ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Defending Freedom on the Electronic Frontier eff.org

Election Security

The efforts of the Russians and others to impact the U.S. elections have led to a long-overdue recognition that our election systems are vulnerable to attack and malfunction across the political spectrum. As recently as February 15, 2018, Michael Chertoff and Grover Norquist penned an op-ed in the Washington Post raising concerns and rightly noting that this is a key cybersecurity concern.

American voting relies heavily on technology. While elections are administered locally, and local control is critical, there is a longstanding tradition of federal assistance in the purchase of equipment plus support for training and administration of local elections, including the Help America Vote Act passed after the “hanging chad” problems in Florida in 2000 and the creation of the Election Administration Commission.

The multiplicity of voting systems across the country doesn’t necessarily make it harder to tamper with U.S. elections. Given the 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 locally and even nationally.

Luckily, there are a few simple things that we can do to make our elections significantly more secure. There are also some dangerous ideas that Congress should work to avoid.

For more information please contact India McKinney at india@eff.org

Good Ideas

Voter Verified Paper Audit Trail. Election results must be *verifiably accurate*— that is, auditable with a permanent, voter-verified 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. Five states (Louisiana, Georgia, South Carolina, Delaware, and New Jersey) have no paper trail and bringing those systems up to the modern standard should be a top priority. Other states have a mix of systems, some with paper trail and some without.

Risk Limiting Audits. 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 nearly all cases, a risk-limiting audit can be performed by counting only a small fraction of ballots cast. For example, MIT professor Ron Rivest calculates 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. Colorado has implemented risk limiting audits and other states should follow.

Include Cybersecurity Expertise on the Election Assistance Commission. The EAC, created after the 2000 election, is charged with assisting state and local election officials and maintaining voluntary guidelines for voting systems, including cybersecurity standards. Most states use these guidelines when purchasing new voting equipment.

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. Some voting machines violate this practice by including modem capabilities; these 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.

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.

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.