in candidate results in all towns except Bradford was 0.87%. However Bradford had up to 29% errors. Including Bradford meant overall the average error in candidate results was 2.5%. If races averaged 2 candidates per office (there could be 1, or 2, or more), then the average candidate had half the vote, so 2.5% error on candidate results means at least 1.25% of ballots had tallying errors. It is likely more ballots had errors, since some errors cancelled, and only the net result for each candidate in each town could be measured. In towns other than Bradford, at least 0.44% of ballots had errors.

Ansolabehere, Burden, Mayer, and Stewart (2018) "Learning from Recounts" Election Law Journal 17:2, found smaller average errors in candidate tallies for precincts in Wisconsin recounted in 2011 and 2016. The average discrepancy was 0.28% of the recount tally in 2011 and 0.18% in 2016. So at least half that many ballots had errors.

Beilman reports hand-counting errors were 3% to 27% for various candidates in a 2016 Indiana race, because the tally sheet labels misled officials into over-counting groups of 5 tally marks, and officials sometimes omitted absentee ballots or double-counted ballots. "Jeffersonville City Council At-large recount tally sheets show vote differences". News and Tribune 2/10/2016, Jeffersonville, IN.

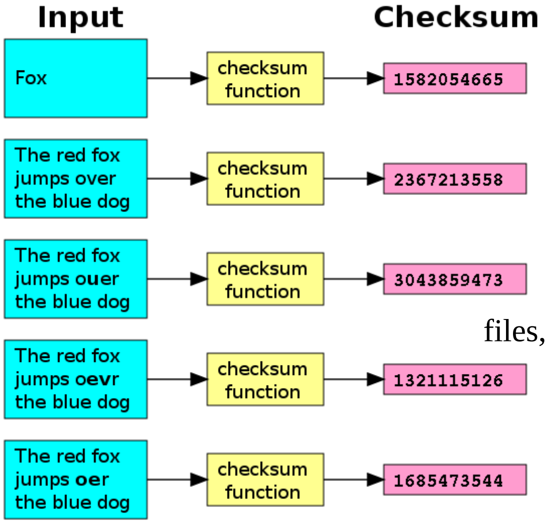
Wisconsin Election Integrity, a citizen group, has had success projecting ballot images in front of a large room of people, where two people have clickers for each candidate being tallied (i.e. 2 people clicking when they see a Biden vote, 2 for Trump votes, 2 for each other candidate being tallied). The pairs compared tallies frequently, and could go up to 300 ballots without mistakes. Anyone could call Stop at any time if they were unsure of a vote, and the group could agree publicly. For a large ballot this approach needs a large staff, and boredom could set in after a few hours. People who think a computer projector is suspect could use an opaque projector though these tend to be small, and changing ballots would be much slower.

When there are computer tallies for each batch, it is possible to hand-tally each batch, compare to computer tallies, and carefully resolve discrepancies. There would be a temptation to accept hand-tallies which match computer tallies, even though the goal is to check independently. I have not seen cost or accuracy measures for this approach.

Both manual approaches are still subject to summation errors and omissions as reported above for Jeffersonville, IN.

Digital Signatures

It is common practice in computer files to take the ones and zeros which make up the file, calculate a special formula which gives a summary number (checksum, hash value, digital signature), and make a permanent record of this number (such as on paper). When other people get the file, they can run the same formula and see if they get the same summary number. Any change in the file, even moving a dot from one place to another, gives a substantially different summary number, so people can go back and insist on getting the correct file. This is much more secure than paper records where forgeries can fool experts.



Checksum is a general term. Hash value and digital signature are more specific and technical terms. The Unix "cksum" utility generates 10 digits. [59]

For elections the summary number needs to be given to the public and/or auditors, so they can identify true copies of the original files.

Microsoft has an explanation of hashes.[60]

On the same page where San Francisco issues their ballot image files, they offer a "SHA" file with a 512-bit hash value for each image file, using the SHA-512 algorithm.[61] Copies of the hash values can also be picked up on paper in person if desired.[62] A better approach would be to create for the file of signatures, a hash which is short enough to read over the phone for checking. San Francisco uses software from QuickHash.[63]

ES&S scanners create digital signatures for image files, though it is not clear they have ever been released to verify the files later.[64]

SHA-512 provides the best assurance that the file is unchanged, if you compare every hash value, character-by character, by hand (since a computer comparison could be erroneous). The value is 512 bits long, which they print in hexadecimal, so they represent 4 bits in each character, cutting the length to 128 characters. Manually comparing signatures of 128 characters seems unrealistic, and there needs to be expert discussion of the reliability of checksums (such as the first or last 6 digits of SHA-512) which are short enough for manual checking.

Colorado has each county calculate hash values on the files electronically sent to the Secretary of State. These hash values are also sent electronically, so a man-in-the-middle attack could corrupt both.[65]

Sample Size Calculations

When errors affect 1% of ballots, sample of 500 ballots has 96% chance that 2 or more batches will see an error. On the other hand when errors affect 0.5% (half a percent) of ballots, the same sample of 500 ballots has 70% chance that 2 or more batches will see error.

If one is willing to rescan all ballots when even one error is found anywhere, the sample can be smaller, or the same sample can catch smaller error rates, but it is against human nature to admit a widespread problem when just one error has been found. Also staff can be unwilling to admit that an error is found when just one error generates a large workload of rescanning.

The spreadsheet at http://votewell.net/vote.xlsx shows these calculations and lets you examine different sample sizes, error levels and jurisdiction sizes. It shows that jurisdiction size has little effect on sample size needed.

1,000 sampled ballots have 96% chance of twice catching errors which affect half a percent of ballots.

It is important for the sample to have some ability to check small errors, down to at least 1% of ballots. While most contests are not close, some are, and US elections have many contests on each ballot to check. It is common for at least one contest on each ballot to be close. From 2014 to 2017, 2% to 5% of election contests had winning margins within one percentage point in Colorado, Massachusetts and West Virginia. 11% to 21% were within five percentage points.

Sub-jurisdictions: These samples are defined for the whole jurisdiction, typically a county, and their effectiveness is given for jurisdiction-wide contests, such as county officials and most state and federal officials. A sample of 500 ballots county-wide will have fewer ballots in small towns or other special districts, so will only catch bigger errors in these small towns.

For example, a town which contains 10% of the jurisdiction's ballots, will have about 10% of the sample. In that size town and sample, an error which affects 6% of ballots has 80% chance of catching 2 errors. On the other hand, the same sample has 95% chance of catching 1 error. So if batches are grouped by precinct, and they are willing to re-scan just the ones from that town when even one discrepancy is found, there is 95% chance of finding and fixing the 6% errors, and 64% chance of finding and fixing errors which affect only 2% of ballots in the town.

For checking results in a town's election, the sample outside of town is also valuable. It will identify and tally any ballots from that town, which were mis-classified elsewhere in the initial processing, so they can be included in checking results for the town. If only the town is sampled (for example an RLA drawn from CVRs for the town), there needs to be a supplemental sample of other ballots to find town ballots not initially classified right.

The spreadsheet at http://votewell.net/vote.xlsx lets you examine other town sizes, sample sizes, and error levels.

The US has **standards** for verifying images in ANSI/AIIM TR34: 1996 (“ANSI/AIIM TR34”), Sampling Procedures for Inspection by Attributes of Images in Electronic Image Management and Micrographic Systems, May 13, 1996, https://law.resource.org/pub/us/cfr/ibr/001/aimm.tr-34.1996.pdf incorporated into federal regulations at 36 CFR § 1237.3(b)(4) These standards discuss samples where as many as 4% of images can be accepted as flawed (4% on p.8. Or 1% on pp.55-56).

