www-nbcnews-com.cdn.ampproject.org

'Online and vulnerable': Experts find nearly three dozen U.S. voting systems connected to internet

By Kevin Monahan, Cynthia McFadden and Didi Martinez

9 - 12 minutes

It was an assurance designed to bolster public confidence in the way America votes: Voting machines "are not connected to the internet."

Then Acting Undersecretary for Cybersecurity and Communications at the Department of Homeland Security Jeanette Manfra said those words in 2017, testifying before Congress while she was responsible for the security of the nation's voting system.

So many government officials like Manfra have said the same thing over the last few years that it is commonly accepted as gospel by most Americans. Behind it is the notion that if voting systems are not online, hackers will have a harder time compromising them.

But that is an overstatement, according to a team of 10 independent cybersecurity experts who specialize in voting systems and elections. While the voting machines themselves are not designed to be online, the larger voting systems in many states end up there, putting the voting process at risk.

That team of election security experts say that last summer, they discovered some systems are, in fact, online.

"We found over 35 [voting systems] had been left online and we're still continuing to find more," Kevin Skoglund, a senior technical advisor at the election security advocacy group National Election Defense Coalition, told NBC News.
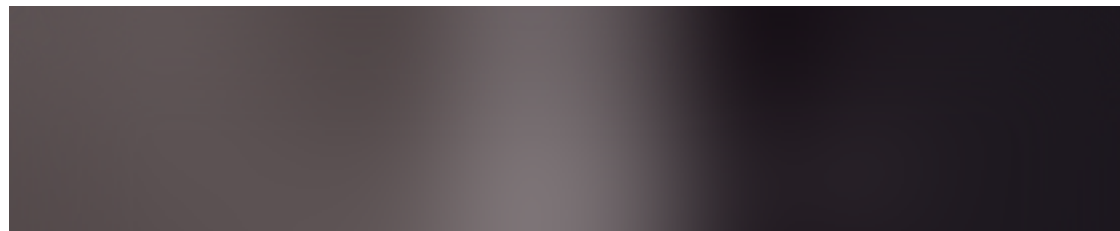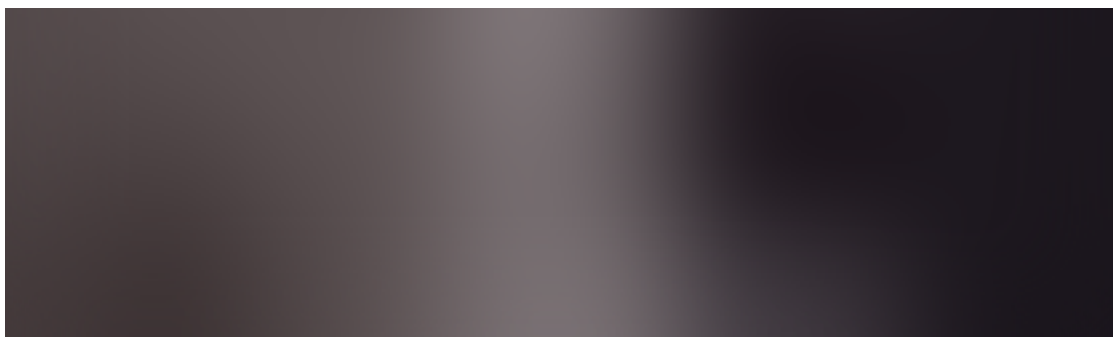
Kevin Skoglund, senior technical advisor at the National Election Defense Coalition.NBC News

"We kept hearing from election officials that voting machines were never on the internet," he said. "And we knew that wasn't true. And so we set out to try and find the voting machines to see if we could find them on the internet, and especially the back-end systems that voting machines in the precinct were connecting to to report their results."

Skoglund and his team developed a tool that scoured the internet to see if the central computers that program voting machines and run the entire election process at the precinct level were online. Once they had identified such systems, they contacted the relevant election officials and also provided the information to reporter Kim Zetter, who published the findings in Vice's [Motherboard](#) in August.

The three largest voting manufacturing companies — Election Systems &Software, Dominion Voting Systems and Hart InterCivic — have acknowledged they all put modems in some of their tabulators and scanners. The reason? So that unofficial election results can more quickly be relayed to the public. Those modems connect to cell phone networks, which, in turn, are connected to the internet.

The largest manufacturer of voting machines, ES&S, told NBC News their systems are protected by firewalls and are not on the "public internet." But both Skoglund and Andrew Appel, a Princeton computer science professor and expert on elections, said such firewalls can and have been breached.

