Don’t just trust, always verify –

The status of post-election auditing in the presidential swing states

August 2025

Susan Greenhalgh
Senior Advisor for Election Security
Free Speech For People

David Jefferson, Ph.D.
Election Integrity Foundation

FREE SPEECH FOR PEOPLE .ORG

EXECUTIVE SUMMARY

Most U.S. elections are conducted using computerized voting systems that are susceptible both to unintended and often undetectable programming errors, malfunctions, and misconfigurations, and also to intentional manipulation and hacking. Because of these vulnerabilities, computer scientists maintain that it is essential first to capture voters' choices on trustworthy, indelible, voter-verified, hand-marked paper ballots and then, after the close of the election, to verify the preliminary computed election outcome using robust post-election audits based on those original paper ballots. Elections should not require trust in either humans or software, but should instead be based on immutable verifiable evidence that is both compelling and transparent to the public.[1]

Widespread myths, overstatements, and exaggerations about voting machine security and procedural safeguards have resulted in misplaced faith in computerized election systems. Election officials and other stakeholders, motivated to boost voter confidence have overestimated and overstated the security of the voting systems, while underestimating their vulnerabilities.

Auditing election results became even more essential recently because the software that runs most election equipment was compromised by partisan allies of Donald Trump in 2021 and 2022. Election software was purloined in several jurisdictions around the U.S. with the deliberate help of election insiders, introducing additional security risks. Unfortunately, there have been almost no efforts as yet to mitigate the new threats arising from that fact.

How effective were the audits conducted in the seven swing states in the November 2024 election? Did they provide strong evidence that verified the correctness of the election outcomes? We examined the post-election audits in Arizona, Georgia, Michigan, Nevada, North Carolina, Pennsylvania, and Wisconsin. Our assessment found the following:

- In Michigan the post-election audits are conducted months after the election, and elections are certified based entirely on computerized totals before examining any paper ballots. To date, Michigan has not published its state-wide post-election audit report. [2]
- Georgia requires all in-person voters to use computerized ballot marking devices (BMDs) statewide.[3] In Pennsylvania, 30% of in-person voters must vote on these devices.[4] These computerized devices do not provide the trustworthy record of voter intent necessary for an effective audit.
- Nevada primarily uses direct record electronic voting machines (DREs) with paper audit trails and BMDs to record votes.[5] These computerized devices also do not provide the trustworthy record of voter intent necessary for an effective audit.
- Georgia, Pennsylvania and Nevada all claim to conduct "risk-limiting audits" (RLAs), which are generally acknowledged as the gold standard of auditing. In fact, none meet the requirements for a true RLA.
- Pennsylvania is bound by court settlement[6] to conduct risk-limiting audits on all election contests. But in apparent non-compliance with the settlement, not only does it not adhere to the requirements of a risk-limiting audit, in 2024 Pennsylvania only conducted its "RLA" on one contest, the state treasurer's contest.
- Current Nevada statute directs the state to audit 2% of ballots for all contests, in addition to its "RLA" but there is no evidence the 2% audit was conducted.[7]
- Arizona audits include many effective provisions, and are more transparent than other states, providing evidence to support the election outcome, but they could be enhanced.
- North Carolina's audits adhere to several effective practices, but like Arizona, its audits could be improved to provide stronger evidence that its election outcomes are correct.
- Wisconsin audited far more ballots than any other state, but its audit results were published months after the election was certified. Moreover, officials published no source documentation or details of the audit counts, thus providing little transparency.

In short, most of the swing states contested in the 2024 presidential election did not provide strong, independent evidence that the computer generated outcomes were correct. The election outcomes are primarily dependent on computerized results. A few states have provided some evidence to support their computerized results, but improvement is necessary if the audits are to provide strong evidence of the election outcomes and act as a safeguard against miscounts or manipulation.

INTRODUCTION

"Trust but verify," is a phrase often applied to elections. In a democracy, elections determine who will wield tremendous power to control millions, billions, or trillions of other people's dollars, and potentially engage the nation in military actions or wars that cost countless lives. Because of the enormous stakes we must not just blindly trust that the human officials, the programmers, and the machines all worked perfectly and acted honestly. Election outcomes must be verified. It is a matter of U.S. national security that we get them right. Hence, we suggest revising the old chestnut to a more modern version in the context of elections: Don't just trust — always verify.

Verifying the outcomes of elections through post-election audits is broadly recognized in the security community as an essential element of trustworthy elections. There are various types of post-election audits that can include auditing voter registration rolls, examining compliance with election laws and regulations, assessing the conduct of procedures, and more. Generally, the term "post-election audits" is recognized to mean an audit that independently examines paper ballots and compares them to the results reported by computerized voting systems. For this report, we are specifically examining these types of post-election audits.[8]

As the reliance on computerized election systems has increased in the last few decades, computer scientists and experts emphasized that it is crucial that (a) votes be recorded indelibly by hand-marking on durable paper ballots,[9] (b) that those ballots be properly secured against deletion, modification, or additions,[10] and (c) they are used to independently audit the output of the computerized systems via direct human examination of the original ballots.[11]

Researchers, election administrators, and election stakeholders have examined many different audit practices and algorithms, provided recommendations and guidelines for their conduct, and published numerous papers on auditing theory and practice.[12]

In recent years, attention to security has increased dramatically and the focus on post-election audits has grown accordingly. At present, forty-five states claim to perform some form of post-election audit for at least some contests.[13]

Following the 2020 election and Donald Trump's claims the election had been stolen, there was a national chorus of assurances from election officials, legislators, advocacy groups, vendors, and other "experts" claiming that our elections are robustly audited. Later, both before and after the 2024 elections, those same parties reiterated those claims as they sought to build voter confidence by declaring that some kind of audit would be conducted, without any description of its kind or quality.

> "Our elections are secure. We all use paper ballots. We all have audits."
> Michigan Secretary of State Jocelyn Benson testimony before the U.S. Senate Rules Committee, March 12, 2024.[14]
>
> "After ballots are canvassed and tabulated, post-election audits are conducted to ensure every vote is accurately counted and no discrepancies are found."
> National Task Force on Election Crisis' tweet, November 25, 2024.[15]
>
> "...our elections are secure and transparent, and the outcomes are verified by the audited paper ballots that 97% of voters cast (including in all of the swing states)."
> David Becker, Center for Election Innovation and Research and a CBS news contributor on elections, post on LinkedIn.[16]

But in practice, we need to ask just how effectively those audits check whether the computerized outcomes are correct, and whether they provide strong evidence for their conclusions either way.

How sure are we that those audits would detect and correct an incorrect outcome due to misconfiguration, software bugs, human procedural errors, hacking, malicious code, or other malfeasance? Many studies have been published identifying theoretical principles and best practices for conducting post-election audits.[17] However, since 2018 according to our review, there has been no published evaluation of the states' actual audit practices or of their quality.[18]

In this paper we examine the post-election audits conducted in the presidential swing states of 2020 and 2024: Arizona, Georgia, Michigan, Nevada, North Carolina, Pennsylvania, and Wisconsin. Similar studies should really be done of other states as well. Although we chose the swing states for this study, we are in no way suggesting that the certified election outcomes in those states in the 2020 or 2024 elections were incorrect, and certainly not that any of those elections were "stolen." Instead, we are evaluating whether the audits, as actually conducted, really provided compelling statistical evidence that the election outcomes were correct. It should be clear that the results of the election can be perfectly correct even if the audits are faulty and our trust in them is unwarranted. Through this study we hope to understand the deficits in current post-election audits, and encourage the adoption of stronger, more meaningful audit practices in all states.

MYTHS AROUND ELECTION SECURITY

In order to appreciate why meaningful, effective post-election audits are essential, it is important to understand the vulnerabilities and risks inherent in computerized election systems that could lead to incorrect outcomes. Election officials, legislators, vendors, and some activists seeking to bolster voter confidence have often exaggerated or misled the public to believe voting systems are much more secure than they really are. In this section, we explain some of the more common myths about election systems.

Myth: Voting systems can be trusted because they are rigorously tested and certified.

