Securing the Nation's Voting Machines

A Toolkit for Advocates and Election Officials

On March 23, 2018, Congress approved $380 million "to improve the administration of elections for Federal office, including to enhance election technology and make election security improvements." These funds are available to states immediately.

While states will have flexibility in how they use this money, Congress has emphasized the importance of having a voter-verified paper record of every vote. In a memo accompanying the appropriations, Congress also recommended those paper records be used to conduct post-election audits, ensuring voting machines have produced an accurate result.

This toolkit, created jointly by the Brennan Center for Justice, Common Cause, the National Election Defense Coalition, and Verified Voting, is meant as a roadmap for advocates and election officials nationwide as local jurisdictions consider purchasing new voting machines. It also suggests best practices for conducting post-election audits.

Purchasing New Machines

Which voting machines should be replaced immediately?

Any voting equipment that does not use a paper ballot marked by the voter, either manually or with a ballot marking device, should be replaced **immediately**. These machines do not retain a paper ballot for recounts and audits, meaning that there may be little or no recourse for an accurate recount if any errors occur. Over the past decade, many states have replaced direct-recording electronic machines (DREs) — voting equipment that records directly into computer memory — with voting systems that use voter-marked paper ballots.

Voting equipment that produces a "Voter Verifiable Paper Audit Trail" (VVPAT) is better than equipment that only records votes in computer memory. However, VVPATs recorded on continuous rolls of thermal paper are difficult and costly to audit, and voters are much less likely to verify their votes on such machines.

In 2006, only 24 percent of registered voters lived in counties using all-paper ballot voting systems. As awareness of security risks has grown, that percentage has more than doubled. Today, 53 percent of registered voters live in counties using all paper ballots.

In addition to replacing paperless voting machines, states and counties should also replace older voting equipment that a) can no longer be serviced by the machine vendor or b) runs an operating system no longer supported by the original software vendor. In a recent Brennan Center survey, election officials in 33 states reported that their equipment needs to be replaced by 2020. Of these officials, two-thirds said they have inadequate funds to obtain new equipment. Many of the voting machines they use are no longer manufactured, and with replacement parts often not available, election officials are relying on eBay and unregulated vendors to keep these machines functioning.

Why are paper ballots important?

Paper ballots create tangible, tamper-evident and auditable records of how each voter voted. When these ballots are retained securely, they provide trustworthy hard-copy evidence that election officials can use for regular post-election checks to address the possibility that the computerized voting systems might have been hacked, misprogrammed, or simply malfunctioned.

What are the benefits of replacing paperless voting machines with machines that use paper ballots?

Increased security. Today's security threats are even greater than the threats posed when antiquated voting systems were originally purchased. Security experts warn of the growing cyber threats to our election systems as hackers become increasingly sophisticated. They have successfully targeted election agencies and infrastructure around the world, as well as local election authorities here in the United States.

Even systems not connected to the internet are vulnerable to viruses and malware spread through portable memory devices. Furthermore, sophisticated software attacks can be designed to be inactive and undetectable during pre-election testing. While all computers are vulnerable to software errors and mechanical malfunction, paper ballot-based voting, coupled with secure chain-of-custody procedures, provides a trustworthy means of detecting and recovering from an attack or malfunction.

Public confidence. Close elections happen in every state. Election officials understand that heated political campaigns can result in additional scrutiny of the election administration system in general. When voters' only recourse is to rely on the proper functioning of a computer and its software, there can be doubt about the integrity of the election. Using voter-marked paper ballots as a check on the computers will make our systems auditable, boosting voter confidence in case of a recount.

What equipment should be purchased?

States and counties should purchase paper-based voting systems in which the voter is able to mark the ballot themselves with a pen or pencil. Voters who want or need assistive technology can use ballot marking devices to mark paper ballots. Ballots marked in a polling place should be cast on a system that will notify voters if they have made correctable mistakes (for instance, voting for too many candidates or failing to make a readable mark for a particular contest). The voting system must retain those ballots for recounts and audits.

What are ballot marking devices?

While most voters mark their paper ballots with a pen or pencil, not everyone can do so. Ballot marking devices are special-purpose computers with a user interface such as a touchscreen or keypad that allow a voter to mark a paper ballot. Voters who use these machines do so instead of marking their choices with a pen or pencil. Ballot marking devices incorporate a variety of assistive technologies for people with vision and mobility disabilities, can allow voters to adjust the text size of ballots displayed on screen, provide a read-aloud audio function as a method of ballot verification other than visual inspection, and permit jurisdictions to present ballots in multiple languages.[1]

Federal law requires that each polling place provide voters with disabilities a means of voting privately and independently. Having at least one ballot marking device in each polling place can help satisfy this requirement.