Missing ballots or images: Sometimes we know or suspect that some ballots have been lost, and they cannot be found, such as because of a theft, or a fire in the delivery vehicle. The first question is whether enough were lost to change some contests' outcomes. If so, officials and/or a judge have to decide whether to:

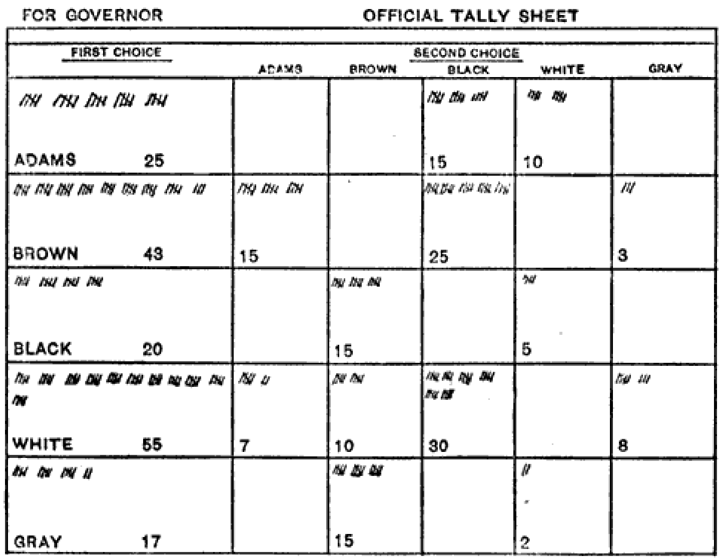
A. Use ballot images if they have already been made, and if other images are found to be reliable,
B. Obtain new votes from the voters or neighborhood whose ballots were lost, if they can be identified,
C. Have a whole new election for all voters,
D. Base the result on remaining votes which have not been lost.

If the missing votes are *too few* to change outcomes, ballot image audits can ignore them. However RLAs depend more on their sample. RLAs still need to add a corresponding number of pretend ballots to the sample, treat them as votes for losers, and see if the *sample* can still confirm the winner or call for a 100% hand tally.

Approval voting: The same sample size calculations apply to approval voting, where voters mark as many candidates as they wish, and winner is the one with most votes.

Ranked choice voting and similar: A sample can also check ranked choice voting (RCV) instant runoff voting (IRV), or single transferrable vote (STV), where voters number the candidates. Candidates are sorted by the number of ballots who ranked that candidate #1. Lowest candidate is eliminated, and ballots which had named that candidate #1are added to other candidates based on these ballots #2 choice. Then new lowest remaining candidate is eliminated and those ballots are also distributed to others, etc. One sample checks all stages.

Hand-tallying RCV or IRV ballots, or a sample of them, takes slightly more time than plurality or approval voting: In each team, for each contest, one person, watched by another, reads each ballot's first and second choices:[66] "For Governor, Brown first, Gray second," and stacks them in a separate pile for each combination. Others can independently tally in a matrix at the same time, or wait and count the stacks. This step takes the same time as plurality or approval voting. The first two rounds of elimination can be done from this matrix. If more rounds are needed, the losers' stacks can be re-sorted to conduct the next rounds, which take little time, since the losers by definition had the fewest ballots. Sample size for audits by hand-tallying a sample in this way needs consideration of the margin at each stage, which does not have a published approach.



FOR GOVERNOR OFFICIAL TALLY SHEET

FIRST CHOICE		SECOND CHOICE				
		ADAMS	BROWN	BLACK	WHITE	GRAY
ADAMS	25			15	10	
BROWN	43	15		25		3
BLACK	20		15		5	
WHITE	55	7	10	30		8
GRAY	17		15		2	

Machine selection and analysis of cast vote records for an RLA is described by Blom et al.[67] They use software to choose a sample size and "sample only cards with CVRs that contain particular contests." Then they manually require "the auditors to record what they see on the ballot." The approach uses software to identify hypotheses which would yield a different winner, select enough sample to reject each hypothesis with statistical confidence, and calculate the risk limit on the combined result. The process uses SHANGRLA software which "incorporates several different statistical risk measurement algorithms." They identify the Kaplan-Martingale function. Instead of adjusting the tests for the presence of multiple hypotheses,[68] they take the approach that "there are multiple null hypotheses, but the audit reverts to a manual count if any one of them can't be rejected."[69] They also say "you can trust SHANGRLA or choose to reimplement your own." SHANGRLA is open source, and:

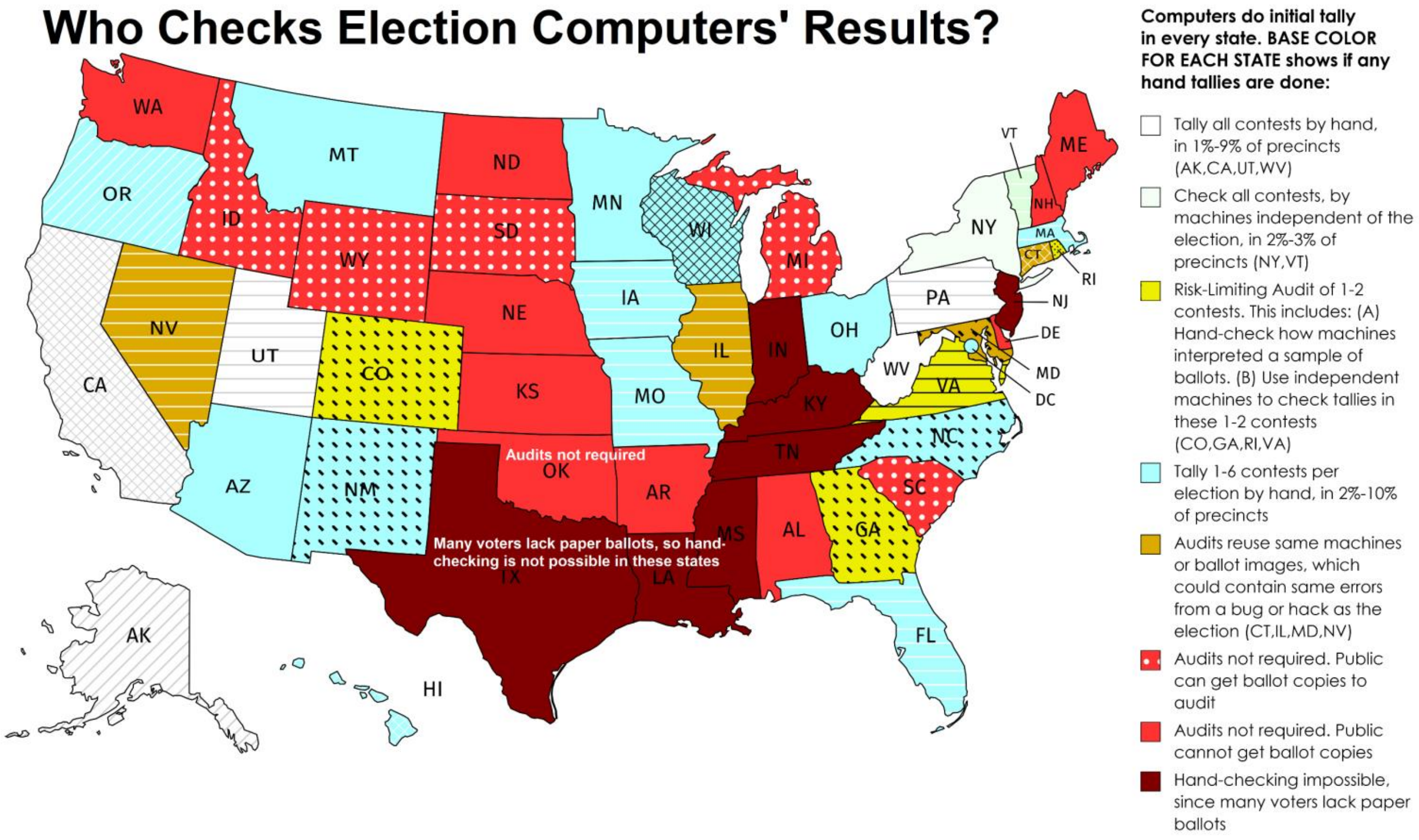
1. There is no way for the election office or public to know what program is really running inside a high-risk machine.
2. So observers also need to run their own program (or a copy of SHANGRLA which they have verified) on the data, on their own machine.
3. SHANGRLA selects CVRs and corresponding ballots from a seed it is given. Observers need to see that the seed is randomly selected, re-run the software to see that the CVR selections followed from this seed, and see that sample ballots are immediately examined without time to alter them.
4. Public display of sample paper ballots needs to be slow enough in an RLA to let observers copy down the rankings on each ballot for this later independent reanalysis.
5. Independent observers need to understand and evaluate the statistics needed.
6. Observers who disagree need a transparent way to resolve disagreements.