Election systems in the U.S. are almost entirely computerized, yet computers are prone to unintentional programming errors (bugs), misconfigurations, errors in administration, and to malicious and potentially undetectable cyber-attacks.[19] To assess their functionality, reliability, and accessibility, they are typically subject to some form of state and/or federal testing and certification prior to adoption by a jurisdiction and deployment in elections.[20] In addition, voting machines usually undergo pre-election "logic and accuracy" (L&A) testing before each election aimed at checking that the machines are working properly and are configured correctly.[21]

These practices are important but do not guarantee the machines will operate correctly during an election. The truth is that testing and certification have limited value.[22] For example, testing the software prior to a jurisdiction adopting a system cannot assure that the software installed for a particular election is identical to that tested. Furthermore, no software testing program can test it in all the configurations used in all of the states and jurisdictions where the system might be deployed. More generally, it is a principle of computer science that, while testing may uncover some bugs or security vulnerabilities, no amount of testing, however extensive or elaborate, can prove that a system is free of bugs or security vulnerabilities,[23] and consequently almost no software system of any size is ever free of them. In addition, the federal EAC guidelines applied to the voting equipment in use today are known to be generally lax[24] and woefully outdated. All federally certified election equipment currently in use has been tested to guidelines adopted twenty years ago, in 2005.[25]

The agency responsible for setting federal guidelines and certifying voting machines – the U.S. Election Assistance Commission (EAC) – has been criticized for dysfunction,[26] inaction,[27] a sloppy approach to cybersecurity[28] (that resulted in the EAC itself being hacked),[29] delaying adoption of updated voting standards,[30] partisanship,[31] and alleged self-dealing.[32]

Moreover, the EAC guidelines, such as they are, are not even required, but are voluntary. States may choose to adopt them or ignore them. In fact, most states do not require EAC certification, although some have their own certification programs somewhat patterned on the EAC process.[33] Nevertheless, this flawed certification process is often cited as a critical safeguard that will ensure election system accuracy.

> "ES&S voting systems are certified under strict federal standards and guidelines, including rigorous security, accuracy and reliability testing."
> ES&S Voting System's "Let's get the facts straight" webpage.[34]

Under the circumstances, such claims are exaggerated at best.

Most states also require L&A testing once the ballot information files have been loaded onto the voting machines prior to each election. This L&A testing is a best practice to check ballot configuration, but it's not foolproof, nor is it any defense against malicious cyberattacks. Configuration errors regularly occur that are not caught by L&A testing. For example:

- In the 2024 congressional primary in Utah, the voting system failed to aggregate vote totals accurately, causing the county to delay certification until it could hand count ballots.[35]
- In 2023, voting machines in Northampton, Pennsylvania swapped all the votes between two Superior Court candidates.[36]
- In 2022, Monmouth County, NJ's voting system counted multiple precincts twice causing the losing candidate to be certified as the winner. Months later the error was discovered and a recount found that the original election results were wrong.[37]
- In DeKalb County, Georgia in 2022, a candidate appeared to get few votes because of a configuration error. A hand count of ballots subsequently showed that she actually won the contest.[38]
- In 2019, the machines in Northampton County, Pennsylvania erroneously counted zero votes for one candidate in several precincts. A recount of the paper ballots found the candidate actually won.[39]

These errors are in principle detectable by thorough L&A testing, but were not detected. In most of these examples, the errors were so significant that it was obvious to election officials that there was a problem, causing them to investigate and correct the error (with the exception of Monmouth County, New Jersey in which the losing candidate was named the winner). Of course, less pronounced errors may occur more frequently without being detected.

L&A testing is certainly not an effective defense against the possibility of deliberately malicious software in voting systems. Despite frequent assurances from election administrators and vendors that pre-election testing would uncover any vote changing malware, these assertions ignore the fact that malware can easily be rigged to be inactive during L&A testing, and only change or miscount votes during a real election.[40] Of course any competent hacker would attempt to do exactly that. This played out in a different technological world in the famous Volkswagen diesel emissions scandal. Volkswagen diesel cars were programmed with software that instructed the cars' computers to restrict harmful emissions while they were undergoing emissions testing, but to allow the cars to emit a much higher level of pollutants during regular driving.[41]

Myth: Voting machines are never connected to the internet.

Perhaps the most commonly repeated myth about election security is the false claim that voting machines cannot be manipulated because they are never connected to the internet. This is misleading or outright false on several fronts.[42] First, some states like Florida,[43] Michigan,[44] Minnesota,[45] and Wisconsin,[46] use wireless cellular modems in their polling place tabulators to transmit unofficial election results from each precinct to the county election management server that aggregates vote totals. The precinct tabulators are thus online at least briefly on election night, and the central server they transmit to must be online all evening on election night. Researchers have in practice found some of these servers connected to the internet for days, weeks, and even months.[47]

An election security researcher from the National Institute of Standards and Technology described the risk this way:

> Use of wireless modems "...make the voting system a node on the internet... [and] also could potentially provide an entryway for remote attackers, not just close-range remote attackers. Once you're on the internet ... nation-state attackers may have access to you. What's the impact of that? It could be a loss of confidentiality and integrity of that voting system and that information that's on the voting system... If you're able to inject malware into the voting system, now you can change the data, now you can change the information that's within the voting system, or change the behavior of the voting system itself..."[48]

And yet, the fallacy that voting machines are never connected to the internet is repeated by highly placed government officials,[49] election administrators,[50] voting system manufacturers,[51] and the press,[52] further misleading the public about the cyber security risk profile of election systems. The risk of using wireless modems is often dismissed or minimized with misleading or meaningless claims like "the machines are only connected after voting is over," "the machines are only connected for a short time," or "the modems are only used to transmit unofficial results." These claims, even if true, are not effective safeguards, and are simply deflections from the fact that the machines are indeed connected to the internet and can be vulnerable to internet based attacks[53] from anywhere in the world.

Even worse is the fact that over thirty states permit ballots from some classes of voters to be transmitted from the voters' private computers or mobile devices to their home jurisdictions by internet (i.e. email or fax), which means these ballots are exposed to remote attacks.[54] In these states, the state office or local jurisdiction must have a server connected to the internet all during Election Day, and sometimes for days or weeks in advance of election day, just to receive those electronically-transmitted ballots.

Without strict quarantine protocols in place, that server could expose other parts of the system to the internet.

Even strictly prohibiting internet connections does not guarantee these systems are immune to cyberattacks. Before each election, voting equipment must receive ballot definition information to provide the machines with the list of races and candidates and related information about order and layout of the ballots. The ballot definition files are typically produced by the state, county, or by a vendor on a computer. They are then loaded onto the individual machines via removable media, often a USB stick. Likewise, software updates for voting machines are often uploaded from removable media. Computer security experts have demonstrated that by compromising the system that provides either ballot definition files or software updates an election can be compromised on the scale of an entire jurisdiction or, in some cases, an entire state.[55]

Finally, claims that election systems are secure merely because they are not connected to the internet ignores the very real risk that an insider with physical access can compromise voting systems. This has long been recognized by security and intelligence agencies as a significant threat,[56] and in fact some of the most scandalous recent election integrity breaches in Georgia, Colorado, Michigan, and Pennsylvania have been caused by arguably criminal actions committed by election insiders.[57]

All these facts generally go unacknowledged in favor of misleading assertions that voting systems cannot be hacked because they lack connectivity. Although it is certainly correct that election equipment should never be connected to the internet, claims that they are secure because they are not connected are misleading at best.

Myth: Elections cannot be manipulated on a large scale because they are decentralized and because there are so many different, incompatible voting systems.

This talking point is aimed at asserting in particular that a national election for president cannot be compromised. However with a minimum of scrutiny it can be shown to be clearly false. For one thing, presidential elections are not nearly as decentralized as one might think. They are decided by the Electoral College vote, and those votes are almost all assigned through a state level "winner take all" model. All of a state's electoral votes could potentially be determined by manipulating votes in just one county. For example, more than half of the registered voters in the swing state of Arizona are concentrated in Maricopa County.[58] To impact the entire state, a potential attacker need only subvert the results in that one county.

Similar cases of a single jurisdiction having a very heavy or dominant effect on an entire state's electoral vote include Los Angeles County (Los Angeles, California), Clark County (Las Vegas, Nevada), Cook County (Chicago, Illinois), Fulton County (Atlanta, Georgia), Cuyahoga County (Cleveland, Ohio), King County (Seattle, Washington), Wayne County (Detroit, Michigan), Salt Lake County (Salt Lake City, Utah), Oahu County (Honolulu, Hawaii), Anchorage Municipality (Anchorage, Alaska), St. Louis County (St. Louis, Missouri), and Miami-Dade County (Miami, Florida).

The argument that the variety of different voting systems in use necessarily makes it more difficult to hack an election is also fallacious. It would have some weight if it were necessary to compromise multiple types of voting systems in a state in order to swing the electoral votes. But as we have just seen, in a close election it often suffices to compromise a single jurisdiction, and just that jurisdiction's system, to decide the outcome of any statewide contest. e.g. president, governor or U.S. senator.

Moreover, in states that are not dominated by a single jurisdiction, it may be necessary for an attacker to compromise more than one, but the variety of voting systems gives attackers multiple choices as to which voting systems to attack, allowing them to choose among those with the weakest security.

