Election security means much more than just new voting machines

April 9 2018, by Jamie Winterton

In late March, Congress passed a significant spending bill that included US$380 million in state grants to improve election infrastructure. As the U.S. ramps up for the 2018 midterm elections, that may seem like a huge amount of money, but it's really only a start at securing the country's voting systems.

A 2015 report by the Brennan Center law and policy institute at New York University estimates overhauling the nation's voting system could cost more than $1 billion – though the price could be partially offset by more efficient contracting. Most voting equipment hasn't been updated since the early 2000s. At times, election officials must buy voting machine hardware on eBay, because the companies that made them are no longer in business. Even when working properly, those machines are not secure: At the 2017 DEF CON hacker conference, attackers took control of several voting machines in a matter of minutes.

Securing electoral systems across the U.S. is a big problem with high stakes. This federal money being provided to states now may not be the last of its kind, but it's what's available right away, and it must be used as efficiently as possible.

1. A reliable backup system: Paper ballots

The security community has been clamoring for paper ballots for years. Now, with evidence of election hacking in 2016 and the vivid

demonstration of voting machine vulnerability, the idea is gaining traction.

Paper ballots aren't perfect – remember "hanging chads"? – but they provide a physical record that can be compared to electronic records. And if there are discrepancies between the two, paper provides a way to track down the source of the problem. Even if votes are counted electronically, keeping paper ballots provides a way to validate and verify the results if they're in question – rather than just hoping the electronics are secure.

2. Examining the whole problem

Discussing the Senate Select Committee on Intelligence's investigation into Russian efforts to manipulate state election systems, Chairman Richard Burr, a North Carolina Republican, said, "It's clear the Russian government was looking for vulnerabilities." U.S. election officials should do the same: Probe election systems to identify weaknesses, but then also fix them.

And like the Russians, the U.S. must think about the entire electoral system. Beyond the machines that tabulate votes, which have been at the center of the conversation, there are many other pieces in the system. These include the ways people register to vote, where their records are kept, and how they are verified at the polls as legitimate voters. And there's what happens after votes are tabulated, as they're being reported from individual polling places to central municipal records and up to state election officials.

At least 10 states' voting registration systems were compromised, most likely by the Russians in the lead-up to the 2016 U.S. presidential election. Despite relief that votes themselves were not changed, these registration systems dictate who is allowed to vote and where, and how

voting materials (like referendum information and absentee ballots) are distributed. Elections are often determined by small margins. Selectively disenfranchising a small percentage of voters could very well swing the results.

3. Securing voters, not just machines

Election security isn't a problem that will be solved just with technology. Democracy depends on people – specifically, their trust that the system is valid and secure. If that trust continues to erode, fewer of them will participate in elections, and some may begin to reject officially reported results.

In 2016, voter turnout was at a 20-year low, with only 55 percent of eligible citizens casting votes. Younger voters have lower turnout than older voters – for example, while more than 70 percent of eligible voters over the age of 60 cast votes in 2016, only 43 percent of people in the 18-to-29-year-old bracket did so.

The government must not only act, but also reassure the electorate that those actions reflect how seriously officials are taking public concerns. States may want to consider something similar to the "Hack the Pentagon" program, which has been publicly visible as well as effective in flushing out security issues in specific Defense Department systems. "Whether you're a well-funded government like the U.S. or anyone else, you have to work with the hacker community," said Katie Moussouris, who helped start "Hack the Pentagon" and also created Microsoft's bug bounty program. It's a bold move, but inviting white-hat hackers to publicly probe election systems – and paying them for information on the vulnerabilities they find – would show voters that states are serious about solving problems.

There is a lot of work to do to secure U.S. elections, but $380 million is

a good way to start. If states spend it in the most meaningful ways – patching both their machines and the population's trust – they will build a system that's secure, trustworthy and works for all the people.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: Election security means much more than just new voting machines (2018, April 9) retrieved 25 April 2024 from https://phys.org/news/2018-04-election-voting-machines.html