A *ballot image audit* can also handle the example of ranked choice voting in the paper by Blom et al. It would, like all ballot image audits, start by comparing a good sample of ballots to images, to verify the image files. Then independent auditors would rerun all stages of interpreting the image files to create independent CVRs, tallying and eliminating candidates to find the election winner, using 100% of the image files. If independent auditors disagree on the tallies and winner, they can pinpoint the discrepancies, as in any ballot image audit, examine them, and get a judge's ruling if needed. Statistical tests would tell how much confidence the overall result has, given the sample size and design. If statisticians disagree on the statistical tests, their disagreement does not affect the winner. It just affects the confidence reported.

Endnotes

[1] **31 states audit:** *No Audit* in Alabama, Arkansas, Delaware, Idaho, Kansas, Louisiana, Maine, Michigan, Mississippi, New Hampshire, New Jersey, North Dakota, Oklahoma, South Carolina, South Dakota, Texas, Wyoming. Audits done only if officials choose to in Indiana. Nebraska, Washington. (*Total of 20 states, out of 51 states and DC*).

Table of state audit rules: http://www.votewell.net/audits.html



Who Checks Election Computers' Results?

Computers do initial tally in every state. BASE COLOR FOR EACH STATE shows if any hand tallies are done:
□ Tally all contests by hand, in 1%-9% of precincts (AK,CA,UT,WV)
□ Check all contests, by machines independent of the election, in 2%-3% of precincts (NY,VT)
Risk-Limiting Audit of 1-2 contests. This includes: (A) Hand-check how machines interpreted a sample of ballots. (B) Use independent machines to check tallies in these 1-2 contests (CO,GA,RI,VA)
Tally 1-6 contests per election by hand, in 2%-10% of precincts
Audits reuse same machines or ballot images, which could contain same errors from a bug or hack as the election (CT,IL,MD,NV)
Audits not required. Public can get ballot copies to audit
Audits not required. Public cannot get ballot copies
Hand-checking impossible, since many voters lack paper ballots
Audits not required
Many voters lack paper ballots, so hand-checking is not possible in these states
WA
OR
CA
ID
NV
MT
WY
UT
AZ
CO
NM
ND
SD
NE
KS
OK
TX
MN
IA
MO
AR
LA
WI
IL
MI
IN
OH
KY
TN
MS
AL
GA
FL
SC
NC
VA
WV
PA
NY
VT
NH
ME
MA
CT
RI
NJ
DE
MD
DC
AK
HI

All states tally votes with computers, which have bugs, and can be hacked by insiders or annual updates. If ballots or copies are made available, independent tallies can check results.
DIAGONALS mean some types of ballots are excluded from checking: AK,OR-small precincts; CA-ballots not tallied on election day (43%); CT,WI-early+absentee+provisional ballots; WI-primaries
HORIZONTAL lines: laws do not require results to be corrected when audits find errors: CA,CT,FL,HI,IA,IL,MA,MO,NV,PA,UT,VA,VT,WI
CROSSHATCH: both the above problems: CA,CT,WI
BLACK dots or lines: audited contests have good samples of ballots, likely to catch any significant errors by machines interpreting ballots in the races checked: CO,MD,NC,NM,RI,VA
Sources: State laws and rules for 2020, as cited at VerifiedVoting.org/auditlaws Color version at commons.wikimedia.org/wiki/File:State_audits.png

[2] **Omit many contests** from audits: They audit **1** contest in Colorado, Iowa, Florida, Georgia, Tennessee, North Carolina, Washington. **2-4** contests in Minnesota, Oregon, New Mexico, Connecticut, Ohio, Hawaii, Wisconsin, District of Columbia, Montana. **5-6** in Arizona, Missouri, Massachusetts, Texas. **Unknown** in Rhode Island, Virginia.

Officials audit **all** contests in Alaska, California, Illinois, Indiana, Kentucky, Maryland, Nevada, New York, Pennsylvania, Utah, Vermont, West Virginia.

[3] **Audits omit many ballots:** Alaska, Oregon-small precincts; California-ballots not tallied on election day (43% in 3/20); Hawaii, Virginia, Wisconsin-early & absentee ballots; Ohio, Wisconsin-primaries.

Laws do **not** require results to be corrected when audits find errors in: California, Connecticut, Florida, Hawaii, Iowa, Illinois, Massachusetts, Missouri, Nevada, Pennsylvania, Utah, Virginia, Vermont, Wisconsin

[4] Only the District of Columbia and Massachusetts require that the public can see ballot markings during audit, to verify staff accuracy. http://www.votewell.net/audits.html

[5] **Embezzlement arrests**: https://www.ojjdp.gov/ojstatbb/crime/ucr.asp?table_in=1

[6] 67,000 reports of computer breaches: https://www.securityweek.com/deep-analysis-more-60000-breach-reports-over-three-years Most were reported by the hackers. Only13% were reported through official channels. These were not reported at election companies or local governments. If hackers don't reveal election theft, we won't know.

[7] *2020 Cost of **Insider Threats** Global Report*. Sponsored by ObserveIT and IBM https://go.proofpoint.com/wp-ponemon-itm-cost-of-insider-threats.html

[8] Brennan Center list of voting machine errors,"brennancenter.org/sites/default/files/2019-08/Report_Voting_Machine_Failures_Database-Solution.pdf In addition, Heritage has a database of 1,300 fraud from 1982-2000. Three quarters involved ineligible people voting, and the other quarter included fraud by election officials https://www.heritage.org/voterfraud/search Assessed by Brennan Center https://www.brennancenter.org/sites/default/files/2019-07/Report_HeritageAnalysis_Final.pdf

[9] RLAs are supported by the American Statistical Association, Common Cause, Public Citizen and other groups. https://electionaudits.org/files/Audit%20Principles%20and%20Best%20Practices%202018.pdf

Doubts about RLAs in actual practice have been voiced by Mercuri https://www.cnet.com/news/electronic-voting-and-partial-audits/ and Citizens Oversight https://copswiki.org/Common/M1938

[10] Lindeman+Stark, Gentle Introduction to Risk-limiting Audits stat.berkeley.edu/~stark/Preprints/gentle12.pdf

[11] **Unreliable locks:** Insiders go in with keys: Cuyahoga County, OH (Cleveland) election workers entered storage rooms in advance and secretly went through the ballots to make public audits appear problem-free. In court these staff "*countered that the board had always done things that way - with the knowledge of its attorney*," Turner, Karl. (2007-11-5). "Elections board workers take plea deal." Cleveland Plain Dealer.