ELECTION SYSTEMS WERE AT HIGHER RISK IN 2024 BECAUSE THEY HAD BEEN BREACHED BY PARTISAN ACTORS

In addition to the established security risks identified above, the machines provided by the two largest voting system vendors, Election Systems & Software (ES&S) and Dominion Voting Systems, were known to be at a higher risk in 2024 because their systems had been compromised by partisan actors.[59]

Following the 2020 election there was a coordinated, multistate effort by allies of Donald Trump to obtain access to voting system software in several states.[60] Software from Dominion Voting Systems was copied and covertly shared with a network of partisan operatives.[61] ES&S voting machines were also improperly obtained by Trump supporters who possessed them for months, and purportedly intended to use them to illustrate ways to rig elections.[62] This illicit possession of critical voting software and systems is likely the largest known election cybersecurity breach in the U.S. and posed a serious threat to the security of the 2024 elections and more in the future.

Though there have been limited, localized investigations,[63] there is no evidence that any federal investigation of the purloined voting system software has been conducted.[64] The security threats inherent in the unauthorized distribution of voting data and software has never been officially addressed or mitigated, and the threats still exist.

Combined Dominion and ES&S equipment capture and count nearly 70% of all votes nationwide. Ninety-six percent of Arizona voters use Dominion and ES&S equipment. 100% of Georgia voters vote on Dominion machines. 98% of Nevada votes on Dominion voting machines, and the remainder uses ES&S. 69% of Michigan voters' ballots are counted on Dominion or ES&S equipment. 89% of Pennsylvania voters ballots are counted on Dominion or ES&S equipment. ES&S counts 92% of North Carolina ballots. And either ES&S or Dominion counts 97% of Wisconsin votes.[65]

Possessing copies of voting system software enables potential attackers to create their own working replicas of the voting systems, test them, probe them, instrument them, and develop malicious exploit code to attack them stealthily. Adversaries can decompile the binary software to produce a version of the source code, study it for vulnerabilities, and develop malware designed to be installed by unskilled accomplices with minimal physical access to the voting equipment.[66] Attacks could also be launched by compromising the vendors or their employees responsible for programming or configuring voting systems, enabling large scale distribution of malware.[67]

Despite the lack of response to these breaches, the serious risks posed by the misappropriation of the voting software have been identified by other relevant parties. Before it was known that partisan operatives had taken its software, Dominion Voting Systems objected vehemently to providing its software to the same partisan actors (who ultimately got copies through officially-aided heists), stating that to give its software to biased actors would cause "irreparable damage" to the "election security interests of the country."[68] Similarly, before it was known that Georgia's data and election software had been taken in Coffee County, the Georgia Secretary of State's chief information officer testified that copies of the software would give the possessor a "road map" to the ways the system could be accessed.[69] Separately, the Georgia Attorney General opposed providing copies of the software to lawyers for the Trump campaign in a late 2020 election challenge, arguing that images of the voting system software would provide "the keys to the software kingdom."[70]

CRITERIA FOR EFFECTIVE POST-ELECTION AUDITS

In this assessment of the auditing effectiveness in the swing states we considered criteria established by the Center for American Progress (CAP) for assessing post-election audit practices as described in its 2018 report "Election Security in all Fifty States."[71] We note that our review differs somewhat in focus from the CAP evaluation. CAP sought to grade the states on their election procedures to identify shortcomings and inform policy reforms. Our goal is simply to understand whether the audits conducted provide evidence to justify confidence that the election outcomes have been verified, particularly in light of the voting system software security breaches. Here are the audit properties we considered:

Are the audits performed before the election outcomes were officially certified?

In some states the audits are performed only after certification of election results, which means that any potential errors detected by the audit cannot be corrected, and the audit cannot correct an erroneous outcome. This renders the audit completely ineffective as a safeguard.

Are the audits mandatory?

Post-election audits are sometimes not mandatory, or mandatory only for some contests. If an audit is not performed, then there is no assurance beyond trust in the voting systems that the outcome is correct. And even a perfectly conducted audit of some contest says nothing about whether any other contest was decided correctly.

Are there paper ballots and are they primarily hand marked by voters, rather than machine marked paper ballots or all-electronic ballots?

It is imperative that paper ballots be used to provide an indelible, tangible record of voter intent in order to perform a meaningful post-election audit, and the only practical way to assure that virtually all ballots are in fact voter-verified is if they are hand-marked by voters. Ballots recorded electronically by DRE or BMD do not provide strong evidence of voter intent. Likewise, ballots cast over the internet (even if they are printed at the election office) are not trustworthy records of voter intent. Machine-marked ballots are not considered trustworthy because after voters make their vote choices on a touchscreen DRE or BMD there are hundreds of thousands of lines of invisible, proprietary software involved in processing those choices in order to produce the VVPAT or paper ballot of record for scanning, counting, and auditing. The trustworthiness is further diminished by the fact that most voters simply do not carefully verify that their VVPAT or machine-marked ballots correctly represent their choices. Worse, in some cases they simply cannot do so even if they try because their votes are encoded in a QR code that is not human readable.

Procedures and policies must also be in place to ensure that the paper ballots have been protected under rigorous chain of custody practices, that only validly cast ballots are counted, and that no validly cast ballots have been removed or altered.

Is the audit conducted by hand count?

Some states allow the audit to be conducted by recounting ballots using the same computerized system that counted the ballots the first time. If the system initially counted votes incorrectly, an audit may just reaffirm an incorrect outcome. For example, Pennsylvania allows an audit to be conducted by a different machine tabulator than the one used for the original count. However, if both tabulators are configured with the same election definition file and use the same software, both may contain the same configuration errors, bugs, or malicious logic. If there were errors, they would produce the identical erroneous outcomes and potential problems would go undetected and uncorrected.

Are the ballots or machines selected for the audit chosen at random?

It is fundamental that the ballots or machines subject to the audit be chosen at random from the set of all ballots after they have been cast.[72] This prevents attackers from being able to target machines or ballots that they know will not be audited. Concerns that audits may be gamed to avoid scrutiny or cover up errors are not unwarranted. In 2004 two election workers from Cuyahoga County, Ohio were initially convicted[73] of rigging the 2004 post-election audit. (The convictions were later overturned on a legal technicality). Although the law required three random precincts to be chosen for audit, the workers selected precincts for the official audit only after pre-counting them to assure that they had no discrepancies, thereby avoiding the possibility of a legally mandated escalation to hand recounting of all precincts under Ohio law at the time. The county election supervisor actually defended the workers, claiming they did nothing wrong.[74]

Are all categories of ballots—regular, early voting, absentee, provisional, and military and overseas—included in the audit?

Excluding some categories of ballots from the audit weakens its value, misses possible errors, and may enable attackers to target their manipulation to a segment of ballots that won't be audited. Despite wide acceptance of this best practice, there are instances where audits have been weakened by excluding some ballots. For example, in 2017 California passed legislation to exclude from the audit all ballots received by mail after Election Day, and all provisional ballots.[75]

Does the audit escalate to examine more ballots or proceed to a full hand count if errors are found?

When conducting an audit based on a percentage of ballots cast, the audit should expand to count more ballots, up to a full hand count, if sufficient discrepancies persist. Further, if the audit expands to a full hand count with an outcome that does not agree with the original computer generated outcome, the outcome of the hand count should determine the winners and an investigation initiated as to why the machine canvass was wrong.

In an RLA, the audit proceeds until sufficient evidence has been accrued, in accordance with the risk-limit that the outcome is correct, or until there is a full hand count.

Are the audits conducted publicly with the data and results made available immediately for public review and independent verification?

Audits that are conducted without transparency do not provide evidence to the public that the election was decided correctly. Some states conduct audits but do not publish the actual audit results, instead publishing only a summary of the results as interpreted by the election officials who ran the election and the audit, or in the worst cases, just a declaration that an audit was conducted. In addition, some states' rules require the audit to be conducted in a timely manner, but do not make the results available to the public or candidates until months after the election, rendering the audit valueless to provide a check on the results.

Is the audit binding on the certified results?

Whenever a properly conducted, full-hand count audit determines that the machine-generated outcome was actually incorrect the audit result should be legally binding, superseding the outcome of the machine counts.

Are contests in districts that span multiple jurisdictions audited to examine ballots and potential errors across the entire district, or are separate audits conducted within each jurisdiction?

Most states only conduct audits by county, failing to consider the audit results of contests across county lines, such as Congressional and legislative districts. There is usually no simple mathematical way to combine the results of two county-level audits to produce a valid audit for a district that encompasses only part of each county. Small but widespread discrepancies that occur in multiple, individual counties or municipalities may be overlooked or disregarded, even though the errors may signal a broader, systemic issue.

RISK-LIMITING AUDITS

RLAs are widely recognized as the most effective type of post-election audit, and are often touted as the auditing "gold-standard"[76] because they are designed to limit the risk of certifying an incorrect election outcome. Put another way, they can limit the risk of certifying an election outcome that does not reflect the will of the voters. Because swing states Georgia,[77] Nevada,[78] and Pennsylvania[79] claim to conduct a "risk-limiting audit" (RLA), we also want to review the properties that must be present in a proper RLA.

