What We Know: Voting Technology and Security

Published August 19, 2020

When voters head to the polls in any election – local, state or federal – they need to know their vote will count and not be subject to malicious interference from foreign nations, malfunctioning machinery, buggy software or human error. Without public confidence in the election system, our democracy is at risk.

The consensus among computer scientists, statisticians, and security experts is that human-readable paper ballots are essential to voting security. Systems that directly record votes electronically without a paper trail are not secure since there is no way of knowing when or if such machines have been compromised or hacked. Ensuring each ballot is recorded in a paper trail that is routinely audited in an efficient, statistically-sound way limits the risk that errors or attacks can affect election results. Such audits can provide statistical evidence of whether an election outcome is accurate with a high level of confidence[1].

The Help America Vote Act of 2002 provided funds to help states and counties upgrade voting equipment and many adopted electronic voting machines[2]. But today many voting systems are outdated and vulnerable to interference or errors and some states and counties lack the funds to replace them. A lack of regular, ongoing funding for election security remains one of the primary concerns of election officials[3, 4]. Despite these challenges, election administrators across the country are working to address election security issues and many recently replaced outdated paperless machines and moved to using paper ballots**.**

While the federal U.S. Election Assistance Commission[5] provides voluntary guidelines and certifies voting systems, individual states have authority over election activities and voting methods and procedures vary greatly from state to state. Policymakers and election officials must consider a number of factors when evaluating voting system technology and processes, here we summarize the scientific evidence related to the following:

- **Voting systems with paper ballots are most effective at protecting and recording individual voters' intent. Systems that rely on directly recording votes electronically are a security risk.**
- **Routine election audits such as risk-limiting audits offer statistical evidence of whether an election outcome is accurate.**
- **While innovative election software and hardware is in development, online voting is not secret or secure**

VOTING MACHINE TECHNOLOGY

What voting technologies are most effective in protecting individual voters' intent?

The science is clear: a voter verifiable paper trail is critical to protect the voter's intent. Voting machines that directly record votes without creating a paper record are not secure.

Paper ballots marked by hand and then hand-counted or fed into a scanner offer the highest level of security because voters make their choices directly and the paper ballots can be audited to verify the results. Of any potential voting method, hand-marked paper ballots provide the fewest opportunities for undetected tampering or computer errors.

> *"Paper ballots form a body of evidence that is not subject to manipulation by faulty software or hardware and that can be used to audit and verify the results of an election."*

Securing the Vote: Protecting American Democracy, 2018 report by the National Academies of Sciences, Engineering, and Medicine

But hand-marked paper ballots may not be practical for all U.S. voters. Electronic voting increases access to the polls for individuals with disabilities and others that may encounter difficulty using paper ballots[6]. The Help America Vote Act mandates at least one accessible voting machine per precinct but advocates argue that such separate voting systems discriminate against the people who need them. Many districts have used electronic voting systems for decades with voters, administrators, poll workers, and other stakeholders familiar and comfortable with such voting methods, an important factor in voter confidence.

In the 2016 election, the majority of Americans voted using hand-marked paper ballots. Approximately two-thirds of U.S. counties used hand-marked paper ballots and the remaining one-third of counties used ballot marking devices or direct recording electronic systems[7].

There are many models of ballot marking devices, most use a touchscreen interface for voters to make their selections[8]. Ballot marking devices frequently offer a number of assistive features that allow voters with disabilities or who may have difficulty marking paper ballots to make their vote selections. Voters are able to check their selections for accuracy and then cast their votes by placing their printed paper ballot in an optical scanner. The ballots are stored and can be used by election officials for audits[9].

Ballot marking devices may be vulnerable to mechanical errors such as printer malfunctions as well as coding errors[10]. Some experts question how frequently voters check the accuracy of their vote, correctly remember their electoral choices for every race, or notice errors when they verify their ballot[11, 12, 13]. More research is needed on this issue.