Since 1850, people have known how to create a master key from any key in a building, such as a borrowed restroom key. Blaze, Matt. "Cryptology and Physical Security: Rights Amplification in Master-Keyed Mechanical Locks" "few institutions want to spend the money for robust security... in a battle between convenience and security, convenience has a way of winning." "Many Locks All Too Easy To Get Past". New York Times, 1/23/2003. Atttackers who cannot find key blanks can 3D-print them from a photo of the lock: Burgess, Wustrow & Halderman; (2015). "Replication Prohibited: Attacking Restricted Keyways with 3D-Printing"

"Roger Johnston... has conducted vulnerability assessments on more than a thousand physical security and nuclear safeguard devices, systems, and programs. It's his opinion that all security technologies and devices can be defeated—usually 'fairly easily'...

"The typical security manufacturer isn't likely to have good insider threat security, so product tampering at the source is a risk...Then [the security device] will sit on loading docks, and then sit again, sometimes for months, somewhere at the end user, and only then is it installed" said Johnston. "But no one knows what the interior is supposed to look like, and manufacturers don't supply pictures, so it's impossible to tell signs of tampering."

... "The problem at a lot of organizations is that they're afraid to encourage employees to think about these kinds of things, and they're also afraid of what they'll find... many don't want to see the expensive technology they bought easily compromised... Looking at your security devices from the perspective of attackers will always point out flaws... acknowledge that they are a possibility... And appreciate which threats devices can and can't protect against." http://losspreventionmedia.com/insider/retail-security/physical-security-threats-and-vulnerabilities/

Access to locked courthouses: "*gained access to the building's server room, and even found that a judge had left their computer open and unlocked on their bench at the front of a courtroom. Underneath the laptop, for good measure, was a sticky note with a password written on it... hundreds of white-hat hackers who work across the US as professional penetration testers—the rare kind that perform physical intrusions rather than mere over-the-internet hacking... few nights' string of intrusions... many of the alarm systems they'd encountered in the past weren't properly armed and never actually dialed out to responders... glaring vulnerabilities in the security of the state's judicial system. Those vulnerabilities, they say, were swept under the rug... Coalfire staffer had easily gotten into a courthouse during daylight hours by impersonating a state IT worker. Then he'd simply sat down and plugged a computer into the network... They snaked a tiny boroscope camera under doors to check for alarms or security guards. They picked old-fashioned pin-and-tumbler locks on doors and desk drawers with simple lock picking tools, finding key cards in drawers and using them to get past other internal doors in the building. They used DeMercurio's cutting board shim trick and a tool that slides under a door and reaches up to hook its inside handle. At one point they made clever use of a can of compressed air—the kind meant for cleaning dust out of keyboards—to trigger an infrared motion sensor: Angle the propellant gas through the door's crack to the sensor inside, and it registers as a temperature change, tricking the sensor into believing a person had approached from within and unlocking the door to let them out... between those windows and the building's server room, there wasn't a single locked door... the Iowa judicial branch seems to have taken entirely the wrong lesson from the whole Coalfire affair. A new set of precautions it released last October forbids courthouse break-ins of the kind Coalfire performed entirely. Never mind that Coalfire's testing revealed security flaws as basic as unlocked doors and windows, ones that could be used to access highly sensitive criminal justice information like juror identities and evidence. "They just said 'We're obviously insecure, and now we're going to make sure we never test again,'""* wired.com/story/inside-courthouse-break-in-spree-that-landed-two-white-hat-hackers-in-jail/

Lockpicking is widely taught and practiced:. "The Strange Things That Happen at a Lock-picking Convention".. Different techniques apply to electronic locks:. "Exclusive: High-security locks for government and banks hacked by researcher".and. "Inside an Epic Hotel Room Hacking Spree". Lockpicking is a legal sport: https://en.wikipedia.org/wiki/Locksport

[12] **Unreliable seals:** "*no seal is unspoofable (just as no lock is undefeatable)... The optimal choice of a seal depends on the details of your security goals, threats, and adversaries and your personnel... amateurs can attack seals in a way that leaves little (and sometimes no) evidence... Sometimes the consternation and delays that a suspicious seal creates for superiors... make front-line employees reluctant to raise their concerns."* http://www.alu.army.mil/alog/issues/JulAug12/Choose_Use_Seals.html

When seals are missing or broken, nothing usually can be done. *"An attacker who simply cuts, removes, or destroys tamper-indicating seals (without doing anything else) can attempt to call the legitimacy of the election into question... it must be difficult for the attacker to counterfeit a seal... I am not sure how much experience with injection-molding of plastics one needs to be able to do this, but really that is rarely the point: in the vast majority of cases there are much easier attacks—either the simple removal and replacement of the original seal, or the purchase of extra (legitimate) seals and changing their serial number, or the purchase of extra seals to re-use some of their parts with the serial number of the original seal... I demonstrated for the judge the complete removal and replacement of all seals with no visible evidence of tampering... 'To the court's untrained eye, most of the seals appeared unaltered with a few showing minimal damage.' [Opinion 2010, p. 52]... corrupt election officials may hire corrupt seal inspectors... or deliberately fail to train them... Consider an audit or recount of a ballot box, days or weeks after an election... The tamper evident seals are inspected and removed—but by whom?... the public must be able to receive training on detection of tampering of those particular seals."* https://www.cs.princeton.edu/~appel/voting/SealsOnVotingMachines.pdf

[13] Morrell. Ballot Accounting Audits Best Practices Guide. https://democracyfund.org/idea/knowing-its-right-limiting-the-risk-of-certifying-elections/

[14] Michigan: detroitnews.com/story/news/politics/2016/12/12/records-many-votes-detroits-precincts/95363314
Wayne County:https://www.detroitnews.com/story/news/politics/2016/12/05/recount-unrecountable/95007392/

[15] Colorado, Georgia and Rhode Island have done **statewide RLAs.**
Maryland did a test in two counties. Maryland State Board of Elections. (2016-10-04). "Post-Election Tabulation Audit Pilot Program Report." Page 16.
California tested RLAs in several counties, which generally created ballot images and sent them by internet to a graduate student at the University of California at San Diego (UCSD) for independent counting. The report does not mention hash values or UCSD's computer security. California Secretary of State. (2014-07-30). "Post-Election Risk-Limiting Audit Pilot Program 2011-2013, Final Report to the United States Election Assistance Commission." Pages 12-13, 16

[16] Maryland State Board of Elections. (2016-10-04). "Post-Election Tabulation Audit Pilot Program Report." Page 27.