There are different ways to conduct an RLA that we do not detail here.[80] In general terms, randomly selected ballots are inspected by hand until either those ballots give strong evidence that the reported outcome is correct, or every ballot has been manually inspected so that the true winner is known. If the full hand count outcome disagrees with the computer generated result, the hand count result replaces the machine count result. In this way, an RLA is effective in limiting the risk that a wrong election result caused by machine errors will not be certified.

In order to do this, RLAs have specific prerequisites including but not limited to: trustworthy evidence of voter intent (which in practice requires paper ballots marked directly by the voter by hand as the primary voting method);[81] comprehensive ballot accounting; and procedural audits to ensure the reliability, completeness, security and legitimacy of the ballots. RLAs must also be conducted before certification and, should a full hand count be conducted, the hand count must be the official binding election results.[82]

In order to provide public evidence and trust promised in an RLA, all procedures and data must be published so the computations can be independently checked.[83] None of the so-called "risk-limiting audits" conducted in Georgia, Nevada and Pennsylvania come close to meeting these requirements and are not true RLAs.

EXAMINATIONS OF SWING STATE AUDITING PRACTICES

Arizona

Overall, Arizona's audits satisfy many of the important criteria we identified, but they have deficiencies which limit their ability to provide strong evidence to either confirm the election outcome or correct a potentially incorrect outcome.

Arizona law A.R.S. § 16-602[84] directs county election officers to conduct a hand count audit of up to five contests on the ballot, including two federal and two state contests. An audit is required for each countywide primary, special, general and presidential preference election, and is performed before certification. In presidential election cycles, the presidential race is always included in the audit.

For all ballots cast in person, 2% of precincts or two precincts, whichever is greater, are selected at random and hand counted. Of early and mail ballots, 1% or 5000 ballots, whichever is less, are randomly selected for hand counting. Provisional ballots are not included in the audit at all. In a state where a large fraction of the ballots is cast early or by mail, this means that the fraction of ballots that is included in any audit is generally far smaller than 2%. The Arizona audit can expand if counting discrepancies are found. If the hand counts of precincts or batches of early and mail-in ballots differ more than the designated margin[85] for discrepancies in two successive hand counts, the audit sample is doubled. If discrepancies between the hand count and machine count persist, the audit is expanded to a full hand count. But because the audits are conducted by county and not by contest, if the contest district extends beyond the jurisdiction that is conducting the expanded hand count audit, precincts outside of that jurisdiction will not necessarily be included in the expanded hand count.

If persistent discrepancies require a full hand count audit, the audit results can be binding on the official results only if the contest that is the subject of the expanded audit is fully within the jurisdiction(s) conducting a full hand count. In other words, for contests spanning multiple counties, including a presidential contest, unless every county experiences discrepancies sufficient to trigger full hand counts, a full hand count across all the relevant jurisdictions will not be conducted and the audit results cannot replace the computer-generated results.

Even though Arizona's post-election audits are mandated by law, in November 2024, two counties did not perform the post-election audits because "the County Chairs of the two political parties did not designate the required members for the Hand Count Election Board (A.R.S. § 16-602(B)(7)."[86] Thus, a political party can apparently prevent a county's post-election audit by simply refusing to participate.

Documents of the counties' hand count audits are published on the Secretary of State's website, offering greater transparency and accountability into the process than most states provide.[87]

In 2024, according to records posted on the Secretary of State's website,[88] a little over 42,000 ballots were audited of 3,428,011[89] ballots cast, or 1.2% statewide. Two counties did not participate. The largest county, Maricopa, audited 11,745 ballots out of 2,078,460 ballots cast, meaning the largest county audited slightly less than 0.6% of ballots.

Arizona's audit provided some evidence that the computer-determined outcomes in those contests are correct, but in future, these audits can be further enhanced to provide even stronger evidence of correct outcomes.

Georgia

Georgia law § 21-2-498[90] requires the Secretary of State to conduct a "risk-limiting audit," and Ga. Code § 21-2-498.1[91] directs the State Election Board to conduct a pilot ballot image audit. Both audits must be concluded before certification. In 2020 the "RLA" audited only the presidential contest.

Georgia's "RLA" is, however, fatally flawed because Georgia's election system does not provide reliable voter verified evidence of voter intent, which is necessary for a meaningful risk-limiting audit.[92]

Georgia requires all in-person voters to cast ballots on computerized BMDs that record votes in QR codes printed on a ballot summary card along with human readable text. Georgia's scanners read only the QR code on each ballot to count the votes, ignoring the human readable text accompanying it. Out of 5,250,047 ballots cast in Georgia in the November 2024 election, nearly 5 million were recorded by BMDs, creating an insufficiently trustworthy audit record.[93]

Although the audit process in Georgia does review the human readable text (ballot summary), research has established that voters do not adequately review their ballot summary printouts to verify that they are accurate.[94] Furthermore, additional research[95] has determined that these machines lack properties necessary to ensure the voted ballots printed by BMDs are reliable evidence of voter intent. As UC Berkeley Professor of Statistics Philip Stark, the inventor of risk-limiting audits, has clarified:

> "Risk-limiting audits can assure that the votes recorded on paper ballots are tabulated correctly, but no audit can assure that the votes on paper are the ones expressed by the voter on a touchscreen: Elections conducted on current BMDs cannot be confirmed by audits."[96]

Because Georgia does not have hand marked paper ballots for voters who vote in person at the polls, its "risk-limiting audit" cannot properly confirm that the declared election outcome is correct. The outcome may, of course, be correct, but the audit does not provide strong evidence that it is.

Georgia also does not perform compliance audits or basic ballot accounting before the "RLA" is conducted, which is necessary to ensure that the ballots were validly cast and securely preserved for the audit. Investigations into the 2020 "RLA" in Georgia found significant errors in ballot accounting and reconciliation.[97] In addition, the Secretary of State has excused some discrepancies between the hand count and the computer count that were discovered in the course of the audit by claiming they were within an undefined and unknown "expected margin of error."[98] To handwave vote count inconsistencies without a quantitative basis is not part of any credible risk-limiting audit.[99]

In 2024, Georgia also conducted a ballot image audit, in which votes recorded in PDF ballot image files are counted by humans and compared with vote counts of the same ballots done by machine.[100] Among other things, this is supposed to verify that the human readable record of the votes matches the QR code records that the machine scanners actually read and count. However, public reviews of the published ballot images have revealed procedural errors in this audit process. Although the Secretary of State[101] and vendor[102] claimed to audit every contest on every ballot, the audit omitted several contests and failed to uncover over 1600 miscounted votes in a small, local contest in Sumter County.[103] The Georgia Secretary of State has said he initiated an investigation into the improper vote counts in Sumter County that were not detected in the ballot image audit, but so far, no report has been published.[104]

Furthermore, Georgia audit procedures are not legally binding on election outcomes. Even if they expose problems, including possibly determining that the winners declared by the machine counts were just wrong, the audit outcome does not legally prevent the certification of the incorrect outcome.

Michigan

Although Michigan election officials have publicly touted their post-election audits as providing proof of soundness of the election outcomes,[105] the actual audit procedures do not support such claims. Michigan's post-election audits are conducted well after certification and only published months later. The statewide report of the audit of the 2024 election has still not been published as of this writing (July 2025).

According to the Michigan Department of State's report "Audits of the November 3, 2020 General Election" published April 21, 2021,[106] the audits that are conducted are primarily procedural audits that include a hand count of only one precinct in each selected jurisdiction for one race. The purpose of these audits is primarily to determine if election workers followed proper procedures.

In 2020, the Secretary of State also announced plans to perform a "risk-limiting audit" following the 2020 election. Conducted months after the election, the Michigan "risk-limiting audit" also did not have full participation of all jurisdictions, preventing some ballots from being included. The Department of State ultimately termed the "risk-limiting audit" an "exercise" because of the incompleteness of the data.[107]

There is no evidence published by the Michigan Department of State regarding its 2024 post-election audit.

Nevada

In 2024, Nevada Rev. Stat. § 293.394,[108] required the state to conduct a pilot "risk-limiting audit" in accordance with guidance set out by the Secretary of State. Nevada Administrative Code 293.255[109] also requires an audit of 2% of the voter-verified paper audit trail (VVPAT) produced by the touchscreen voting machines, but this has been effectively supplanted by the RLA. Though the statutory language remains in place, there is no evidence the 2% VVPAT audit was conducted.[110]

The post-election "RLA" does not meet basic requirements to be qualified as an actual risk-limiting audit. It is not required to be conducted prior to certification and is not binding on the results. The audit report published by the Secretary of State's office is merely a sparse summary that provides no actual evidence from the audit,[111] and is unlikely to reduce any public skepticism.