Ballot marking devices also vary widely in design and configuration. Some devices offer "all in one" or "hybrid" modes that cast and tabulate votes in one device increasing risk[14], as compromised code can affect both the cast ballot and the tabulated result[15]. Some ballot marking devices have features that permit the voter to skip viewing and manually scanning their paper ballot, these 'auto-cast' features are less secure[16].

Some designs may make it more difficult for voters to verify their ballot. For example, some ballot marking devices keep ballots under glass, preventing voters from using assistive tools to examine their choices or making it difficult to see the text because of glare[17]. The use of barcodes on paper ballots also presents additional risk as barcodes containing vote selections could potentially differ from the human-readable portion of the paper ballot [18]. Officials should adopt rigorous audit procedures to mitigate the risk from barcodes.

Direct recording electronic (DRE) systems record a voter's selection directly to the machine's memory and automatically tabulate votes. Many leave no physical record of the cast vote. Some newer direct recording electronic systems may come equipped with printers for voter-verifiable paper audit trails, but voters cannot verify that their electronically recorded vote matches the vote on the paper[19]. These direct recording systems feature numerous vulnerabilities, from malicious hacking to coding errors[20, 21]. Computer scientists have demonstrated the speed and ease with which an individual can alter these machines undetected[22]. The National Academies of Sciences, Engineering and Medicine recommended that these machines be removed from service as soon as possible[23]. In early 2019, the US. Election Assistance Commission released draft updates to its voluntary guidelines that would establish stricter standards that voting systems be auditable and enable evidence-based elections. Direct recording electronic systems would not meet these proposed guidelines[24].

When considering electronic election systems, officials should consider[25]:

- ✓ Does the system provide an auditable, human-readable paper ballot
- ✓ Can voters easily review and verify their selections in print before submitting their ballot?
- ✓ Is the system used to mark the ballot distinct and separate from the system used to record the results?
- ✓ Does the system allow for ballot designs that follow best practices set forth by the U.S. Election Assistance Commission and the National Institute of Standards and Technology?
- **X** Does the system have design flaws that introduce opportunities for unobservable ballot changes that violate the principle of "software independence," such as printers that are part of the same mechanism where cast ballots are collected?[26]

ELECTION AUDITING

What is the most effective way to ensure the accuracy of election results?

The evidence shows that the routine use of statistically driven risk-limiting audits would be the most effective way to ensure the accuracy and security of elections.

With the increase in the use of technology to record and tally votes, auditing election results before they are certified can provide additional assurance of the integrity of the results [27].

While election officials may conduct a number of procedural audits, absent any concerns or with a sufficient margin of victory, election results are often certified without any audit of votes[28].

Risk-limiting audits are designed to provide statistical evidence of whether the outcome of the election is accurate with a high level of confidence[29, 30]. An initial random sample of ballots is examined based on the margin of victory in an election, the total number of cast ballots, and a predetermined level of certainty that the audit will detect and correct an incorrect outcome. If necessary, additional ballots would be examined until there is statistical support for the accuracy of the election outcome. Risk-limiting audits are meant to be a more efficient and statistically sound process than traditional post-election audits that tally a fixed percentage of ballots[31]. Risk-limiting audits require an auditable paper trail, highlighting one of the major weaknesses of paperless direct recording electronic systems[32].

The National Academies of Sciences, Engineering, and Medicine report and general scientific consensus support audits as an essential component of ensuring accurate, secure elections[33]. Risk-limiting audits are endorsed by the American Statistical Association[34].

Colorado, where voters primarily vote by mail, was the first state to conduct risk-limiting audits for statewide elections[35, 36]. Rhode Island[37], Virginia[38] and Nevada[39] passed legislation mandating risk-limiting audits while California[40, 41], Indiana[42, 43], and Georgia[44] passed legislation implementing risk-limiting audit pilots. Michigan[45], New Jersey[46] and Pennsylvania[47] also began administering risk-limiting audit pilots. These pilot programs are an effective way to introduce risk-limiting audits and begin training officials. Washington[48] and Ohio's[49] audit procedures now allow for the option of risk-limiting audits [50, 51].