[17] Weighing ballots on scale: If batch includes different types of ballots, such as computer-generated or mailed, they need to be weighed separately, with separate lookup tables to give count of ballots for each weight. Weighing is endorsed in item 4e *"weighing ballot batches on a precision scale"*, on page 12 of https://electionaudits.org/files/Audit%20Principles%20and%20Best%20Practices%202018.pdf A page of 8.5 x 11 paper (20-pound bond or 50-pound offset) weighs 4.54 grams or a sixth of an ounce. The scale has to be accurate enough to make those distinctions in piles of 200 to 500 ballots (2-5 pounds), 1 part in 200-500. Weights are proportionately heavier for 24-pound paper and larger ballots. An electronic scale can be that accurate, and may be trusted more than hand-counting the piles. https://www.mt.com/us/en/home/library/know-how/industrial-scales/weighing_votes.html

[18] **Ballot image audits:** Humboldt County CA since 2008. "Unique Transparency Program Uncovers Problems with Voting Software". *Wired*.
Seven counties in Florida: Stofan, Jake. (2018-04-25). "Leon County among Florida precincts to implement Clear Audit for elections." *WCTV*.
Clear Ballot (2016-12-14). "Clear Ballot's Audit of Florida's Presidential Election Results a Success."
Six towns in Vermont: Elder-Conors, Liam. (2016-11-23). "Vermont Secretary of State's Office to Audit Election Results from 6 Towns." Vermont Public Radio.
Vermont Secretary of State. (2014-11-17). "Secretary of State Jim Condos to conduct election audit."
Maryland: Moretti, M. Mindy. (2016-12-08). "Maryland conducts first statewide audit of election results." *electionlineWeekly*.
Walker, Natasha. (2017-02-13). "2016 Post Election Audits in Maryland."U.S. Election Assistance Commission's Technical Guidelines Development Committee.
Ryan, Tom and Benny White. (2016-11-30). "Transcript of Email on Ballot Images." Pima County, AZ email concerning Maryland experience.
Lamone, Linda H. (2016-12-22). "Joint Chairman's Report on the 2016 Post-Election Tabulation Audit." Maryland State Board of Elections.
Maryland State Board of Elections. (2016-10-04). "Post-Election Tabulation Audit Pilot Program Report."

[19] Checks are shredded: "check truncation" https://www.ffiec.gov/exam/check21/faq.htm
"The lack of access to original checks necessitates the need for revised check review procedures and employee training, and a review of check security features such as watermarks." https://www.fdic.gov/news/news/inactivefinancial/2004/fil5404.html

[20] **Cast Vote Records** are computer files showing voter choices from each ballot. They can be spreadsheets, with one row per ballot and one column per contest or per candidate. Each cell shows the voter's choice for the contest, as interpreted by the election computer. For multi-sheet ballots, there may be one row for each sheet of the ballot.

[21] Software independence was defined by Rivest, 2008 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.140.2530&rep=rep1&type=pdf

[22] Easy creation of master keys: Blaze, Matt. "Cryptology and Physical Security: Rights Amplification in Master-Keyed Mechanical Locks"

[23] Easy creation of key blanks: Burgess, Wustrow & Halderman; (2015). "Replication Prohibited: Attacking Restricted Keyways with 3D-Printing"

[24] Johnston on physical security: http://losspreventionmedia.com/insider/retail-security/physical-security-threats-and-vulnerabilities/

[25] Turner, Karl. (2007-11-5). "Elections board workers take plea deal." Cleveland Plain Dealer.

[26] Government covert entry: Electronic Frontier Foundation, "Peekaboo, I See You: Government Authority Intended for Terrorism is Used for Other Purposes". Also McGuire, Sneak and Peek Warrants-Necessary for our Safety...?

[27] **Locks on drop boxes:** https://www.forbes.com/sites/marcwebertobias/2020/11/09/the-security-of-ballot-collection-boxes-one-can-be-opened-in-thirty-seconds-or-less/?sh=204e80b45f76

[28] Coalfire testing of courthouse security: wired.com/story/inside-courthouse-break-in-spree-that-landed-two-white-hat-hackers-in-jail/ "*gained access to the building's server room, and even found that a judge had left their computer open and unlocked on their bench at the front of a courtroom. Underneath the laptop, for good measure, was a sticky note with a password written on it... hundreds of white-hat hackers who work across the US as professional penetration testers—the rare kind that perform physical intrusions rather than mere over-the-internet hacking... few nights' string of intrusions... many of the alarm systems they'd encountered in the past weren't properly armed and never actually dialed out to responders... glaring vulnerabilities in the security of the state's judicial system. Those vulnerabilities, they say, were swept under the rug... Coalfire staffer had easily gotten into a courthouse during daylight*

hours by impersonating a state IT worker. Then he'd simply sat down and plugged a computer into the network... They snaked a tiny boroscope camera under doors to check for alarms or security guards. They picked old-fashioned pin-and-tumbler locks on doors and desk drawers with simple lock picking tools, finding key cards in drawers and using them to get past other internal doors in the building. They used DeMercurio's cutting board shim trick and a tool that slides under a door and reaches up to hook its inside handle. At one point they made clever use of a can of compressed air—the kind meant for cleaning dust out of keyboards—to trigger an infrared motion sensor: Angle the propellant gas through the door's crack to the sensor inside, and it registers as a temperature change, tricking the sensor into believing a person had approached from within and unlocking the door to let them out... between those windows and the building's server room, there wasn't a single locked door... the Iowa judicial branch seems to have taken entirely the wrong lesson from the whole Coalfire affair. A new set of precautions it released last October forbids courthouse break-ins of the kind Coalfire performed entirely. Never mind that Coalfire's testing revealed security flaws as basic as unlocked doors and windows, ones that could be used to access highly sensitive criminal justice information like juror identities and evidence. "They just said 'We're obviously insecure, and now we're going to make sure we never test again,'""

[29] Lockpicking sport: "The Strange Things That Happen at a Lock-picking Convention"

[30] Electronic locks: "Exclusive: High-security locks for government and banks hacked by researcher".and. "Inside an Epic Hotel Room Hacking Spree"

[31] Appel on seals https://www.cs.princeton.edu/~appel/voting/SealsOnVotingMachines.pdf *"An attacker who simply cuts, removes, or destroys tamper-indicating seals (without doing anything else) can attempt to call the legitimacy of the election into question... it must be difficult for the attacker to counterfeit a seal... I am not sure how much experience with injection-molding of plastics one needs to be able to do this, but really that is rarely the point: in the vast majority of cases there are much easier attacks—either the simple removal and replacement of the original seal, or the purchase of extra (legitimate) seals and changing their serial number, or the purchase of extra seals to re-use some of their parts with the serial number of the original seal... I demonstrated for the judge the complete removal and replacement of all seals with no visible evidence of tampering... 'To the court's untrained eye, most of the seals appeared unaltered with a few showing minimal damage.' [Opinion 2010, p. 52]... corrupt election officials may hire corrupt seal inspectors... or deliberately fail to train them... Consider an audit or recount of a ballot box, days or weeks after an election... The tamper evident seals are inspected and removed—but by whom?... the public must be able to receive training on detection of tampering of those particular seals."*

[32] Johnston & Warner on seals http://www.alu.army.mil/alog/issues/JulAug12/Choose_Use_Seals.html *"But no one knows what the interior is supposed to look like, and manufacturers don't supply pictures, so it's impossible to tell signs of tampering."*

... "The problem at a lot of organizations is that they're afraid to encourage employees to think about these kinds of things, and they're also afraid of what they'll find... many don't want to see the expensive technology they bought easily compromised... Looking at your security devices from the perspective of attackers will always point out flaws... acknowledge that they are a possibility... And appreciate which threats devices can and can't protect against."

[33] **Linking paper ballots to their images:** Batches of centrally scanned ballots are in the same order as images, so matching them is straightforward. Ballots scanned in polling places fall randomly into ballot boxes, so are not in the same order as images.

It is best to scan ballots centrally, not at polling places where the scanners are widely vulnerable to errors and meddling.