Further, because Nevada uses DRE voting machines with supposedly voter-verified paper audit trails (VVPATs) for in-person voting, this system does not provide a reliable and trustworthy source record of voter intent that is required for a meaningful post-election audit and thus cannot provide strong evidence of the correctness of the election outcome.[112]

North Carolina

North Carolina N.C.G.S. § 163-182.1(b)(1)[113] includes provisions for a hand-to-eye examination of paper ballots compared to machine totals. Two sample sets of ballots are randomly selected from each county that may include an entire precinct, early voting site, or absentee ballot batch.[114] State law does not specify that the audit be conducted before the certification of the results. The November 2024 North Carolina post-election audit results[115] were published the same day as the election was certified.[116]

The audit report provides descriptions of all the discrepancies found and links to spreadsheets detailing the samples selected and the hand and machine counts. Audits are conducted by county, not by contest, limiting the ability of the audit to find problems that cross county lines.

North Carolina's audits have some important favorable characteristics. The audit is conducted by hand, the audit batches are selected at random, and the audit is conducted publicly. In years with a presidential contest, the presidential race is audited. The audit results can be binding on the outcome if a full hand count is required. But in close contests only a small sample of ballots will be audited and the sample is only expanded if "significant" anomalies are recorded. In this context the term "significant" is undefined in law or regulation. According to the North Carolina State Board of Elections Post-Election Audit report for the November 5, 2024 General Election, discrepancies between hand count and machine counts are frequently categorized as "likely hand count error" and dismissed without further investigation.[117] This practice could thwart meaningful investigation into possible vote count errors by the machines.

In 2024, 5,723,987 ballots were cast in North Carolina.[118] According to the State Board of Election's Post-Election Audit Report for the General Election on November 5, 2024,[119] over 260,800 ballots were examined in the "hand to eye" count, but we note that approximately 9,000[120] of the ballots audited were cast on ballot marking devices and cannot be considered trustworthy audit records.

With over 580,000 ballots cast, Mecklenburg County (which includes the city of Charlotte) is the state's largest jurisdiction. Mecklenburg audited 1,202 ballots total, but because Mecklenburg County uses ballot marking devices for in-person voting, these are not reliable audit records.

North Carolina's audit offered evidence that the computerized results are correct, but these audits can be strengthened to provide stronger evidence of election outcomes.

Pennsylvania

In 2019, the Commonwealth of Pennsylvania entered into a court settlement that required the implementation of "risk-limiting audits" for all contests.[121] In apparent non-compliance with the agreement, Pennsylvania has instead only conducted a procedure termed a "risk-limiting audit" on one contest in each primary and general election. After the November 2024 election, Pennsylvania selected only the state treasurer race for its "RLA."

Separately, Pennsylvania Statute § 3031.17[122] requires all counties to conduct a "2% statistical recount," which is a recount of 2% of the votes cast, or two thousand votes whichever is the lesser. The recount is done at the county level and counties may choose to perform the recount by hand or by rescanning ballots through a different tabulator than used for the initial count.[123] The "2% statistical recount" was conducted before certification in 2024 but this is not required in statute.

Merely using a different machine to recount ballots usually cannot provide a meaningful check on the initial vote count because all ballot tabulators in a county are more than likely to have been configured by the same election management system (EMS). If there was a ballot configuration error in the EMS, either accidental or malicious, this could cause all machines programmed by that system to incorrectly tabulate votes.

We examined the county reports for the "2% statistical recount"[124] and found that only 31,307 of auditable, primarily hand-marked ballots were audited by hand.[125] This represents only 0.44% of 7,034,206 ballots cast in the presidential race.[126] This is because some counties conducted their audits by machine and were excluded, and because large counties like Philadelphia were only required to audit a maximum of two thousand ballots according to the statute. Despite the perception that Pennsylvania's elections are subject to a 2% post-election audit, the reality is that far fewer reliably voter-verified ballots are actually examined by hand, diminishing the evidence supporting the election outcome.

Similarly, the Pennsylvania "RLA" suffers from other deficiencies. In addition to its failure to audit the contested races at the top of the ticket, not all counties participated in the audit. Several jurisdictions, including the city of Philadelphia, which has more than a million registered voters, do not record votes primarily by hand marked paper ballots.[127] The audit was not publicized or open to citizen observers.

For a full critique of the Pennsylvania "risk limiting audit," we recommend this resource published by Protect Our Votes Philly and endorsed by other civic organizations including Indivisible Philadelphia, March on Harrisburg, and Represent US Pennsylvania: "How Pennsylvania's 'risk-limiting audits' fall short of the mark due to critical shortcomings in procedures and transparency."[128]

Wisconsin

Wisconsin Statute §7.08(6) directs the Wisconsin Election Commission to conduct a post-election audit to assess the performance of its election equipment with respect to the error rate limit established in the Help America Vote Act of 2002. It does not aim to establish the probability that its declared election outcomes were correct.

Wisconsin's post-election audit report was published March 7, 2025,[129] four months past the certification deadline. The detailed results of the audit were not made public. Only a summary that included no original audit records was published, providing little transparency and no source documentation for its conclusions.

The Wisconsin Election Commission selected 373 "reporting units" that are comprised of one or more election wards. Ballots were hand-counted and compared to the machine tallies within the ward. Equipment errors identified in the audit were attributed to improper marks on ballots or creases. Audits do not escalate if errors are found and they are not binding on outcomes anyway.

In total, 370,230[130] ballots were audited of 3,422,918 ballots cast,[131] constituting the largest audit sample examined in 2024, but the fact that the audit is conducted months after the election renders it ineffective as a safeguard against miscounts or manipulation, and unable to provide timely evidence regarding the election outcome. Though the audit was more comprehensive than most, the lack of source records and documentation diminishes the transparency, reliability, and credibility of the audit.

CONCLUSION

Votes cast in U.S. elections are primarily counted by computers, which are inadequately secured, regulated and tested. Moreover, as with all computers they are susceptible to unintentional programming errors, malfunctions, misconfigurations, errors in administration, and malicious cyberattacks.

Despite the commonly repeated assurances that voting equipment cannot be manipulated, it can be. Although there are no verified cases of technical voting systems hacks in the U.S. that succeeded in changing the vote counts, the myths that voting systems are unhackable do not stand up to serious scrutiny.

All election results counted by computers should be verified with meaningful, timely, robust, public, and binding post-election audits based on a reliable, voter-verified record of the voters' selections.

In 2024, the need to confirm the computer-generated election outcomes was amplified because the nation's election infrastructure had suffered the most serious known election security breaches when the voting equipment that records and counts votes for both ES&S and Dominion voting systems was misappropriated by partisan operatives in the prior years.

Despite the severity of the security breaches there has been no comprehensive investigation into the unauthorized copying and distribution of voting data and software, and they have never been addressed or mitigated as a security threat to future elections.

A review of the post-election audits conducted in the seven key swing states reveals that, despite claims that the election was robustly audited, they were not. Though some states' audits conform to some, but not all, best practices necessary to provide convincing evidence the election outcomes were correct, others fall far short. And some states appear to disregard auditing obligations required by law or court settlement.

Though a few states conduct the post-election audit before certification, Wisconsin's post-election audit was published four months after the election. Michigan has yet to publish a state-wide report on its post-election audit.

With the exception of Arizona, most states do not provide documentation of the audit counts in the audit reports. This means the audits lack transparency and traceability, and could enable concealment of election irregularities.

Three states purport to conduct "risk-limiting audits" but these practices are inconsistent with the requirements for true RLAs.

Overall, the audits conducted were inadequate to provide strong evidence to confirm the computer-generated results provided by the election equipment used, much of which is running software that has been misappropriated and distributed to partisan actors. Although we do not dispute the outcome of the 2024 presidential election, we find that the audits in the swing states did not provide the necessary strong evidence of its correctness that the public deserves.

About the Authors

Susan Greenhalgh is the Senior Advisor on Election Security for Free Speech For People. Ms. Greenhalgh has previously served as vice president of programs at Verified Voting and at the National Election Defense Coalition, advocating for secure election protocols, paper ballot voting systems and post-election audits. Recognized as an expert on election security, she has been invited to testify before the U.S. Commission on Civil Rights and has been an invited speaker at meetings of the MITRE Corporation, the National Conference of State Legislatures, the Mid-West Election Officials Conference, the International Association of Government Officials, the Election Verification Network and the E-Vote-ID conference in Bregenz, Austria. She is a frequent source for reporters from The New York Times, The Washington Post, The Wall Street Journal, Politico, USAToday, Associated Press, National Public Radio and other leading news outlets. She has appeared on CNN and MSNBC's The Rachel Maddow Show, and various other television news shows. She has a B.A. in Chemistry from the University of Vermont.