"AT&T and Verizon and so on try and protect as best they can the security of their phone network from the rest of the internet, but it's still part of the internet," Appel explained. "There can still be security holes that allow hackers to get into the phone network."

The 35 systems Skoglund's team found represent a fraction of total voting

systems nationwide, though he believes they only captured a portion of the systems that are or have been online. Earlier this week, Skoglund showed NBC three election systems were still online even after officials had been told they were vulnerable.

For election systems to be online, even momentarily, presents a serious problem, according to Appel.

"Once a hacker starts talking to the voting machine through the modem, the hacker cannot just change these unofficial election results, they can hack the software in the voting machine and make it cheat in future elections," he said.

The National Institute of Standards and Technology, which provides cybersecurity frameworks for state and local governments and other organizations, recommends that voting systems should not have wireless network connections.

Skoglund said that they identified only one company among the systems they detected on line, ES&S. ES&S confirmed they had sold scanners with wireless modems to at least 11 states. Skoglund says those include the battleground states of Michigan, Wisconsin and Florida.

While the company's website states that "zero" of its voting tabulators are connected to the internet, ES&S told NBC News 14,000 of their DS200 tabulators with online modems are currently in use around the country.

NBC News asked the two other major manufacturers how many of their tabulators with modems were currently in use. Hart said that it has approximately 1,600 such tabulators in use in 11 counties in Michigan. Dominion did not respond to numerous requests from NBC News for their sales numbers.

'Vulnerable to hacking'

With the 2020 presidential election only ten months away, Appel and Skoglund believe all modems can and should be removed from election systems.

"Modems in voting machines are a bad idea," said Appel. "Those modems that ES&S [and other manufacturers] are putting in their voting machines are network connections, and that leaves them vulnerable to hacking by anybody who can connect to that network."

Recommended

The state of Michigan is currently grappling with this issue. Since the 2016 election, Michigan authorized $82 million dollars to upgrade its election systems. Some of that money was spent on tabulators with wireless modems. But now, some state officials worry that the machines may pose a security risk and are pushing to have the modems removed.

Others are not so sure, and the state has set up an advisory committee.

Jake Rollow, director of communications for the Michigan Department of State, said in a statement to NBC News, "Even though the results are unofficial, if these unofficial results were disrupted or manipulated, it could still cause confusion on Election Day."

"The department will consider the advisory commission's recommendations to improve the security of the process," Rollow continued. "The specific steps taken would depend on the recommendation and the timeline required to make changes effectively."

Last fall, when ES&S gave NBC News an exclusive tour at its headquarters in Omaha, Neb., Chief Executive Officer Tom Burt defended using modems when asked about the Sprint and Verizon modems seen in ES&S's testing area.

"There's a small percentage of jurisdictions in the country -- a lot of them are in Florida -- who have decided they want to modem unofficial results to the election office," he said. "Generally speaking, the media in those locations are kinda clamoring to get unofficial results as quickly as possible."

When asked if the desire for speed was at odds with accuracy and security, Burt said, "it's not my place to judge that."

NBC News reached out to the Department of Homeland Security, which declined to comment on the topic of modem security in voting machine tabulators and scanners.

'Inviting trouble'

Critics also argue ES&S has mislead jurisdictions into thinking their DS200 tabulators with modems are certified by the U.S. Election Assistance Commission, a claim they say is grounds for an investigation.

In a letter obtained by NBC News sent to the EAC on Tuesday, the nonprofit public interest group Free Speech for People and the National Election Defense Coalition asked the agency to look into whether ES&S violated agency regulations by implying that DS200 voting machines with modems are EAC certified.

"ES&S has repeatedly advertised its DS200 with internal modem — a critical component to ES&S's voting systems — as being EAC certified when, in fact, it is not," the letter said. "We therefore again respectfully request that EAC investigate and take action to correct this serious issue."

"Once you add that modem, you are de-certifying it," Skoglund said. "It is no longer federally certified. And I don't know that all these jurisdictions are aware of that because ES&S is advertising otherwise."

But Skogland points to some good news. He believes there is time to make real change before the 2020 election.

"We should be unplugging all of these machines from the internet," Skoglund said. "Even for elections nights."

Appel agreed. "We can not make our computers perfectly secure," he said. "What we should do is remove all of the unnecessary, hackable pathways, such as modems. We should not connect our voting machines directly to the computer networks. That is just inviting trouble."

These two tech experts also agree on the path forward, saying they are comforted by the fact that most Americans will vote this year on hand-marked paper ballots which are counted by machine and can be recounted by hand if the situation warrants.