If a jurisdiction scans in polling places, there are still options. When a sample of precinct-scanned ballots is selected, one approach is to use software to search the image file for the image with corresponding choices. If multiple images match, the shapes of voter marks vary enough to find the corresponding image and manually decide if the scan is a good copy of the paper ballot. If no image matches, the scan was unreliable and needs to be redone.

Another approach is to have the polling place scanners print a number on the ballot corresponding to the image, using a rare ink color, like brown or orange, so it can't be accused of adding votes.

A final approach is re-scanning in a sequential batch, as done with Clear Ballot in seven Florida counties https://www.wctv.tv/content/news/Leon-County-among-Florida-precincts-to-implement-Clear-Audit-for-elections-480847661.html and six Vermont towns https://www.vpr.org/post/vermont-secretary-states-office-audit-election-results-6-towns#stream/0

[34] The value of **checking all contests**, not just a sample, is that

(a) All contests matter. There are millions of dollars at stake in land use decisions and public spending in every local election, whether schools, council, prosecutor, judge, sheriff, etc. Many people see that elections for President and Congress have high consequences. Students are far more affected by school board decisions on what is taught, how and by whom. Property values and neighborhood quality are far more affected by zoning, school siting and law enforcement decisions. Even where only 10% of adults vote in local elections, the ability of these informed, committed voters, often teachers, to choose candidates without election errors, protects the other 90% of citizens from the worst candidates.

(b) Audits of random contests have no deterrence effect on other contests, so all contests must be checked, because penalties for being caught are minimal: Few frauds are caught, it is nearly impossible to prove a mistake was intentional or who did it, crime families doing election theft will sacrifice peons, foreigners won't be extradited for trial, and sentencing guidelines have tiny penalties: Election offenses start at "level" 8 to 14, which give prison terms for a first offender of 0-21 months and a $2,000-$75,000 fine. Sentences can be adjusted up or down depending on circumstances. Michael Cohen's 3-year sentence for multiple major convictions, including his illegal campaign contribution, is a good example. He served a year in prison.

[35] **Cast Vote Records** are computer files showing voter choices from each ballot. They can be spreadsheets, with one row per ballot and one column per contest or per candidate. Each cell shows the voter's choice for the contest, as interpreted by the election computer. For multi-sheet ballots, there may be one row for each sheet of the ballot.

In any case, the CVR rows and ballots and ballot images don't show the voter's name, since they come from the ballot, which does not have the voter's name. CVRs reflect the computer's understanding of a voter's choices, and usually identify the precinct, and type of ballot issued, such as different party ballots used in a primary. They do not identify which voter filled out those choices, unless the voter herself did something unique, such as writing her own name in a write-in space, or she had the only Libertarian ballot in the precinct.

You can see examples of CVRs and ballot images, online from Dane County WI (ES&S machines) and San Francisco (Dominion machines).

[36] **Check totals of cast vote records:** Lindeman+Stark, Gentle Introduction to Risk-limiting Audits. p.3, section B(i) "*ballots sum to the contest totals for every candidate.*" https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf.

Item 4b *"reconciliation to ensure that all votes from all audit units are correctly summed in the election totals*", on page 12 of https://electionaudits.org/files/Audit%20Principles%20and%20Best%20Practices%202018.pdf

Lindeman et al. Comments re statistics of auditing the 2018 Colorado elections. p.2. "*the Secretary of State has the ability to compare reported contest results with the CVRs it receives, but there is no publicly observable means to verify that this comparison has been done correctly.*" https://www.sos.state.co.us/pubs/elections/VotingSystems/riskAuditFiles/NotesOnStatistics-2018ColoradoPrimariesElectionAudit.pdf

[37] Ballots often have two double-sided sheets of paper, containing 4 pages of selections. They may have more, or they may have one sheet. 2-person teams scan sheets in batches. A convenient batch size is 200 sheets. This is easy to lift, keep straight and handle, doesn't create too many records, and doesn't take too much time to count to a random point in the batch to check a random ballot. Time needed per batch, initial estimates:

- 2 minutes to pull sheets from box and scan (see below to adapt for ballots scanned at precincts)
- 1 minute to print 10 copies of digital signature and give to observers and multiple officials. The digital signature does not reveal contents of the images; images themselves are not distributed or tallied before election day. Simultaneously weigh batch on accurate enough scale to give the number of sheets, compare to scanner count of images. Any mismatch means a misfeed.
- 1 minute to get 2 random numbers (from dice, lottery balls etc.)
- 3 minutes average to count to those 2 random sheets in stack (by hand, machine or scale)
- 2 minutes to *electronically project the 2 random images*, and use *opaque projector to project the corresponding 2 sheets*, on screen for public comparison. Observers can photograph all or some of these images to verify later that these are in the digital file when the file is available after election day.
- 1 minute average to close out box or resolve problems (usually zero problems, occasionally will have misfeed or scanner flaw and need 10 minutes to re-scan and re-check or count again to the right ballot)
- 10 minutes total per batch, instead of 2 minutes pure scanning and boxing time

If these times are even close, officials can do these steps with early and mailed ballots every day as they arrive, before election day. Each team can do 40 batches per shift (40 x 10' = 400' = 6h 40m). In 2 weeks, 10 working days, each team can do 400 batches. At $15/hour and 2 staff per team, two weeks cost $2,400. A big county with a million ballots and 2 million sheets will have 10,000 batches, 200 sheets per batch, an average of 1000 batches per day in the 2 weeks before election day, so they need 25 teams, costing a total of $60,000. If most ballots come in the last week, they can have more teams, using more space, or 2 shifts, in the last week.

10,000 batches give random sample of 20,000 verified images, which should let people trust the image files even on close elections. Dr. Stark's tool says 20,000 is enough sample (out of 2 million sheets, which he calls ballot cards) to check a winning margin of 2,802 votes, at 95% confidence. This is 0.3% of the million ballots; all these estimates are for ballots with 2 sheets, 4 pages. A small jurisdiction can sample more sheets per batch, without much extra time, to get a similarly effective sample. https://www.stat.berkeley.edu/~stark/Vote/auditTools.htm

For ballots scanned at precincts: When they come back to a central location, the scans already made can be checked by comparing to random sheets, as above. If precinct ballots fell randomly into the box and are hard to compare to the images, it may be faster to rescan at central office, so order of images matches stack of sheets. On election night, this checking needs 10 minutes per batch of 200 ballot sheets, so a team can check 18 batches (3,600 ballot sheets) in 180' = 3 hours.

At one team per 18 precincts, small counties will need only 1-3 teams on election night. A big county with 180 precincts needs 10 teams.

As we shift to mailed ballots, it becomes more important and more feasible to verify images on a flow basis, and stop trusting seals and locks.

[38] **Chain of custody:** Item 4b "*Compliance audits assess the trustworthiness of the paper trail.*", on page 12 of https://electionaudits.org/files/Audit Principles and Best Practices 2018.pdf

Lindeman+Stark, Gentle Introduction to Risk-limiting Audits. p.2 "*If the compliance audit does not generate convincing affirmative evidence that the ballots have not been altered and that no ballots have been added or lost, a risk-limiting audit may be mere theater*" https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf.