Dr. David Jefferson is a computer scientist, an internationally recognized researcher in election cybersecurity for 25 years, and advisor to five Secretaries of State of California on voting technology issues. In that time, he has written, spoken, testified, and been interviewed widely on the subject of elections and voting security. In 1999, he chaired the technical committee of California Secretary of State's Task Force on Internet Voting, whose report was the first major study to expose the security dangers of online elections. In 2003, he was a member of the Secretary of State's Task Force on Touchscreen Voting, whose recommendations led to voter verifiable audit trails for electronic voting machines. He served on the Secretary of State's Technical Advisory Board and later on the Voting Systems Technology Assessment and Advisory Board, and, in those capacities, he led and co-authored several technical studies on reliability and security issues with the voting systems used in California. He also served as Chair of the Secretary of State's Post-Election Audit Standards Working Group, the panel that invented the notion of risk limiting audits (RLAs), which has come to be regarded as the gold standard for election security. In 2004, he was co-author of the SERVE Security Report, which detailed severe security vulnerabilities in the Defense Department's proposed Internet voting system and led to the cancellation of the program. Before joining the Board of the Election Integrity Foundation, Dr. Jefferson was a past chair of the Boards of the California Voter Foundation and of Verified Voting. He has a B.S. in Mathematics from Yale University and a Ph.D. in Computer Science from Carnegie Mellon University.

About Free Speech for People

Free Speech For People (FSFP) is a non-profit, non-partisan public interest legal organization that works to renew our democracy and our United States Constitution for the people. As part of our mission, we are committed to promoting, through legal actions, secure, transparent, trustworthy and accessible voting systems for all voters. FSFP has consistently advocated for more secure, audited, and transparent voting systems, rooting our policies and objectives in scientific research and facts.

Acknowledgments

The authors would like to thank Philip B. Stark, Paul Burke, Neal McBurnett, Pam Smith and members of the State Audit Working Group for their valuable feedback on this report.

ENDNOTES

1. Stark, P.B., Wagner, D, "Evidence Based Elections," IEEE SECURITY AND PRIVACY, SPECIAL ISSUE ON ELECTRONIC VOTING, 2012.
https://www.stat.berkeley.edu/~stark/Preprints/evidenceVote12.pdf
2. Some counties have published their individual audit reports but they may not provide any information about the ballots audited or the results. See, for example, Plainfield Michigan's audit results, https://plainfieldmi.org/news_detail_T10_R1038.php.
3.https://verifiedvoting.org/verifier/#mode/navigate/map/voteEquip/mapType/ppEquip/year/2024/state/13
4.https://verifiedvoting.org/verifier/#mode/navigate/map/voteEquip/mapType/ppEquip/year/2024/state/42
5.https://verifiedvoting.org/verifier/#mode/navigate/map/voteEquip/mapType/ppEquip/year/2024/state/32
6. Stein v. Boockvar, Civ. No. 16-6287 (E.D. Pa. Apr. 29, 2019)
7. We contacted the Nevada Secretary of State's office requesting the results of the 2% audit and were referred to published information regarding the so-called "RLA."

8. For more information see: National Conference of State Legislatures' Post-Election Audits and MIT Election Data and Science Lab Project's Post-Election Audits | MIT Election Lab.
9. Appel, Andrew, and Philip B. Stark. "Evidence-based elections: Create a meaningful paper trail, then audit." 4 GEO. L. TECH. REV. 523—541.
10. Id.
11. National Academies of Sciences, Engineering, and Medicine. 2018. "Securing the Vote: Protecting American Democracy," Washington, DC: The National Academies Press. https://doi.org/10.17226/25120.
12. See eg. Bretschneider, J., Flaherty, S. and Stark, P. (2012) "Risk-Limiting Post-Election Audits: Why and How Contributing editors." Available at: https://www.stat.berkeley.edu/~stark/Preprints/RLAwhitepaper12.pdf.; Garland, L. et al, "Principles and Best Practices for Post-Election Tabulation Audits," (2018). Available at: https://www.amstat.org/docs/default-source/amstat-documents/audit-principles-and-best-practices-2018.pdf (Accessed: 5 February 2025). Norden, L. et al. "Post-election audits: Restoring trust in elections," (2007). Available at: https://www.brennancenter.org/sites/default/files/2019-08/Report_Post-Election-Audits-Restoring-Trust-in-Elections.pdf (Accessed: 5 February 2025); Andrew W. Appel, "Effective Audit Policy for Voter-Verified Paper Ballots in New Jersey," (Mar. 9, 2007). Available at: http://www.cs.princeton.edu/~appel/spapers/appel-nj-audits.pdf; Orey, R. et al, "Bipartisan Principles for Election Audits," (2021), available at: https://bipartisanpolicy.org/report/bipartisan-principles-for-election-audits/; "Election Audits Across the United States | U.S. Election Assistance Commission (2022)," www.eac.gov. Available at: https://www.eac.gov/election-officials/election-audits-across-united-states;
13. See: https://verifiedvoting.org/verifier/#mode/navigate/map/auditLaw/mapType/audit/year/2024
14. U.S. Senate Rules Committee Hearing; Administration of Upcoming Elections, 12 Mar 2024, https://www.congress.gov/event/118th-congress/senate-event/LC72674/text
15. https://x.com/ElectionTask/status/1861128053553873032
16. Available at: https://www.linkedin.com/posts/davidjbecker_united-states-voter-turnout-activity-7262836788090617857-Wkbh/?utm_source=share&utm_medium=member_ios
17. See: supra note 12.
18. In 2018, the Center for American Progress published "Election Security in All Fifty States," which graded states on their election security practices including post-election audits. We incorporate some of its criteria in our review of post-election audit practices.

19. Norden, L., Brennan Center. “THE MACHINERY of DEMOCRACY: VOTING SYSTEM SECURITY, ACCESSIBILITY, USABILITY, and COST,” the BRENNAN CENTER for JUSTICE VOTING TECHNOLOGY ASSESSMENT PROJECT LAWRENCE NORDEN, PROJECT DIRECTOR VOTING RIGHTS & ELECTIONS SERIES, (2006).
20. See: National Conference of State Legislatures, “Voting System Standards, Testing and Certification,” https://www.ncsl.org/elections-and-campaigns/voting-system-standards-testing-and-certification
21. See: U.S. Election Assistance Commission Quick Start Guide, “Logic & Accuracy Testing,” https://www.eac.gov/sites/default/files/electionofficials/QuickStartGuides/Logic_and_Accuracy_Testing_EAC_Quick_Start_Guide_508.pdf
22. Congressional Research Services, “Election Systems: Recent Action by the U.S. Election Assistance Commission,” (April 2024). Available at: https://crsreports.congress.gov/product/pdf/IN/IN12343
23. See also Stark, P.B., and R. Xie, 2022. “They may look and look, yet not see: BMDs cannot be tested adequately,” Proceedings of E-Vote-ID 3 2022, Lecture Notes in Computer Science, Springer-Nature, Cham https://link.springer.com/chapter/10.1007/978-3-031-15911-4_8
24. “A Framework for Election Vendor Oversight.” Brennan Center for Justice, 2019, www.brennancenter.org/our-work/policy-solutions/framework-election-vendor-oversight
25. U.S. Election Assistance Commission, which is responsible for setting voluntary voting system guidelines, updated the guidelines in 2021. At this time only one system has been certified to meet these standards and it is not yet in use. See: https://www.eac.gov/voting-equipment/system-certification-process
26. See: Starks, Tim. “EAC losing key expert reflects crisis at Commission,” Politico, 9 May 2019. Available at: https://www.politico.com/newsletters/morning-cybersecurity/2019/05/09/eac-losing-key-expert-reflects-crisis-at-commission-615709 and Geller, Eric. “Key Federal Election Agency Parting Ways with Embattled Top Staffer - POLITICO.” POLITICO, Politico, 18 Sept. 2019, www.politico.com/story/2019/09/18/election-assistance-commission-brian-newby-1501884. Accessed 6 Feb. 2025.
27. See: supra note 24.

