The Feds Want To Stop Election Hackers, But States And Voters Are Wary

Steven Melendez

October 4, 2016

After hackers said to be linked to Russia stole data from voter registration systems in Arizona and Illinois earlier this year, the federal Department of Homeland Security offered digital security assistance to state and local election officials around the country.

In August, Homeland Security Secretary Jeh Johnson also raised the possibility of declaring some election-related systems to be "critical infrastructure." Under an executive order issued by President Barack Obama in 2013, that would likely mean federal officials would work with local authorities to coordinate voluntary security standards for those systems.

So far, 21 states have reached to DHS for assistance, Johnson said in a statement released on Saturday. But some state officials and activists have expressed fears that even voluntary assistance programs and especially a future critical infrastructure designation could lead to unprecedented level of federal involvement in elections.

"This suggestion caught many elections officials by surprise and rightfully so," Georgia Secretary of State Brian Kemp told a Congressional subcommittee last week. "The administration of elections is a state responsibility. Moreover, this suggestion came from an agency completely unfamiliar with the elections space and raised the level of public concern beyond what was necessary."

Kemp and other state and local officials have expressed concern about federal officials setting standards about how elections are conducted. While Johnson has emphasized that taking assistance from DHS is voluntary, skeptics worry federal officials will ultimately set legal or de facto standards that states will feel compelled to follow.

"It's one thing if they want to make recommendations to the states on how to improve cybersecurity," says Hans von Spakovsky, a manager at the conservative Heritage Foundation's Election Law Reform Initiative and a former member of the Federal Election Commission. "It's quite another if they want to come in and dictate what states do, because that then brings the federal government into trying to run election administration, which is not a role given to the federal government. That's been done by the states throughout our entire history."

Skeptics worry federal officials will ultimately set legal or de facto standards that states will feel compelled to follow.

In terms of digital threats, security researchers have warned for years that some electronic voting machines are disturbingly easy to tamper with. Just last week, Princeton University computer science professor Andrew Appel again urged Congress to help phase out touchscreen machines that don't generate a backup paper record of ballots cast, making them especially vulnerable to tampering or accidental data loss.

But experts say it's unlikely that hackers could exploit bugs in voting machines to reliably sway a national election. Since the machines aren't internet-connected, that would require hackers surreptitiously getting physical access to large numbers of individual machines at precincts scattered across the country.

"What is more realistic is a smaller number of confirmed intrusions that maybe again aren't enough to change the outcome on the national level but are enough to undermine people's confidence in the results," says Julian Sanchez, a senior fellow at the libertarian-leaning Cato Institute who studies cybersecurity. "I think that's a more likely scenario."

Attackers looking to undermine confidence could steer clear of voting machines altogether, and focus their attacks on internet-enabled systems. That could mean entering false names into online registration systems or tampering with them to cause check-in delays and long lines at polling places, according to Joe Kiniry, CEO and chief scientist ofFree & Fair, a company that develops open-source voting software.

"You don't even have to touch the voting machines," he says. "You just mess up the database."

Or, Kiniry says, attackers could interfere with online systems that publicize results after ballots are cast: Even if they can't actually change the official tallies and the right numbers ultimately make it to the public, they could still sow doubt among voters about the results.

In theory, DHS should be able to help local election authorities with limited tech resources to keep their systems more secure, providing services like digital vulnerability scans to agencies that request them and helping share information about known risks.

"They do offer that: You can contact DHS if you're an elections jurisdiction and they'll come and help you," says Pamela Smith, president of Verified Voting, which advocates for transparency and verifiability in election technology. "It's important to do vulnerability scanning or testing. If you haven't done anything like that or you're not even sure what that means because you didn't used to have know those things to be an election official, then [they're] here for you."

Even if hackers can't actually change the official tallies, they could still sow doubt among voters about election results.

Verified Voting advocated for declaring voting equipment to be critical infrastructure back in 2013, when federal agencies sought public input on implementing Obama's cybersecurity order. The designation could help marshal more resources to protect elections, at a time when some local authorities lack the tech expertise needed to implement their own cybersecurity programs.

In a 2013 filing, Smith and others from the group wrote, "Given that large corporate entities, banks, government institutions, and others have experienced security breaches and sometimes sustained significant losses despite being well-resourced, it is unlikely that an under-resourced elections office, if targeted, would be able to evade similar breaches or even detect them in a timely manner."

But with trust in the federal government at near-historic lows, increased DHS involvement might not be the best way to address worries about vote tampering and legitimacy, Sanchez notes. And formally classifying election technology to be critical infrastructure,alongside the nation's dams, nuclear facilities, food supply, and other sectors, doesn't necessarily mean it'll be kept free from hackers. "Lots of things are designated critical infrastructure," Sanchez says. "It doesn't prevent those companies from getting hacked from time to time."