Since seals, locks, security cameras and guards can be breached without a trace (see pages 2-3), it is hard to identify what "*convincing affirmative evidence*" would look like. For more details, the Audit Principles and Best Practices 2018 cites: Stark, An Introduction to Risk-Limiting Audits and Evidence-Based Elections, for the Little Hoover Commission https://www.stat.berkeley.edu/~stark/Preprints/lhc18.pdf

- *Check that the number of ballots ... [is consistent at each step]*
- *Check signature verification...*

- *Review surveillance video...*
- *Check each seal against its photograph...*
- *Record any discrepancies.*

Better than any of these would be comparing ballots to digitally signed ballot images created and verified against ballots before the ballots went into storage.

Bernhard et al. Public Evidence from Secret Ballots. "*No state has (or had) adequate laws or regulations to ensure that the paper trail is conserved adequately, and that provide evidence to that effect.*" https://arxiv.org/pdf/1707.08619

The public knows the weaknesses of locks, and anyway mistrusts local officials. Most people would assume local officials can go in to work on the stored ballots any time they want to without keeping proper records. Covid social distancing gives an extra excuse to go into storage alone.

[39] **Covert entry:** There are no statistics on how often criminals enter rooms undetected, but law enforcement often does so, so ability to enter rooms undetected is widespread at least in law enforcement and former law enforcement: Electronic Frontier Foundation, "Peekaboo, I See You: Government Authority Intended for Terrorism is Used for Other Purposes". Also McGuire, Sneak and Peek Warrants-Necessary for our Safety...?

[40] Sample size calculations are in a separate section of the paper and in a spreadsheet http://votewell.net/vote.xlsx

[41] Errors in hand counts are in a separate section of the paper.

[42] **RLAs' limited sample sizes**: Georgia in 2020 did check the close Presidential race, after huge pressure from President Trump and the public, but did not check any of the close local elections in Georgia's 159 counties on the same day.

Colorado has picked contests for its RLAs with samples up to 358 per county in 2020 general election, 868 in the 2020 primary, 313 in 2019 local elections, 381 in the 2018 general, 351 in the 2018 primary.

[43] Poorvi Vora. "***fixed-time-fixed-manpower audit***" Exhibit B. Pages 20-23 in Maryland, 2016. "Joint Chairman's Report on the 2016 Post-Election Tabulation Audit" https://www.elections.maryland.gov/press_room/documents/PostElectionTabulationAuditLegislativeReport.pdf

[44] **Dr. Stark's "Tools** for Comparison Risk-Limiting Election Audits" calculate initial sample sizes for any total error rate and risk limit, at https://www.stat.berkeley.edu/~stark/Vote/auditTools.htm#

The graph in this paper assumes 40,000 voters. To calculate those initial sample sizes it uses Dr. Stark's default error rates of 1 in 1,000 for 1-vote errors, and 1 in 10,000 for 2-vote errors. He considers these defaults conservative. His tool shows the gap between winner and loser which corresponds to a given sample size and risk limit. In order to show a total error rate, this gap is similarly treated as having a tenth as many 2-vote errors as 1-vote errors, consistent with his assumptions. This means the number of errors is 91.67% of the gap between winner and loser.

RLA samples of 4,000, for risk limits of 5% or 30%, are not in his tool. For example with 5% risk limit and 40,000 voters, winning margin gaps of 92 or 94 votes jump in sample size, from 6,729 down to 3,581.

[45] **Checking scanner counts:** Scanner will say how many images it found. The fastest way to count the paper ballots for comparison is probably to weigh them on a sensitive scale. If batch includes different types of ballots, such as computer-generated or mailed, they need to be weighed separately, with separate lookup tables to give count of ballots for each weight. Weighing is endorsed in item 4e *"weighing ballot batches on a precision scale"*, on page 12 of https://electionaudits.org/files/Audit%20Principles%20and%20Best%20Practices%202018.pdf A page of 8.5 x 11 paper (20-pound bond or 50-pound offset) weighs 4.54 grams or a sixth of an ounce. The scale has to be accurate enough to make those distinctions in piles of 200 to 500 ballots (2-5 pounds), 1 part in 200-500. Weights are proportionately heavier for 24-pound paper and larger ballots. An electronic scale can be that accurate, and may be trusted more than hand-counting the piles. https://www.mt.com/us/en/home/library/know-how/industrial-scales/weighing_votes.html

[46] **Multifeed:** Scanner may pull in more than one ballot at a time, so count of images is less than count of ballots. It may also be possible for a glitch to put an image of one ballot in the file twice. Weight will identify these too. If both happen in a batch, cancel each other and weight matches, the error will be found by the random sample in the same way as other random errors.

[47] **Image availability:** There is a long-standing division between states which release ballot images to the public and states which do not, by law or court decisions. https://commons.wikimedia.org/wiki/File:Ballot-foia.png

In states which do not release ballot images to the public, giving these images to approved auditors lets independent audits proceed, while public discussion continues on release to the public. The auditors can be outsiders, like CPAs or professors, or officials from another part of the government. A powerful possibility is to have a committee of people who came in second in recent elections and are not running in the current election, since they will be motivated to look closely at the system.

A concern with releasing images of ballot sheets to the public is that rare styles will reveal rare types of voters. Options for election officials to minimize association of ballots with individuals include:

a) Ballots do not need to identify precinct, voting location or date or voting method (e.g. provisional or absentee).

b) English can be on the same ballot with each of the less common languages and enough English-speakers can use these ballots so users of the less common language cannot be identified. An extra benefit is that bilingual voters using the bilingual ballot can see and complain about mis-translations.

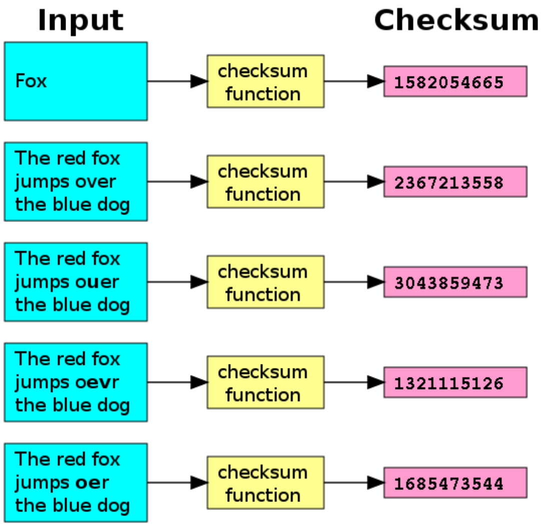
c) Special districts which have different boundaries can be printed on separate sheets which are scanned separately to reduce the need for rare ballot styles.

d) Ballot marking devices can mark ballots so they look the same as hand-marked ballots.

e) Ballots with a signature or unique write-in can be recognized as not necessarily from that voter, and handled according to local law. Some voters sign their ballots or write themselves in as a write-in candidate; which some election officials have taken as a reason to remove transparency from vote counting, at high cost, even though any voter can put any other voter’s name on a ballot (Pat can put Kim’s name on Pat’s ballot).

[48] **Checksum or hash:** It is common practice in computer files to take the ones and zeros which make up the file, calculate a special formula which gives a summary number (checksum, hash value, digital signature), and make a permanent record of this number (such as on paper). When other people get the file, they can run the same formula and see if they get the same summary number. Any change in the file, even moving a dot from one place to another, gives a substantially different summary number, so people can go back and insist on getting the correct file. This is much more secure than paper records where forgeries can fool experts.

Checksum is a general term. Hash value and digital signature are more specific and technical terms. The Unix "cksum" utility generates 10 digits. https://commons.wikimedia.org/wiki/File:Checksum.svg



For elections the summary number needs to be given to the public and/or auditors, so they can identify true copies of the original files.

