Election Security

Everyone wants to live in a society where our elections are free, fair and accurate. In the past few elections, Americans of all political stripes have recognized our election systems are vulnerable to attack and malfunction.

Some concerns are legitimate, but others rely on false claims regarding election equipment fraud and procedural misconduct It is critical that we recognize the what changes we need for our voting systems and recognize when suggestions and concerns are ill-founded or aimed at generating mistrust of American democratic institutions rather than ensuring correctly run elections.

EFF has been involved in election security issues in the U.S. for 20 years and was one of the first organizations to sound the alarm about paperless electronic voting systems. One frequent claim we see is that the multiplicity of voting systems across the country makes it more difficult to tamper with election results. Sadly, that is not necessarily the case. With close margins in so many races across the country, tampering in a small number of precincts can easily lead to the wrong person being elected (or a proposition passing or failing) locally and even nationally. On the other hand, false claims of fraud aimed at undermining election results and preventing citizens from voting poses a different kind of threat to election security. We need to build security and resilience into our election systems.

Happily, there are a few simple things that we can do to make our elections significantly more secure and increase public confidence in the election results. There are also some dangerous ideas that lawmakers should avoid.

Good Ideas

- **Voter Verified Paper Audit Trail.** Election results must be verifiably accurate—that is, auditable with a permanent, voter-verified paper record that is independent of hardware or software. For electronic voting machines, the machine must print a paper record that the voter can check, and which is preserved for use in recounts and audits. The Brennan Center estimates that 93% of all votes cast during the 2020 election had a paper record, up from 82% in 2016. Since 2020, more states have switched to systems that produce paper records of the votes cast. In the 2024 election, only Louisiana and certain counties in Texas and Mississippi are likely to use paperless voting equipment. Bringing those systems up to the modern standard should be a priority. In addition, if the ballots generated by a voting machine include barcodes or QR codes, they must also include human-readable text to enable verification by voters, and audits and recounts by election officials.
- **Risk-Limiting Audits (RLAs).** Risk-limiting audits use statistical sampling to achieve high-confidence audits with a cost low enough that they can be

performed on every election. In many cases, a risk-limiting audit can be performed by counting only a small fraction of ballots cast. For example, MIT professor Ron Rivest calculated that Michigan could have checked just 11% of the ballots and achieved 95% confidence that their machine-counted result correctly named Donald Trump the winner of Michigan's electoral votes in 2016. Closer contests may require a greater fraction of votes to be counted. For example, in 2020, due to the tight margin of the race in Georgia, the RLA was conducted by a full manual tally of all votes cast. RLAs help jurisdictions better allocate their resources by checking more ballots in close contests and fewer ballots when the margins are wider. Colorado, Georgia, Nevada, Pennsylvania, Rhode Island and Virginia require RLAs and other states should follow. Further, best practices require audits to be conducted before the official election results become final and to change incorrect outcomes.

- **Replace Outdated Voting Equipment.** Modern electronic voting machines have a lifespan of 10 to 20 years, and for most systems this number is closer to 10. Small technical failures of voting equipment may lead to harmful misinformation about the reliability of election results, even if the checks incorporated into the election administration process can catch any issues that may cause significant disruptions. In November 2024, most states are expected to be using voting equipment that was first fielded more than 10 years ago at least in some of their counties. Furthermore, some of these voting machines have been discontinued, which makes it difficult to find replacement parts.
- **Air Gaps and Chain of Custody.** High-security systems are best secured by ensuring they never connect to the Internet, dial a modem, or communicate wirelessly. Any voting machines that violate this practice by including modem capabilities should be replaced. Air gaps mean that updates must be hand-delivered on SD cards or thumb drives; chain of custody procedures must be used to ensure those updates are not tampered with or generated on compromised computers.
- **Protections for Security Researchers.** Voting machine manufacturers sometimes use the law to intimidate legitimate security researchers out of criticizing flaws in their machines. This harms election security and should be discouraged.
- **Paper Backups for Electronic Poll Books.** Currently over 85% of registered voters live in jurisdictions using electronic poll books, up from 49.5% in 2016. Electronic poll books expedite the voting process, decrease the costs, and offer additional functionalities supporting the election administration. However, they are also vulnerable to technical failures, power outages, or cyberattacks. Jurisdictions using electronic poll books should have backup voter lists in the form of pre-printed paper copies, or at least, in the form of digital copies on a nonnetworked device, to avoid long lines that might deter citizens from voting in the event of a technical failure. Polling places should also have enough provisional ballots in case there are errors in the backup copies. To minimize security risks, jurisdictions using electronic poll books should avoid or limit wireless connectivity, opting for a hardwired connection whenever possible.

- **Emergency Paper Ballots.** Jurisdictions using electronic voting machines should make available emergency paper ballots to ensure that citizens can vote even if voting technologies fail. This means keeping a sufficient number on hand at all times.
- **Transition the Election Office Websites to .gov Domains.** In 2020, the FBI identified dozens of illegitimate websites that mimicked official election websites to mislead the voters. Transitioning to .gov domains can help combat misinformation by making it easier for the public to distinguish between authentic and fake websites. Using .gov also has security benefits because multi-factor authentication is enforced on all accounts in the .gov registrar and .gov domains require busing a secure HTTPS connection.
- **Multi-Factor Authentication.** Multi-factor authentication should be implemented on the systems and applications that provide access to sensitive data or administrative functions within the election infrastructure.

Bad Ideas

- **Internet Voting.** Voted ballots sent via Internet simply cannot be made secure currently. Worse, they make easy and inviting targets for attackers, from lone hackers to foreign governments seeking to undermine US elections. Unlike commerce and other sorts of online transactions, the security, privacy, and transparency requirements for online voting are much more complex and stringent. Internet voting is sometimes proposed as a method to enhance inclusivity, but there are better ways to make elections more accessible. For example, states can bring voting devices directly to voters who are unable to vote at in-person voting locations, or provide a well-designed remote accessible vote-by-mail (RAVBM) option, which would allow eligible voters to download their ballot on their own device, mark it using their own software, and print and return the ballot according to the rules in their jurisdiction.
- **Electronic-Only Audits.** After the 2016 election, many Wisconsin counties simply ran ballots through their tabulating machines a second time and called it an "audit." But if machines are broken or compromised, the same inaccuracies they registered the first time will show up again the second time. This is why voter-verifiable paper audit trails and risk limiting audits are critical.
- **Elimination of All Vote Counting Machines.** In 2023, eight states introduced bills that would effectively ban the use of vote counting machines. While hand counts are critical in post-election audits and recounts, requiring humans to hand count all ballots cast at the election night to get the initial election results could hinder election administration. Vote counting machines can count large quantities of ballots more quickly and more accurately than humans do under the demanding conditions of the election night. Some smaller jurisdictions already hand count all ballots and they should continue doing so. However, requiring all jurisdictions to implement election night hand counts is not feasible due to its high cost. Instead, the accuracy of the unofficial results from vote counting machines should be checked by RLAs.