The New York Times | https://nyti.ms/2kP8L3v

U.S.

Wary of Hackers, States Move to Upgrade Voting Systems

By MICHAEL WINES OCT. 14, 2017

WASHINGTON — State election officials, worried about the integrity of their voting systems, are pressing to make them more secure ahead of next year's midterm elections.

Reacting in large part to Russian efforts to hack the presidential election last year, a growing number of states are upgrading electoral databases and voting machines, and even adding cybersecurity experts to their election teams. The efforts — from both Democrats and Republicans — amount to the largest overhaul of the nation's voting infrastructure since the contested presidential election in 2000 spelled an end to punch-card ballots and voting machines with mechanical levers.

One aim is to prepare for the 2018 and 2020 elections by upgrading and securing electoral databases and voting machines that were cutting-edge before Facebook and Twitter even existed. Another is to spot and defuse attempts to depress turnout and sway election results by targeting voters with false news reports and social media posts.

West Virginia's elections team has added a cybersecurity expert from the state National Guard with a top-secret federal security clearance. Colorado and Rhode

Island will now verify election results via an advanced statistical procedure called a risk-limiting audit.

Delaware is moving its voter-registration list off the state's aging mainframe computer and preparing to replace a 21-year-old electronic voting system that does not leave a paper record of votes to be audited.

Last month, a panel of state, federal and private election experts completed a sweeping revision of guidelines for manufacturers of new voting equipment, the first major overhaul in a dozen years. While the guidelines are voluntary, they are endorsed by all but three states, so manufacturers effectively must meet the new standards to sell their equipment in most of the nation.

Of course, threats to democracy and fair voting — such as gerrymandered election districts and disinformation campaigns on Facebook and other social media platforms — go well beyond election technology. And so far state and federal funds have often failed to match the scale and urgency of the problem. But in a time of widespread skepticism about the security of American elections, ensuring people that their votes have been counted accurately has become a pressing demand.

"What's happening is a psy-ops operation," said Mac Warner, the West Virginia secretary of state. "That's what the Russians are running against us now, trying to erode confidence in our democratic process. We need to assure our citizens that we're aware of these attacks, that we have assistance to counter them, and that when they do occur, don't panic — there are resources to turn to."

In an era of bitter political divisions and elections-rules disputes, the effort to make the vote more secure is notably bipartisan and relatively rancor-free. Republicans like Mr. Warner are largely aligned with Democrats on the need to act before the next presidential election in 2020, and there is some support in both parties in Congress for helping to finance changes.

Experts have warned for years that state and local election equipment and security practices were dangerously out of date, but state and local election agencies short of cash have often lagged in updating their systems. The 2016 election, however, laid bare the seriousness of the threat.

Federal officials have said they are confident that November's election results were not tampered with. But federal intelligence and security officials were so shaken by Russian attempts to compromise the vote that the Department of Homeland Security designated election systems a critical national infrastructure, like banking and the electrical grid, that merit special protection.

The scope of the threat was underscored on Tuesday when a new report concluded not only that widely used voting systems can be breached by hackers — sometimes with almost trivial ease — but that they contain components manufactured in nations like China with a clear interest in undermining American democracy.

"It's really important not to overstate the risk. There are lots of things that can be done to make sure machines are as secure as possible," Lawrence Norden, the deputy director of the Democracy Project at the Brennan Center for Justice of the New York University School of Law. "But when you're dealing with a nation-state, you have to assume that at some point they're going to be successful in their efforts to breach things. The question then becomes resiliency and the ability to show people that you can fix things even if there is a breach."

State officials, who zealously guard their control of elections, have greeted federal efforts to address voting security with wariness. But that, too, has changed. State election directors who were blindsided and angered by the Homeland Security department's critical infrastructure designation will meet with department officials in Atlanta this month to discuss how they can share information about threats. The department also is working to give state election officials security clearances so they can view classified assessments of dangers to the election system.