The specific characteristics of a risk-limiting audit will depend on the voting systems in use but considerations include:

- Risk-limiting audits require a paper trail and are not possible for paperless voting systems

- Risk-limiting audits require a high degree of preparation and coordination among election officials including the use of a ballot manifest, a record of where ballots are physically stored
- Poor ballot design can increase voter mistakes that increase the workload of a risk-limiting audit
- Risk-limiting audits require software to conduct the audit and technical support to ensure the procedures are done properly
- The workforce for the election must be familiar with the election procedures and requirements of the audit to ensure the election is conducted in a manner that fits the planned risk-limiting audit method

Election administrators must also implement rigorous chain of custody and ballot reconciliation practices for protecting the paper audit trail[52].

THE FUTURE OF VOTING TECHNOLOGY

How safe and secure are online voting and other voting systems based on new technology?

There is currently no scientific evidence to support claims that online voting is safe or secure; other technologies are not ready for immediate deployment.

According to a report by the National Academies of Sciences, Engineering, and Medicine, there is currently "no known technology that can guarantee the secrecy, security, and verifiability of a marked ballot transmitted over the Internet." [53]

Online voting presents numerous vulnerabilities and is fundamentally insecure. There is potential for unobserved vote manipulation as well additional security vulnerabilities including potential denial of service attacks, malware intrusions, and privacy concerns. Online voting does not produce a paper trail. In addition, internet voting threatens the secret ballot, a bedrock principle of American elections, as individuals would need to provide digital credentials that cannot be separated from their ballot.

Blockchain-based voting, which relies on a decentralized, distributed digital ledger, has not been proven to be secure and is vulnerable to many of the security flaws inherent in internet voting, such as the potential for malware to alter votes on a voter's local device before the ballot is transmitted and the lack of secret ballots.

Multiple ongoing DARPA projects aim to develop secure hardware focused on developing hardware resistant to software- based attack through novel CPU designs[54,55]. Future systems based on secure hardware could provide additional security, but the technology is still in early development.

End-to-end verifiable election software relies on cryptography to encrypt and protect votes while allowing voters to see their vote was properly recorded, that the vote was correctly tabulated, and that the final vote count matches the cast votes[56]. End-to-end verifiable software can be integrated into existing election systems to enhance the security of voting infrastructure. Recent open-source software packages including end-to-end verifiability systems, such as Microsoft's software development kit ElectionGuard, could increase security if implemented in future elections.

The science is clear: Paper ballots, marked either by hand or machine, are the most effective way to ensure that the votes cast in an election reflect voters' intent. When every vote creates a paper trail that is routinely audited in a statistically-sound method, it provides assurance that votes have been tabulated correctly. Risk-limiting audits provide statistical evidence of whether an election outcome is accurate with a high level of confidence.

---

1 R. V. T. COMMITTEE ON THE FUTURE OF VOTING: ACCESSIBLE, "Securing the Vote: Protecting American Democracy," National Academies of Sciences, Engineering and Medicine, Washington DC, 2018. (Pg. 6-7)

2 The National Commission on Federal Election Reform, "To Assure Pride and Confidence in the Electoral Process," reformelections.org, 2001.

3 Norden, L. et al, "What Does Election Security Cost?," Brennan Center for Justice, 2019. [Online]. Available: https://www.brennancenter.org/our-work/analysis-opinion/what-does-election-security-cost.

4 Howard, E. et al, "Defending Elections: Federal Funding Needs for State Election Security," Brennan Center for Justice, New York City, 2019.

5 "VOLUNTARY VOTING SYSTEM GUIDELINES," US Election Assistance Commission, 2020. [Online]. Available: https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines.

6 l. Schur, "Reducing Obstacles to Voting for People with Disabilities," 2013. [Online]. Available: http://web.mit.edu/supportthevoter/www/files/2013/08/Lisa-Schur-Disability-and-Voting-White-Paper.pdf.

7 Cordova McCadney, A. et al, "Voting Machine Security: Where We Stand a Few Months Before the New Hampshire Primary," Brennan Center for Justice, 2019.