28. Huseman, Jessica. “How the Election Assistance Commission Came Not to Care so Much about Election Security.” ProPublica, 5 Nov. 2018, www.propublica.org/article/election-assistance-commission-came-not-to-care-so-much-about-election-security.
29. Halpern, Sue. “America Continues to Ignore the Risks of Election Hacking.” The New Yorker, 18 Apr. 2018, www.newyorker.com/news/news-desk/america-continues-to-ignore-the-risks-of-election-hacking.
30. Halpern, Sue. “Mitch McConnell Is Making the 2020 Election Open Season for Hackers.” The New Yorker, 12 June 2019, www.newyorker.com/tech/annals-of-technology/mitch-mcconnell-is-making-the-2020-election-open-season-for-hackers.
31. Huseman, Jessica. “How Voter-Fraud Hysteria and Partisan Bickering Ate American Election Oversight.” ProPublica, 22 July 2020, www.propublica.org/article/how-voter-fraud-hysteria-and-partisan-bickering-ate-american-election-oversight.
32. Office of the Inspector General, Investigation Summary Case number OI-VA-24-0103-I, April 5, 2024. Available at: https://oig.eac.gov/reports/investigation/summary-investigation-alleged-false-statements-eac-dc
33. See: U.S. Election Assistance Commission, “State Requirements and the U.S. Election Assistance Commission Voting System Testing and Certification Program,” 3, Aug. 2023. Available at: https://www.eac.gov/sites/default/files/2023-08/State%20Requirements%20for%20Certification%202023.pdf
34. Available at: https://www.essvote.com/faqs/
35. Tomco, Brigham, “Counties Delay Maloy-Jenkins Recount Certification because of Voter Equipment Error.” Deseret News, 2 Aug. 2024, www.deseret.com/utah/2024/08/02/utah-2nd-district-recount-software-error/.
36. MacAulay, Jessica. “Pennsylvania County Reports Voting Machine Issues That Swapped Votes for Superior Court Candidates.” CBSnews.com, CBS Philadelphia, 7 Nov. 2023, www.cbsnews.com/philadelphia/news/election-2023-northampton-county-pennsylvania-superior-court/
37. Sullivan, S.P. “Election Officials Double-Counted Votes, Declared Wrong Winner in N.J. County, AG Probe Finds.” Nj, 6 Sept. 2023, www.nj.com/monmouth/2023/09/lack-of-safeguards-led-to-double-counted-votes-in-nj-county-ag-probe-finds.html.

38. Vigdor, Neil. “Georgia Candidate Who Appeared to Get Few Votes Was Actually in 1st Place.” The New York Times, 6 June 2022, www.nytimes.com/2022/06/06/us/politics/michelle-long-spears-georgia.html.
39. Corasaniti, Nick. “A Pennsylvania County’s Election Day Nightmare Underscores Voting Machine Concerns.” The New York Times, 30 Nov. 2019, www.nytimes.com/2019/11/30/us/politics/pennsylvania-voting-machines.html.
40. Walker, Josiah, et al. “Logic and Accuracy Testing: A Fifty-State Review.” Researchgate.net, 28 July 2022, www.researchgate.net/publication/362386239_Logic_and_Accuracy_Testing_A_Fifty-State_Review.
41. Hotten, Russell, “Volkswagen: The Scandal Explained.” BBC News, 10 Dec. 2015, www.bbc.com/news/business-34324772.
42. Zetter, Kim. “The Myth of the Hacker-Proof Voting Machine.” The New York Times, 21 Feb. 2018, www.nytimes.com/2018/02/21/magazine/the-myth-of-the-hacker-proof-voting-machine.html.
43. Geller, Eric . “The Voting Machine Hacking Threat You Probably Haven’t Heard About.” POLITICO, 14 Oct. 2022, www.politico.com/news/2022/10/14/wireless-modems-could-endanger-midterms-00061769.
44. Mehrotra, Kartikay, “America Won’t Give Up Its Hackable, Wireless Voting Machines,” Bloomberg, 3 Jan. 2020. https://www.bloomberg.com/news/articles/2020-01-03/america-won-t-give-up-its-hackable-wireless-voting-machines?embedded-checkout=true
45. See: supra note 43.
46. Wise, David. “WisPolitics-Review finds Wisconsin voting equipment at times connected to the internet, potentially vulnerable.” WisPolitics, 14 Sept. 2019, www.wispolitics.com/2019/review-finds-wisconsin-voting-equipment-at-times-connected-to-internet-potentially-vulnerable/. Accessed 6 Feb. 2025.
47. Monahan, Kevin, et al. “Experts Find More than 30 U.S. Voting Systems Connected to Internet.” NBC News, 10 Jan. 2020, www.nbcnews.com/politics/elections/online-vulnerable-experts-find-nearly-three-dozen-u-s-voting-n1112436.
48. December 18th 2019 presentation to the EAC’s Technical Guidelines Development Committee, Available at: https://www.eac.gov/events/2019/12/18/eac-technical-guidelines-development-committee-conference-call-meeting-121819 at 28:30.

49. Cassidy, Christina A., and Ali Swenson. “Election 2024: Cybersecurity Head Says There’s No Chance a Foreign Adversary Can Change Results.” AP News, 2 Oct. 2024, apnews.com/article/election-2024-security-misinformation-russia-iran-b93d6bbbf08c5046b4cee70ba7676a52.
50. See: Testimony of Thomas Hicks, U.S. Election Assistance Commission commissioner, before the U.S. House of Representatives Committee on Oversight and Government Reform, Subcommittee on Information Technology. 28 Sept. 2016, available at: https://www.congress.gov/114/chrg/CHRG-114hhrg26124/CHRG-114hhrg26124.pdf
51. See: supra note 42.
52. See e.g.: Tereszcuk, Alexis. “Fact Check: Wi-Fi at Polling Place Does NOT Mean Voting Machines Are Connected to Internet.” Leadstories.com, Lead Stories LLC, 8 Nov. 2022, leadstories.com/hoax-alert/2022/11/fact-check-wi-fi-at-polling-place-does-not-mean-voting-machines-are-connected-to-internet.html.
53. See: supra note 48.
54. Greenhalgh, Susan, et al. “Email and Internet Voting: The Overlooked Threat to Election Security.” Common Cause, 13 June 2024, www.commoncause.org/resources/email-and-internet-voting-the-overlooked-threat-to-election-security/.
55. U.S. Senate Selection Committee on Intelligence, Russian Interference in the U.S. Elections, Expert Testimony by J. Alex Halderman, Professor of Computer Science, University of Michigan, 21 Jun. 2017. Available at: https://www.intelligence.senate.gov/sites/default/files/documents/os-ahalderman-062117.pdf
56. U.S. Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, Election Assistance Commission, Federal Bureau of Investigation, “2024 U.S. Federal Elections: The Insider Threat,” Available at: https://www.ic3.gov/CSA/2024/240628.pdf
57. Brown, Emma et al, “Inside the Secretive Effort by Trump Allies to Access Voting Machines.” The Washington Post, 28 Oct. 2022, www.washingtonpost.com/investigations/2022/10/28/coffee-county-georgia-voting-trump/.
58.https://apps.azsos.gov/election/VoterReg/2025/State_Voter_Registration_January_2025.pdf
59. Ulmer, Alexandra, and Nathan Layne. “Trump Allies Breach U.S. Voting Systems in Search of “Evidence.”” Reuters, 28 Apr. 2022, www.reuters.com/investigates/special-report/usa-election-breaches/.
60. See: supra note 57.

61. Swaine, Jon, et al. “Files Copied from Voting Systems Were Shared with Trump Supporters, Election Deniers.” Washington Post, 22 Aug. 2022, www.washingtonpost.com/investigations/2022/08/22/election-system-copied-files-trump/.
62. Mauger, Craig, “DePerno once said he had a ‘lab’ where he could show how to ‘stuff’ ballots,” The Detroit News, 22 Sep. 2022. https://www.detroitnews.com/story/news/politics/2022/09/03/deperno-said-he-had-lab-where-he-could-show-how-stuff-ballots/7973743001/
63. Cappelletti, Joey, “Trump allies who ‘orchestrated’ plan to tamper with voting machines face charges in Michigan,” Associated Press, 3 Aug. 2023. Available at: https://apnews.com/article/stefanie-lambert-trump-michigan-election-fraud-bf9608af4b0972d41b5f4d303f5f6a29
64. Wire, Sarah, “Are the feds ignoring Trump allies’ multistate effort to access voting systems? Experts raise alarms for 2024,” Los Angeles Times, 9 Mar. 2023. Available at: https://www.yahoo.com/entertainment/anyone-investigating-trump-allies-multi-100017273.html
65. See: https://verifiedvoting.org/verifier/#mode/navigate/map/makeEquip/mapType/normal/year/2024
66. For instance, this technique was used by researchers from the Massachusetts Institute of Technology and the University of Michigan when evaluating the security of an online voting system. See: Michael A. Specter, J. Alex Halderman, “Security Analysis of the Democracy Live Online Voting System,” MIT, University of Michigan, 7 Jun 2020. Available at: https://internetpolicy.mit.edu/wp-content/uploads/2020/06/OmniBallot.pdf
67. See: supra note 55.
68. Cooper, Jonathan J., “Arizona senate issues new subpoena for 2020 election audit,” Associated Press, 27 Jul 2021. Available at: https://apnews.com/article/joe-biden-government-and-politics-arizona-senate-elections-election-2020-e7e26601f50611195fd47a3ffb92c311
69. See: Curling v. Raffensperger, No. 17-cv-02989-AT (N.D. Ga. filed Aug. 8, 2017). Beaver Dep Document 1368-3 Page 157-158.
70. No.1:20-cv-04809-TCB (N.D. Ga filed Nov. 30, 2020), Document 23, page 13. Available at: https://www.dropbox.com/scl/fi/xlvuqfqroogx7vg1sa4p9/Pearson-transcipt-gov.uscourts.gand.284055.23.0-Clean.pdf?rlkey=aghdw5w34rwqxugdxhnk8ij5b&e=1&dl=0