The new guidelines for manufacturers of voting equipment — reduced to five pages from more than 200 — include for the first time principles as basic as a requirement that voting devices produce written records that can be verified, and that software or hardware errors cannot lead to undetectable changes in tallies. They are expected to spur the development of a new generation of cheaper and more secure equipment, said Matthew Masterson, the chairman of the federal Election Assistance Commission.

He said the shared guidelines would allow for the deployment of election software on products like tablets and iPads, which could be ready as soon as the 2020 election, rather than force 50 states to put together their own systems. “It’s going to drive innovation, hopefully save money for election officials, and allow us to test and certify equipment more efficiently,” Mr. Masterson said.

Foreign governments that regularly crack the computers of military contractors and federal agencies will not be daunted by the cyberdefenses of voter databases and electronic pollbooks. A determined adversary could compromise voting equipment at many points along the supply chain, from the factory assembler to the election software programmer to the technician who makes a repair or installs a software upgrade. And in an industry dominated by a handful of companies, malicious tinkering could have a broad impact.

“In computer security, you’re talking much more about the capabilities of local jurisdictions,” said Joseph Lorenzo Hall, the chief technology officer at the Center for Democracy and Technology in Washington. “And they vary dramatically, from L.A., which has a small army of folks, to many jurisdictions that don’t even have a full-time person for their election work. To the extent they have an ability to defend against these attacks, it’s quite limited.”

Mr. Hall said election officials need to be even more vigilant, and impose a “zero-trust networking” policy on their agencies. “Don’t assume that because something is locked in a case that it’s safe,” he said. “Assume they’re already in your system, and set up things that will catch them — honey pots, fake data stores. If anyone hits them, then you know someone’s poking around.”

For all the expressions of resolve, money remains the biggest obstacle to a complete overhaul of the system. Many jurisdictions rely on equipment bought after the 2002 Help America Vote Act, Congress’s response to the problems exposed by the 2000 presidential election, allotted nearly $4 billion for new machines and other reforms. Many of those machines are at or past the end of their service lives; Georgia conducted November’s elections on voting machines running Windows 2000, and parts of Pennsylvania relied on Windows XP.

Most states still use paper ballots that are counted by hand or by machines. But four other states besides Delaware — Louisiana, Georgia, New Jersey and South Carolina — use paperless systems that leave no audit trail, as do large swaths of Pennsylvania and some other states. Virginia scrapped thousands of paperless voting machines in 2015 after discovering that even an amateur hacker could easily and secretly change vote tallies.

A number of states and jurisdictions are replacing old equipment, and Los Angeles County — with 5.3 million registered voters, the nation's largest election district — has designed an election system from scratch, and is asking manufacturers to bid on supplying it.

Bipartisan legislation in both the House and Senate would provide a modest amount of federal money for new machines. But prospects for passage are uncertain, and many states are unable or unwilling to fill the breach.

The South Carolina Election Commission estimates that it could cost $40 million to replace the state's antiquated voting equipment with machines that used auditable paper ballots. So far the State Legislature has come up with $1 million, said Chris Whitmire, a spokesman for the commission.

"We're using the same equipment we've used since 2004," he said. "If $40 million dropped into our hands today, we'd have a paper ballot trail, too."

But even states that cannot afford more secure machines are taking steps to harden their election systems and bolster public confidence in the vote. South Carolina has accepted an offer of free "cyberhygiene" scans of its system by Homeland Security experts. Colorado is upgrading its voting equipment, but it has also begun to receive Homeland Security screenings, added national guard security experts to its election team and tacked a basic security measure onto its voter-registration database: two-step authentication for anyone seeking to log into the system.

State election officials are now in regular contact with federal security and intelligence agencies about threats to the vote, said Trevor Timmons, the chief information officer for Wayne W. Williams, the Colorado secretary of state.

“I’ve spent more time talking to three-letter agencies in the last year than I have in my entire career,” he said.

A version of this article appears in print on October 15, 2017, on Page A1 of the New York edition with the headline: Fearing Hackers, States Upgrade Voting Systems.