8 "Types of Voting Equipment," National Conference of State Legislatures, 2018. [Online]. Available: https://www.ncsl.org/research/elections-and-campaigns/voting-equipment.aspx.

9 "Ballot Marking Devices," Verified Voting, 2019. [Online]. Available: https://www.verifiedvoting.org/ballot-marking-devices/.

10 A. Appel, "Serious design flaw in ESS ExpressVote touchscreen: "permission to cheat"," Freedom to Tinker, 2018. [Online]. Available: https://freedom-to-tinker.com/2018/09/14/serious-design-flaw-in-ess-expressvote-touchscreen-permission-to-cheat/.

11 S. P. Everett, "The usability of electronic voting machines and how votes can be changed without detection," Rice University, 2007.

12 B. A. e. a. Campbell, "Now do voters notice review screen anomalies? a look at voting system usability," in Conference on electronic Voting Technology, 2009.

13 P. B. Stark, "There is no Reliable Way to Detect Hacked Ballot-Marking Devices," 2019.

14 A. Appel, "Reexamination of an all-in-one voting machine," Freedom to Tinker, 2018. [Online]. Available: https://freedom-to-tinker.com/2019/03/08/reexamination-of-an-all-in-one-voting-machine/

15 Torres, R., "Report Concerning the Examaination Results of Election Systems and Software EVS 6021 with DS200 Precinct scanner, DS450 and DS 850 Central Scanners, Expressvote HW 2.1 Marker and Tabulator, Expressvote XL Tabulator and Electionware EMS," Commonwealth of Pennsylvania Department of State, 2018.

16 Appel, A. et al, "Ballot-Marking Devices (BMDs) Cannot Assure the Will of the Voters," SSRN, 2019.

17 "Voting Equipment," National Conference of State Legislatures, 2019. [Online]. https://www.ncsl.org/research/elections-and-campaigns/voting-equipment.aspx

18 A. Appel, "Continuous-roll VVPAT under glass: an idea whose time has passed," Freedom to Tinker, 2018. [Online]. Available: https://freedom-to-tinker.com/2018/10/19/continuous-roll-vvpat-under-glass-an-idea-whose-time-has-passed/.

19 "Voting System Paper Trail Requirements," National Conference of State Legislatures, 2019. [Online]. Available: https://www.ncsl.org/research/elections-and-campaigns/voting-system-paper-trail-requirements.aspx

20 Bannet, J. et al, "Hack-a-Vote: Demonstrating Security Issues with Electronic Voting Systems," IEEE Secuirty and Privacy, vol. 2, pp. 32-37, 2004.

21 Bernhard, M. et al, "Can Voters Detect Malicious Manipulation of Ballot Marking Devices?," 2020.

22 Curling v. Raffensperger, 2019.

23 R. V. T. COMMITTEE ON THE FUTURE OF VOTING: ACCESSIBLE, "Securing the Vote: Protecting American Democracy," National Academies of Sciences, Engineering and Medicine, Washington DC, 2018. (Pg. 7, 80)

24 "Report of the Auditability Working Group," Election Assistance Comission, Washington DC, 2011.

25 "Observations on Voting Equipment Use and Replacement," Government Accountability Office, Washington DC, 2018.

26 "Report of the Auditability Working Group," Election Assistance Comission, Washington DC, 2011.

27 "Post-Election Audits," National Conference of State Legislatures, 2019. [Online]. Available: https://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx.

28 "Post-Election Audits," National Conference of State Legislatures, 2019. [Online]. Available: https://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx.

29 R. V. T. COMMITTEE ON THE FUTURE OF VOTING: ACCESSIBLE, "Securing the Vote: Protecting American Democracy," National Academies of Sciences, Engineering and Medicine, Washington DC, 2018. (Pg. 9, 53, 95, 100)

30 P. B. Stark, "There is no Reliable Way to Detect Hacked Ballot-Marking Devices," 2019.

31 Lindeman, M. et al, "Retabulations, Machine-Assisted Audits, and Election Verification," 2013.

32 Lindeman, M. et al, "A Gentle Introduction to Risk-Limiting Audits," in IEEE SECURITY AND PRIVACY, SPECIAL ISSUE ON ELECTRONIC VOTING, 2012.