Some ballot marking devices produce a standard ballot that displays the voters' marks in human readable form. Some also encode voters' votes into a QR code and/or bar code that also appears on the ballot. If QR or bar codes are used, it is vital that state law require the code and human-readable ballot to be on the same paper, so they can easily be audited to ensure that they contain the same information. Voters should be instructed to carefully review the ballot selections recorded on the paper and confirm they are correct. If an error is found, voters should be instructed to contact a poll-worker and re-mark the ballot. Manual post-election audits and recounts should require election workers to review the human-readable indications to ensure that the scanning computer has not miscounted the ballots.

For a comparison of the features of different ballot marking devices that are currently available and discussion of how they can be used in combination with hand-marked paper ballots, see Verified Voting's "Ballot Marking Devices Features Comparison."

How are voting systems replaced?

The procedure for replacing voting systems varies by state. In some states, the chief state election official may issue a directive, while in others, the state legislature must enact changes to existing law to allow for paper-based systems. Elsewhere, the state board of elections can decertify paperless voting systems and mandate the purchase of paper-based systems.[2]

Who pays for new equipment?

The responsibility for costs related to purchasing, maintaining, and servicing new voting equipment also varies by state. Federal HAVA Election Security Grant funds may be used for a variety of election administration purposes, though in its report language Congress listed replacement of paperless voting equipment first among potential uses of the funds. Additional information about the allocation of this responsibility by state is available here.

If voter-marked paper ballot systems are currently certified, a state or locality may issue a request for proposal to replace their voting equipment. Although procurement regulations vary, many election authorities have previously issued Requests for Proposals ("RFPs") which may be helpful to review. These include Maryland; Dakota County, Minnesota; Jones County, Iowa; and San Francisco, California.

The Belfer Center at Harvard Kennedy School has created a list of security provisions that should be required in all election system RFPs and vendor bids. RFPs should also specify that voting equipment must not include any wireless capability.

Additional Resources:

- Verified Voting's Verifier database and Voting Equipment Descriptions of systems used in each state and local jurisdiction.

- Report by the Brennan Center: America's Voting Machines at Risk as well the 2018 update.

- The Brennan Center's description of different categories of voting equipment.

- Report by the Belfer Center for Science and International Affairs at Harvard Kennedy School: The State and Local Election Cybersecurity Playbook

- Report by the Center for American Progress: Election Security in All 50 States

Counting Paper Ballots and Conducting Post-Election Audits

How are voter-marked paper ballots counted?

Most often, voter-marked paper ballots are fed into an optical scanner which reads voters' marks and then adds them up. In some cases, the voters' marks may also be incorporated into a bar code or QR code to be read by the scanner.

How are votes counted on a scanner sent back to the election office? Why can't they be transmitted directly from the machine?

At the close of polls, the removable memory device containing vote totals (often a thumb drive) and the printed total tape for each machine should be secured and transported from the polling place to the local election office or other central collection point.

Security experts and the US Senate Intelligence Committee have recommended that voting equipment not have wi-fi capability. While some scanners have the built-in option of directly transmitting vote totals to election management systems through wireless or analog modems, this remote connection makes the equipment a potential target for hackers. Some states have resisted voting equipment vendors' efforts to sell equipment with this additional feature. Purchasing agencies should use their leverage as buyers to ensure that the equipment they buy is as secure as possible.

Why are post-election audits necessary?

Replacing paperless voting systems with paper-based systems is just the first step in ensuring accurate election results. As discussed above, most election jurisdictions that use paper ballots count those ballots using a computerized scanner. These scanners, like any computers and the software they use, are vulnerable to hardware and software malfunctions, programming errors, and hacking that may not be detectable through more common pre- and post-election testing and procedures. There have been elections in which the wrong candidate has been initially declared the winner because of a simple software glitch or programming error in the computerized scanner tallying the votes. In some rare cases, scanners have failed to count certain ballots due to calibration or other hardware errors (such as not being able to detect red pen marks).

Routine manual post-election audits designed to provide a high level of statistical confidence can help ensure that election results are correct.

What are the elements of a good audit?

To ensure confidence in election results, election officials should implement routine audit protocols that require the following:

Audits must be conducted on individual election contests. Thorough and effective post-election audits review the results of individual contests that appear on the ballot. This procedure is necessary to test whether the vote tallies for individual contests, e.g., governor or sheriff, are accurate and to certify the correct winner.

