WESTCHESTER COUNTY BOARD OF LEGISLATORS

Voice of the People of Westchester County for over 300 years

Benjamin Boykin II
Chairman of the Board
Legislator, 5th District

MEMORANDUM

FROM: Ben Boykin, Chairman of the Board, Legislator – 5th District

DATE: August 2, 2019

RE: New York Times article 7-26-19 - States Rush to Make Voting Systems More Secure as New Threats Emerge

Please add the attached article to the September 16th Agenda for referral to the proper committees. I suggest it be forwarded to the following committee:

- Public Works
- Budget & Appropriations

States Rush to Make Voting Systems More Secure as New Threats Emerge

A voter in Little Mountain, S.C., in 2016. South Carolina’s State Election Commission said this month that it would introduce a paper-based voting system in January.CreditCreditTravis Dove for The New York Times

By David E. Sanger, Reid J. Epstein and Michael Wines
July 26, 2019

Amid growing warnings about the security of American voting systems, many states are rushing to address vulnerabilities exposed by the 2016 election, even as intelligence officials worry they are fighting the last battle and are not sufficiently focused on a new generation of threats headed into 2020.

Delaware has replaced its voting machines to assure paper backup that would provide a record in case of a breach. South Carolina’s State Election Commission said this month that it would introduce a paper-based voting system in January and planned to “build additional layers of security designed to harden the new system.”

Yet Florida, home of the United States’ best-known presidential balloting problems, like hanging chads in 2000 and still mysterious Russian activity in 2016, once again seems far behind.

And the fear among American intelligence officials is that the federal government and the 50 states may be making the classic mistake of believing their adversaries will use the same techniques again.

“No one expects the Russians will use their old playbook” in the next election, said Suzanne Spaulding, who oversaw election security at the Department of Homeland Security during the Obama administration and is now looking at how Russia is expanding its targets to undermine confidence in the American judicial system.

Other officials point to evidence that Iran, having seen how cheap and easy it is to create election-year chaos in a Western democracy, is already experimenting with the possibilities.

So while the states are thinking about how to ensure every voter can confirm their selections on paper, and in the best case track an encrypted ballot to make sure it is counted, federal officials are war-gaming emerging risks.

The recent ransomware attacks on city governments in Atlanta and Baltimore set off alarm bells among federal officials.

Those attacks, in which online intruders locked up data in certain computer systems, led officials to consider what would happen if skilled hackers, domestic or foreign, locked up a state's voter registration system just before Election Day. Unless state officials were ready with a backup system, or reams of printouts, it could create substantial problems in determining whether all people casting ballots are registered and voting only once.

Several agencies are examining what would happen if hackers turned off the power in contested districts, throwing polling places into the darkness, and with that, the integrity of the vote.

"It wouldn't have to be a long outage" to create the perception that some votes might never be counted, said one official involved in the examination. At the National Security Agency, where a new Cybersecurity Directorate is about to be formed to coordinate defensive and offensive actions, there are new worries that Russian hackers are learning to operate from networks based in the United States — where they know the agency cannot legally investigate.

Less than 16 months from the next Election Day, the picture of American preparedness is mixed. The report issued Thursday by the Senate Intelligence Committee found that "some states were highly focused on building a culture of cybersecurity; others were severely underresourced and relying on part-time help."

Federal officials say they are particularly worried about states like New Jersey, where only three counties are making the first experiments that create a paper trail for balloting. Pennsylvania and Texas also remain major concerns, the officials said.

And despite a flurry of activity across the federal government, coordination is a major challenge — chiefly because President Trump, who has only episodically acknowledged the Russian interference in 2016, reacts badly whenever aides bring up the topic, which he interprets as questioning the legitimacy of his election.

He has never overseen detailed meetings about hardening the American system, and he undermined a White House briefing for reporters about actions it was taking when he joked with President Vladimir V. Putin of Russia, mockingly warning him not to interfere in elections again. Because the administration eliminated the post of White House cybersecurity coordinator last year, interagency meetings on the issue are often held elsewhere, or are convened by House and Senate oversight committees.

Figuring out where to start is not hard. There are a flurry of studies and reports, including the National Academies of Sciences, Engineering and Medicine, Harvard's "Defending Digital Democracy" program that trains campaign workers and state officials, and a new Microsoft program, Election Guard, that the company is providing free to states and election-machine manufacturers so that voters can track their ballots from casting to counting.

Most echo the same advice: Make sure systems have "tamper alarms" that alert officials to intrusions, employ the same kind of two-factor authentication methods for passwords that millions of Americans use for their bank accounts, and conduct regular audits to look for irregularities.

“Despite what you hear from Trump himself, the Department of Homeland Security is very focused on this threat and I feel confident that sufficient resources at that level are being dedicated to addressing it,” said Arizona’s secretary of state, Katie Hobbs, a Democrat.

She added, “If any elections official tells you they are not concerned about this, they are not doing their jobs.”

But money is scarce. Much of the $380 million that Congress allocated two years ago has been spent and Senator Mitch McConnell, Republican of Kentucky, blocked a Democratic effort on Thursday to provide more money to the states for election security.

Many localities say they do not have the funds to spend on gear they will use once a year, at most. In Texas, 106 of its 254 counties have bought new voting equipment since the 2016 elections, said Stephen Chang, the communications director for the Texas secretary of state’s office.

Mr. Chang said the majority of Texas voters will vote on “paper-based voting systems” by the 2020 general election, with counties that include Dallas, Fort Worth and San Antonio already transitioning to voting on paper. But that leaves a vast population relying on electronic voting systems that cannot be properly audited.

New Jersey is perhaps the farthest behind. Its polling places do not use voting machines that create an auditable paper trail, but three of the state’s 21 counties have conducted pilot programs using such machines. Three have bought them, according to Alicia D’Alessandro, a spokeswoman for New Jersey’s secretary of state, Tahesha Way.

Since the 2016 election, she said, the state homeland security office has designated a security expert to monitor voter registration databases and other election infrastructure, and Ms. Way’s office works with federal experts and election officials in other states to detect and repel threats.

The Senate report was less concerned about election machines, which are off-line and usually hard to hack from afar, than the voter registration systems, which are online. Elections officials across the country said there were innumerable attempts from hackers abroad and inside the United States to breach their voter rolls and elections data — most of them amateurish, some skilled. The vast majority of them are turned back with basic firewall technology.

Russian online intruders twice tried in 2016 to infiltrate Wisconsin’s computer systems, and the state’s systems are “scanned” millions of time, according to the Wisconsin Elections Commission. The state said there was “no evidence that Wisconsin’s election systems have ever been compromised.”

In Ohio, Secretary of State Frank LaRose directed county elections officials in June to install intrusion detection devices on computer networks for boards of elections and their vendors. That is akin to a basic car alarm, yet many systems have none.

Kentucky has often been criticized for failing to secure its voter-registration data. A 2018 investigation by ProPublica found that the state’s online voter registration system used an outdated protocol that left its data open to manipulation and did not block access by internet protocol addresses registered in foreign nations — a basic safety measure. The state said the online server in question was separate from the main voter database.

Louisiana election officials said they would not have a paper ballot system in place until after the 2020 election. Tyler Brey, the press secretary for Louisiana’s secretary of state, R. Kyle Ardoin, said that Mr. Ardoin’s office was ordering new voting machines and that they would not be operable in the state until at least 2021.

Mr. Brey also said state officials had been preparing for various contingencies like deflecting phishing emails.