33 R. V. T. COMMITTEE ON THE FUTURE OF VOTING: ACCESSIBLE, "Securing the Vote: Protecting American Democracy," National Academies of Sciences, Engineering and Medicine, Washington DC, 2018. (Pg. 9, 53, 95, 100)

34 "ASA Endorses Post-Election Audits Principles," American Statistical Association, 2019. [Online]. Available: https://www.amstat.org/asa/News/ASA-Endorses-Post-Election-Audits-Principles.aspx.

35 Shellman, D. et al, "Colorado's Implementation of Risk-Limiting Audits," Election Assistance Commission, 2017. [Online]. Available: https://www.eac.gov/colorados-implementation-of-risk-limiting-audits.

36 "The Colorado Risk-Limiting Audit Project (CORLA)," [Online]. Available: http://bcn.boulder.co.us/~neal/elections/corla/.

37 B. C. f. Justice, "Rhode Island RLA Working Group: Pilot Implementation Study of Risk-Limiting Audit Methods in the State of Rhode Island," 3 September 2019. [Online].

38 R. I. B. o. Elections, "Press Release: Board of Elections conducts two additional successful post-election Risk Limiting Audits," 19 December 2019. [Online]. Available: https://www.ri.gov/press/view/37355.

39 Nevada SB 123, Sec. 8 & 86

40 C. S. o. State, "California Secretary of State Proposed Regulatory Action: Risk Limiting Audits Proposed Regulation Text," 2019.

41 A. Appel, "Pilots of risk-limiting election audits in California and Virginia," Freedom to Tinker, 2018. [Online]. Available: https://freedom-to-tinker.com/2018/12/10/pilots-of-risk-limiting-election-audits-in-california-and-virginia/.

42 Indiana SB 405, 2019.

43 V. S. T. O. Program, "Risk-Limiting Audit (RLA) conducted at Porter County, Indiana on January 24-25 2019," Ball State University, 2019.

44 Georgia HB 316, 2019.

45 K. Ottoboni, "Piloting Risk-Limiting Audits in Michigan," Institute for Data Science, 2018. [Online]. Available: https://bids.berkeley.edu/news/piloting-risk-limiting-audits-michigan.

46 T. Gilfillian, "Secretary Way, State Election Officials Take Part In Pilot Risk-Limiting Audit," the State of New Jersey, 2019. [Online]. Available: https://nj.gov/state/press-2019-0308.shtml.

47 “Pennsylvania to Pilot Cutting-Edge Election Security Measures,” Pennsylvania Department of State, 2019. [Online]. Available: https://www.media.pa.gov/Pages/State-details.aspx?newsid=358

48 Washington §29A.60.185

49 Ohio Secretary of State Directive: 2017-14

50 E. Howard, "A Review of Robust Post-Election Audits," Brennan Center for Justice, 2019.

51 Stark, P. B. et al, "Evidence-Based Election," IEEE Security and Privacy, 2012.

52 N. McBurnett, "Auditing Use Case," NIST, 2017. [Online]. Available: https://collaborate.nist.gov/voting/bin/view/Voting/AuditingUseCase.

53 R. V. T. COMMITTEE ON THE FUTURE OF VOTING: ACCESSIBLE, "Securing the Vote: Protecting American Democracy," National Academies of Sciences, Engineering and Medicine, Washington DC, 2018. (Pg. 9)

54 "Hacker Community to Take on DARPA Hardware Defenses at DEF CON 2019," DARPA, 2019. [Online]. Available: https://www.darpa.mil/news-events/2019-08-01.

55 "System Security Integrated Through Hardware and Firmware (SSITH) Proposers Day," DARPA, 2017. [Online]. Available: https://www.darpa.mil/news-events/ssith-proposers-day.

56 A. Appel, "End-to-End Verifiable Elections," Freedom to Tinker, 2018. [Online]. Available: https://freedom-to-tinker.com/2018/11/05/end-to-end-verifiable-elections/.