71. Root, Danielle, et al., “Election Security in All 50 States,” Center for American Progress, Feb. 2018, https://cdn.americanprogress.org/content/uploads/2018/02/11130702/020118_ElectionSecurity-report1.pdf
72. See: supra note 12.
73. “Two Election Workers Convicted of Rigging ’04 Election Recount,” Associated Press, 24 Jan. 2007. https://www.cleveland19.com/story/5984274/two-elections-workers-convicted-of-rigging-04-presidential-recount/
74. “Michael Vu Resigns.” Cleveland 19 News, 6 Feb. 2007, www.cleveland19.com/story/6045103/michael-vu-resigns/
75. https://legiscan.com/CA/text/AB840/id/1647832/California-2017-AB840-Amended.html
76. Norden, Lawrence. “Post-Election Audits” Brennan Center for Justice, 27 Sept. 2018, www.brennancenter.org/issues/defend-our-elections/election-security/post-election-audits.
77. “Georgia’s 2024 Statewide Risk Limiting Audit Confirms Voting System Accuracy | Georgia Secretary of State.” Ga.gov, 2024, sos.ga.gov/news/georgias-2024-statewide-risk-limiting-audit-confirms-voting-system-accuracy.
78. https://www.nvsos.gov/sos/elections/election-information/2024-election-information?os=wtmb%26ref%3Dapp&ref=app
79. “2024 General Risk-Limiting Audit Report.” Pa.gov, 2024, www.pa.gov/agencies/vote/elections/post-election-audits/2024-general-rla-report.html.
80. For more details see: Bretschneider, J., Flaherty, S. and Stark, P. (2012) Risk-Limiting Post-Election Audits: Why and How Contributing editors (affiliations for identification only). Available at: https://www.stat.berkeley.edu/~stark/Preprints/RLAwhitepaper12.pdf
81. Appel, Andrew W., Stark, Philip B., DeMillo, R.A., “Ballot-marking devices cannot assure the will of the voters” 7 Apr. 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3375755
82. Stark, Philip, B. “An Introduction to Risk-Limiting Audits and Evidence-Based Elections,” Prepared for the Little Hoover Commission. Department of Statistics, University of California, Berkeley, 2014.
83. See: supra note 12.
84. https://www.azleg.gov/ars/16/00602.htm

85. The designated margin is determined before each election cycle by the Voter County Verification Committee. For the November 2024 elections, the designated margin was three votes or 1%, whichever is greater for both polling place and early/mail ballot audits. https://azsos.gov/elections/about-elections/elections-procedures/post-election-procedures
86. https://azsos.gov/elections/election-information/2024-election-info
87. https://azsos.gov/elections/election-information/2024-election-info
88. Id.
89. https://apps.azsos.gov/election/2024/ge/canvass/20241105_GeneralCanvass_Signed.pdf
90. https://law.justia.com/codes/georgia/2019/title-21/chapter-2/article-12/section-21-2-498/
91. https://law.justia.com/codes/georgia/title-21/chapter-2/article-12/section-21-2-498-1/
92. See: supra notes 9 and 81.
93. See: supra note 81.
94. Bernhard, M., McDonald, A., Meng, H., Hwa, J., Bajaj, N., Chang, K., Halderman, J. A., University of Michigan, & The Harker School. (2021). "Can voters detect malicious manipulation of ballot marking devices?" In University of Michigan [Journal-article]. https://jhalderm.com/pub/papers/bmd-verifiability-sp20.pdf
95. See: supra note 81.
96. Id.
97. Niesse, Mark. "Georgia investigation finds errors in Fulton audit of 2020 election," 17 July 2023, www.ajc.com/politics/georgia-investigation-finds-errors-in-fulton-audit-of-2020-election/BZ7D5JXOMRBPZIU4PNVYIHQZR4/. Accessed 18 Mar. 2025.
98. "Georgia's 2024 Statewide Risk Limiting Audit Confirms Voting System Accuracy | Georgia Secretary of State." Ga.gov, 2024, sos.ga.gov/news/georgias-2024-statewide-risk-limiting-audit-confirms-voting-system-accuracy.
99. Stark, Philip, B. "An Introduction to Risk-Limiting Audits and Evidence-Based Elections," Prepared for the Little Hoover Commission. Department of Statistics, University of California, Berkeley, 2014.
100. GA Code § 21-2-498.1 (2024)
101. "Raffensperger Announces Results of Ballot Image Audit, Confirms 100% Accuracy of QR Code," Georgia Secretary of State, 25 Nov 2024. https://sos.ga.gov/news/raffensperger-announces-results-ballot-image-audit-confirms-100-accuracy-qr-code

102. https://sos.ga.gov/sites/default/files/2024-11/georgia_ballot_image_audit_report_-_november_general_0.pdf
103. Neisse, Mark, Atlanta Journal-Constitution, “Votes for Mr. Potato Head and fictional characters given to a real candidate in South Georgia race.” 22 January 2025. The Columbian. https://www.columbian.com/news/2025/jan/22/votes-for-mr-potato-head-and-fictional-characters-given-to-a-real-candidate-in-south-georgia-race/
104. Id.
105. See: supra note 14.
106. Michigan Department of State, “Audits of the November 3, 2020 General Election,” (April 21, 2021), https://www.michigan.gov/-/media/Project/Websites/sos/30lawens/BOE_2020_Post_Election_Audit_Report_04_21_21.pdf?rev=84ad08815bdd4d1990188efc596b4763
107. Id.
108. https://nevada.public.law/statutes/nrs_293.394
109. https://www.leg.state.nv.us/Division/Legal/LawLibrary/NAC/NAC-293.html#NAC293Sec255
110. See: supra note 7.
111.https://www.nvsos.gov/sos/home/showpublisheddocument/15625/638682082174300000
112. See: supra notes 9 and 81.
113. https://www.ncleg.gov/EnactedLegislation/Statutes/PDF/BySection/Chapter_163/GS_163-182.1.pdf
114. https://www.ncsbe.gov/about-elections/election-security/post-election-procedures-and-audits#reports
115. https://s3.amazonaws.com/dl.ncsbe.gov/State_Board_Meeting_Docs/2024-11-26/Canvass/Post_Election_Audit_Report_2024_General.pdf
116. https://www.ncsbe.gov/news/press-releases/2024/11/26/state-board-unanimously-certifies-2024-general-election
117. https://s3.amazonaws.com/dl.ncsbe.gov/State_Board_Meeting_Docs/2024-11-26/Canvass/Post_Election_Audit_Report_2024_General.pdf
118. https://er.ncsbe.gov/?election_dt=11/05/2024&county_id=0&office=FED&contest=1393
119. https://s3.amazonaws.com/dl.ncsbe.gov/State_Board_Meeting_Docs/2024-11-26/Canvass/Post_Election_Audit_Report_2024_General.pdf

120. According to the Verified Voting Verifier, Cherokee, Davidson, Davie, Jackson, Mecklenburg, Perquimans, and Warren Counties use ballot marking devices for in-person voting. We tallied the in-person ballots audited in these counties to determine this figure.
121. Stein v. Boockvar, Civ. No. 16-6287 (E.D. Pa. Apr. 29, 2019)
122. https://govt.westlaw.com/pac/Document/NE8D7C3E0343011DA8A989F4EECDB8638?transitionType=Default&contextData=%28sc.Default%29
123. Pennsylvania Department of State "DIRECTIVE CONCERNING THE USE, IMPLEMENTATION AND OPERATION OF ELECTRONIC VOTING SYSTEMS BY THE COUNTY BOARDS OF ELECTIONS," 2011. https://www.pa.gov/content/dam/copapwp-pagov/en/dos/old-website-documents/voting-systems/directives/EVS%20Usage%20Directive.pdf
124. https://www.pa.gov/agencies/dos/resources/voting-and-elections-resources/election-reports.html#accordion-f40322de74-item-696ee3851f
125. We excluded ballots audited in counties that require voters to vote on ballot marking devices in polling places.
126. https://www.electionreturns.pa.gov/General/SummaryResults?ElectionID=105&ElectionType=G&IsActive=0
127.https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2026/state/42
128. "How Pennsylvania's 'risk-limiting audits' fall short of the mark due to critical shortcomings in procedures and transparency," Protect Our Votes Philly, (Original version Nov 28, 2022. Last updated January 21, 2025.) https://docs.google.com/document/d/1gF9iHxqv4Q1X-IYzhSiEtZ3ml17p8mPQM7FV2ySxdx4/edit?tab=t.0
129. "2024 Post-Election Voting Equipment Audit Report." Wisconsin Elections Commission, 13 Mar. 2025, elections.wi.gov/resources/reports/2024-post-election-voting-equipment-audit-report.
130. Id.
131. https://elections.wi.gov/media/30351/download