Manual audits must include a human review of voters' choices. Using a computer to check election results makes the audit process itself vulnerable to hacking, hardware malfunctions, and programming errors. Audits must include a meaningful human inspection of readable, voter-verifiable marks on paper ballots compared with electronic tallies.

Audits must continue until there is adequate confidence in the results. Audit protocols should allow for expanding the number of ballots examined until there is convincing evidence that the election results reflect the choice of the voters.

Audits must be conducted transparently. One main goal of implementing a post-election audit is to increase public confidence in elections. Officials should allow the public to observe the post-election audit process in sufficient detail to confirm that the audit was conducted correctly and did not stop prematurely. Such openness is integral to increasing public confidence in election results.

All ballots must be included in the outcome that is being audited. In each election contest, every vote matters, so every validly cast ballot in the election should be included, such as validly cast provisional ballots, absentee ballots, ballots cast in an early voting process, and ballots cast by overseas and military voters.

Audits must take place before the election is certified. Audits should serve as a compulsory check on the election results, providing an opportunity to confirm or correct the outcome. Therefore, audits should be conducted before certification. If an audit uncovers an incorrect outcome, the previously reported outcome should not be certified.

The choice of ballots to be audited must be random and must occur after the election is held. Some jurisdictions currently announce ahead of time what precincts or contests are going to be audited, which alerts hackers to which precincts they should avoid.

Paper ballots must be adequately curated and tracked during the entire election process. Unless all ballots cast in the election are properly tracked and cared for, the audit cannot be conducted using a trustworthy record of the votes cast.

Audits should provide high statistical confidence that the certified outcome is accurate. While many states have some sort of post-election audits, only Colorado currently mandates a "risk limiting audit," which are post-election audits designed to provide a high level of statistical confidence that a software hack or bug could not have produced the wrong outcome. Rhode Island's legislature recently passed legislation requiring such audits be implemented statewide by 2020. In this current threat environment, where a nation state can easily infiltrate vote tallying systems and the sophisticated actors targeting our elections have billions of dollars of resources, we need the strongest audits possible to protect our democracy.

How are post-election audits instituted?

In some states, it is necessary to pass a law requiring audits, while in others, the chief election official of the state, county or other jurisdiction may issue regulations to require audits.[3] Even without a change in law or regulations, some election officials may have the authority to pilot post-election audits — a one-time test that will allow them to develop best practices that can then inform new laws or regulations.[4]

Other Resources on Post-Election Audits:

- Principles and Best Practices for Post-Election Audits

- A Gentle Introduction to Risk Limiting Audits

- A searchable database cataloging current state laws that require and regulate post-election audits is available at verifiedvoting.org/state-audit-laws.

- The Election Assistance Commission's resources on audits and recounts are here.

Endnotes

[1] Jurisdictions will need to consider both the advantages and disadvantages of choosing ballot marking devices for all voters instead of having one ballot marking device per precinct. Like DRE systems, the choice of ballot marking devices for all voters can be much more expensive than choosing a combinations of voting methods including stations where voters mark the ballot with a pen themselves and ballot marking devices for people with disabilities or people who prefer them. For a more detailed description of optical scan and ballot marking devices, see the Brennan Center's description of voting equipment and Verified Voting's "Voting Equipment in the United States."

[2] For example, in 2007 Maryland enacted HB 18 which required the state elections board to select, certify, and implement a new statewide voting system that uses voter-marked paper ballots. In 2013, North Carolina passed HB 159 decertifying DREs and prohibiting their use in elections held on or after January 1, 2018. This deadline was subsequently extended to September 1, 2019.

California and Virginia have both decertified paperless voting systems.

Minnesota and New York enacted laws to prohibit the use of voting machines connected to the internet. In Texas, the Secretary of State simply issued a directive. In Pennsylvania, the Secretary of State announced that counties would be required to select paper-based systems to replace existing paperless systems by 2019.

[3] For example, Virginia law allows localities to conduct post-election audits upon agreement between the State Board of Elections and the locality. In Ohio, the Secretary of State mandates post-election audits and allows the locality to choose between three different types of post-election audits. While Florida state law requires certain types of post-election audits, municipalities may have authority to pilot other types of post-election audits.

[4] Maine authorizes various state officials and legislative bodies to inspect ballots used in an election which may enable a pilot post-election audit. North Carolina currently requires post-election audits and provides the North Carolina State Board of Elections (SBE) with broad authority over this process. The SBE, subject to some statutory restrictions, may be able to authorize pilots of new types of post-election audits.