Microsoft has an explanation of hashes: https://docs.microsoft.com/en-us/dotnet/standard/security/ensuring-data-integrity-with-hash-codes

On the same page where San Francisco issues their ballot image files, they offer a "SHA" file with a 512-bit (128-character) hash value for each image file, using the SHA-512 algorithm. Click "Final Report" on https://sfelections.sfgov.org/march-3-2020-election-results-detailed-reports . Copies of the hash values can also be [picked up]() on paper in person if desired. A better approach would be to create for the file of signatures, a hash which is short enough to read over the phone for checking. San Francisco uses software from QuickHash https://www.quickhash-gui.org/

SHA-512 provides the best assurance that the file is unchanged, if you compare every hash value, character-by character, by hand (since a computer comparison could be erroneous). This seems unrealistic, and there needs to be expert discussion of the reliability of checksums (such as the first or last 6 digits of SHA-512) which are short enough for manual checking.

Colorado has each county calculate hash values on the files electronically sent to the Secretary of State. These hash values are also sent electronically, so a man-in-the-middle attack could corrupt both.
https://www.sos.state.co.us/pubs/rule_making/CurrentRules/8CCR1505-1/Rule25.pdf

[49] **Random numbers to identify ballots for checking:** One way to get random numbers for each batch is a scratch-off card. If card says to pull the 120th ballot, a sensitive scale is the fastest way to count the first 119 ballots to pull out the 120th ballot, so public or auditors can compare it to the image, printed or displayed on a terminal nearby.

The reasons to check that ballots match images are (a) to fix bad scans immediately, and (b) to prevent doubt that an error or hack switched images as they were made, adding more votes to a candidate than the original ballots showed. This is an unlikely type of error, so **even if checking paper ballots against images can't be done** or done thoroughly, there can still be a very thorough review of the election by doing independent tallies of image files, with valid checksums.

Election companies minimize the risk of counterfeit scanners or software entering the system by including secure private keys in each scanner's hardware. The risk is never zero. Designers use the concept of "trusted systems" which is not an absolute concept, but a continuum depending on the level of evidence which convinces users to trust the software, hardware, storage and security in the system.

[50] **Unreliable security cameras:** ["How to hack a security camera. It's alarmingly simple"](). IFSEC.
["Official Cybersecurity Review Finds U.S. Military Buying High-Risk Chinese Tech (Updated)"](). Forbes.
["Hacking Security Cameras – Schneier on Security"]().

[51] Errors in hand tallies are discussed in a separate section of the paper

[52] **Check totals of cast vote records:** Lindeman+Stark, Gentle Introduction to Risk-limiting Audits. p.3, section B(i) "*ballots sum to the contest totals for every candidate.*" https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf.

Item 4b "*reconciliation to ensure that all votes from all audit units are correctly summed in the election totals*", on page 12 of https://electionaudits.org/files/Audit%20Principles%20and%20Best%20Practices%202018.pdf

Lindeman et al. Comments re statistics of auditing the 2018 Colorado elections. p.2. "*the Secretary of State has the ability to compare reported contest results with the CVRs it receives, but there is no publicly observable means to verify that this comparison has been done correctly.*" https://www.sos.state.co.us/pubs/elections/VotingSystems/riskAuditFiles/NotesOnStatistics-2018ColoradoPrimariesElectionAudit.pdf

[53] **Broken chain of custody:** For example in Michigan 2016, *"state records show 10.6 percent of the precincts in the 22 counties that began the retabulation process couldn't be recounted because of state law that bars recounts for unbalanced precincts or ones with broken seals."* https://www.detroitnews.com/story/news/politics/2016/12/12/records-many-votes-detroits-precincts/95363314/

H.R.1 proposes to forbid relying solely on machine count if chain of custody is broken. It offers no alternative, and ballot images may provide a helpful alternative. F, Sec 1502(a)(2)(B)(i) https://www.congress.gov/bill/117th-congress/house-bill/1/text?q=%7B%22search%22%3A%5B%22hr+1%22%5D%7D&r=1&s=1#

[54] **Prevalence of bugs:** Schneier, "Every piece of commercial software... has hundreds if not thousands of vulnerabilities, most of them undiscovered" https://www.google.com/books/edition/Data_and_Goliath_The_Hidden_Battles_to_C/MwF-BAAAQBAJ?hl=en&gbpv=1&dq=schneier&pg=PT135&printsec=frontcover

Examples of bugs and hacks: http://votewell.net/a/hacks.htm

[55] **Undetected problems:** Kolbe on SolarWinds hack by Russia, *"Chinese, others, they've all built huge capabilities, they're well-resourced, well-staffed, [and] focused on doing exactly this. This is not a one-off, this is not something unusual... I guarantee you that there are other operations similar in size and scope, if not larger, that haven't been discovered."* https://news.harvard.edu/gazette/story/2020/12/harvard-cybersecurity-experts-discuss-russian-breach/

[56] **Unfixed problems:** Schneier. *"many network administrators won't go through the long, painful, and potentially expensive rebuilding process. They'll just hope for the best.*" https://www.theguardian.com/commentisfree/2020/dec/23/cyber-attack-us-security-protocols

Amazon cybersecurity engineer says, "*Why would you care about cloud security? You don't have to bust your ass because you live in a small-town market where you know everybody and you're never going to be out of a job. A lot of companies that are headquartered in remote areas don't have particularly sophisticated IT teams."*

[57] **Embezzlement arrests**: https://www.ojjdp.gov/ojstatbb/crime/ucr.asp?table_in=1

[58] **Who embezzles:** https://www.hiscox.com/documents/2018-Hiscox-Embezzlement-Study.pdf

[59] Image of checksums https://commons.wikimedia.org/wiki/File:Checksum.svg

[60] Microsoft explanation of hashes https://docs.microsoft.com/en-us/dotnet/standard/security/ensuring-data-integrity-with-hash-codes

[61] For San Francisco's hash values, click "Final Report" on https://sfelections.sfgov.org/march-3-2020-election-results-detailed-reports

[62] San Francisco answers on their hash codes http://www.sfelections.org/results/20160607/data/SHA512_FAQ.pdf

[63] https://www.quickhash-gui.org/

[64] https://www.google.com/url?q=https://www.auditelectionsusa.org/wp-content/uploads/2018/12/Exhibit-6.Ballot-Image-Information-on-ESS-System-Issued-11-1-2018.pdf

[65] Colorado hash value procedures: https://www.sos.state.co.us/pubs/rule_making/CurrentRules/8CCR1505-1/Rule25.pdf

[66] Tally sheet for Single Transferrable Vote: http://www.votewell.net/tally.htm#_Toc73094604

[67] Blom et al. "You can do RLAs for IRV" https://arxiv.org/abs/2004.00235

[68] Adjusting for multiple alternate hypotheses is standard practice, since the more hypotheses they test, the more likely at least one test will accidentally give a wrong result. https://www.stat.berkeley.edu/~mgoldman/Section0402.pdf They address this in the next note.

[69] Email 6/24/2021 from Vanessa Teague, a co-author: "We did think about this carefully. RAIRE works by first generating a set of assertions which must be tested by RLA, then (as a completely separate step), testing all of them together. The RLA is parameterized by a chosen risk limit alpha, and we assume that all the tests have the same limit. The crucial composition is: there are multiple null hypotheses, but the audit reverts to a manual count if _any one of them_ can't be rejected. So any effect of multiple hypotheses actually makes the audit more conservative. Compared with a single RLA of the same margin and same risk limit (alpha), RAIRE may take longer to confirm an outcome, but is not any more likely to accept a wrong outcome."