The Washington Post

PowerPost

Follow @powerpost
Get The Daily 202 Newsletter

PowerPost Analysis

The Cybersecurity 202: How Colorado became the safest state to cast a vote

By Derek Hawkins

THE KEY

As local officials across the country scramble to hack-proof their voting systems ahead of the midterm elections, there's one state that is paving the way as a leader in election security.

Colorado has done virtually everything election experts recommend states do to stave off a repeat of 2016, when Russian hackers targeted 21 states as part of the Russian government's massive election interference campaign.

The state records every vote on a paper ballot. It conducts rigorous post-election audits favored by voting researchers. Nearly every county is equipped with up-to-date voting machines. Election officials take part in security trainings and IT workers test computer networks for weaknesses.

Secretary of State Wayne Williams told me the state benefited from having some of those measures in place before 2016. Once the extent of Russia's digital campaign in the presidential election became clear, he made it a priority to invest more in them, he said.

"If people perceive a risk, they're less likely to participate in voting," Williams said. "We want to protect people from that threat, and we want to people to perceive that they are protected from that threat."

Although there's no evidence that votes were altered in 2016, the stakes are high.

The Senate Intelligence Committee, which is investigating Russia's interference, released a report this week affirming that states should be the main entities running elections. But lawmakers said they're still concerned about potential vulnerabilities in election infrastructure.

For instance, the committee found, voting systems across the United States are outdated. Thirteen

states use machines that don't have paper records of votes as backup counting systems, and five of those states use paperless machines exclusively. What's more, lawmakers fear the vendors of election equipment and software may be "an enticing target for malicious cyber actors" – and authorities at all levels have little insight into their security practices.

Despite these concerns, there is near consensus on how states should secure their election systems.

The recommendations from experts and the federal government boil down to three main steps:

- **Switch to paper ballots or voting machines that produce a paper trail.** This creates a physical record of the vote and, unlike electronic voting machines or machines connected to the Internet, hand-marked ballots can't be hacked.

- **Check the results using a "risk-limiting audit,"** which counts a sample of ballots by hand and compares them to machine tallies and is especially effective in close races. While a majority of states require post-election audits, **experts widely agree that only risk-limiting audits are comprehensive enough to detect a cyberattack**.
- **Conduct frequent and rigorous risk assessments** — and make sure election workers are well trained to identify it when something goes wrong.

Nationwide, states are taking a variety of measures to bolster their election systems ahead of November, from replacing old equipment to conducting vulnerability tests to hiring new staff. **But few, if any, have gone as far as Colorado has — indeed, many states don't have the funding to make the upgrades.**

Although more than half of all states require post-election auditing, only Colorado, Rhode Island and New Mexico use risk-limiting audits. Delaware, Georgia, Louisiana, New Jersey and South Carolina all rely exclusively on electronic voting machines without a paper audit trail. Pennsylvania is struggling to replace its outdated, hackable equipment.

"Colorado is certainly hitting all the high points that we've been arguing others should," said Joseph Lorenzo Hall, chief technologist at the Center for Democracy and Technology and an expert on voting systems. **"It's hard to compare states apples-to-apples because they're so different, but Colorado has really been a leader."**

Williams said Colorado's voting process helped put it ahead of the curve: The state allows citizen initiatives and tax debt decisions to be included on ballots, so he says that paper ballots are just more practical given the long list of items people are asked to vote on.

The state has been proactive in other ways, too. Its county clerks, for example, use two-factor authentication to access voter registration databases, which Russian hackers targeted in 2016. And in 2017 it became the first state in the country to complete a statewide risk-limiting audit.

“In Colorado, even if something happens, I don’t have to worry about it because there’s a process in place,” said Marian Schneider, president of the nonprofit organization Verified Voting. **“It’s almost like a disaster recovery plan for elections — that if a disaster were to befall the vote count, we could recover from it.”**

PINGED, PATCHED, PWNED

PINGED: John Bolton, President Trump's national security adviser, and his aides are considering ending the position of White House cybersecurity coordinator, Politico's Eric Geller reported yesterday.

Rob Joyce, who currently holds the position, heads to the National Security Agency on Friday. “Bolton’s deputy, Mira Ricardel, supports the idea of eliminating the coordinator role, according to two of the sources,” Geller writes. “ 'She’s thinking about whether to simply pick up the [cyber] function on her own,' said [a former U.S. official], who added that the odds were '60-40' that the White House would eliminate the job.”

— A few more juicy details from the story:

- **The decision to eliminate the post may not be a done deal.** Christopher Krebs, a top DHS cyber official, was apparently seeking suggestions for a new coordinator at the RSA Conference in San Francisco.
- **Yet others said White House staffers were told not to offer their own replacement ideas.** One former official said the aides in charge of cybersecurity issues on the National Security Council were “a little on pins and needles when they heard that.”

Chris Painter, who served as State Department cyber coordinator during the Obama administration, said terminating the position “would be a huge step backwards:”

PATCHED: The House Foreign Affairs Committee yesterday passed a bill aiming to encourage ethical hackers to explore the State Department's online systems in search of weaknesses or bugs, Nextgov's Joseph Marks writes.

The legislation, titled Hack Your State Department Act, would direct the secretary of state to "design and establish a Vulnerability Disclosure Program (VDP) to improve Department of State cybersecurity