The machines America votes on seem to be capturing the interest of some in Congress. The House Committee on Administration held a congressional hearing yesterday which was the first time the heads of the three major vendors, representing at least 80 percent of U.S. voting machines, appeared together for questioning. While lawmakers questioned them about foreign influence in their supply chains and whether they would comply with more federal reporting requirements, the presence of modems in some of their tabulators was mentioned but not pursued.

EDITOR'S NOTE (Feb. 7, 2020, 11:15 p.m.): A previous version of this article stated that Kevin Skoglund and his team had found election

systems using ES&S scanners with wireless modems connected to the internet in 11 states and the District of Columbia. The coalition says it is no longer certain that the number of states is correct, so the figure has been removed from the article.
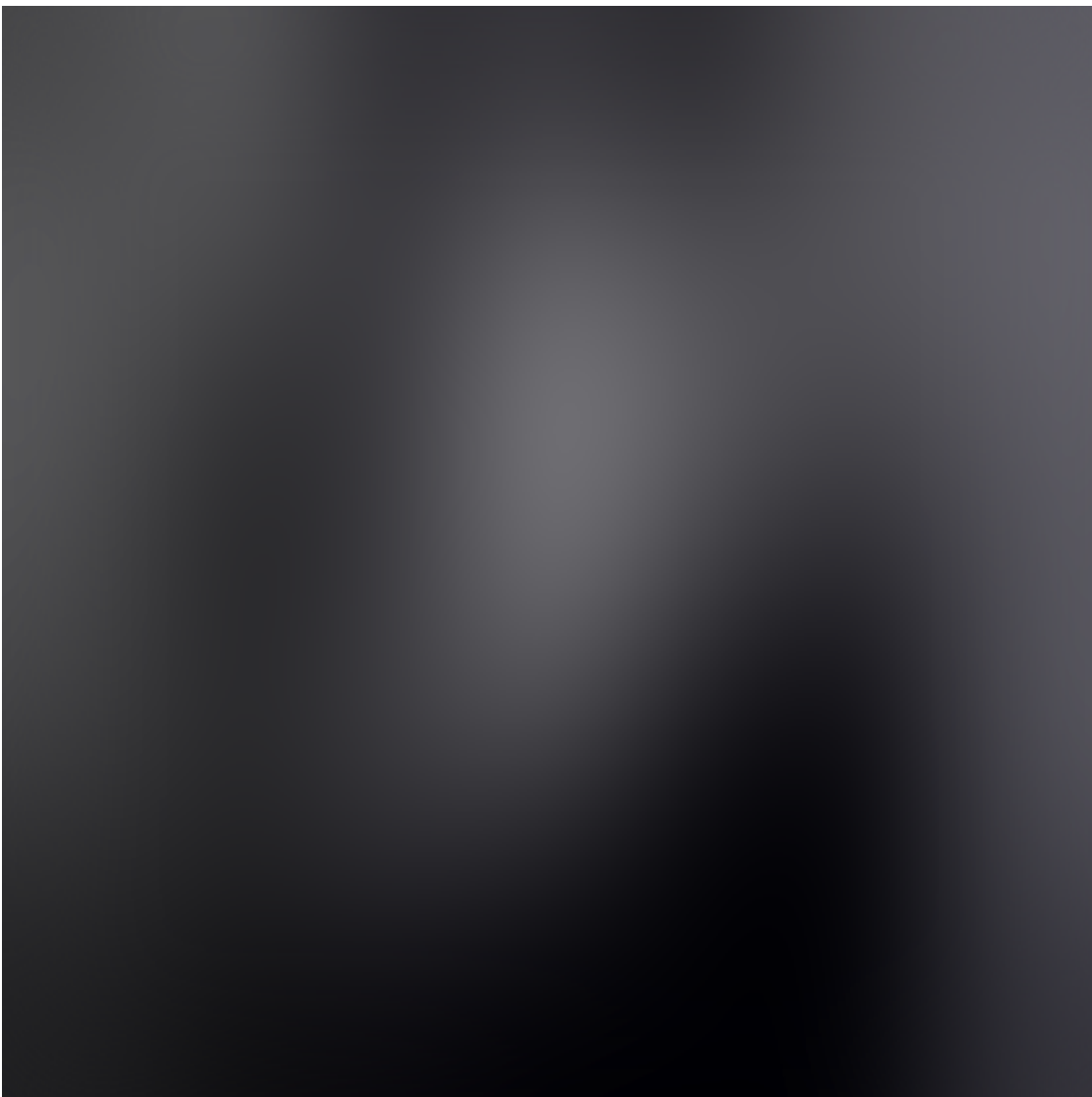
Kevin Monahan

Kevin Monahan is a producer for the NBC News Investigative Unit.
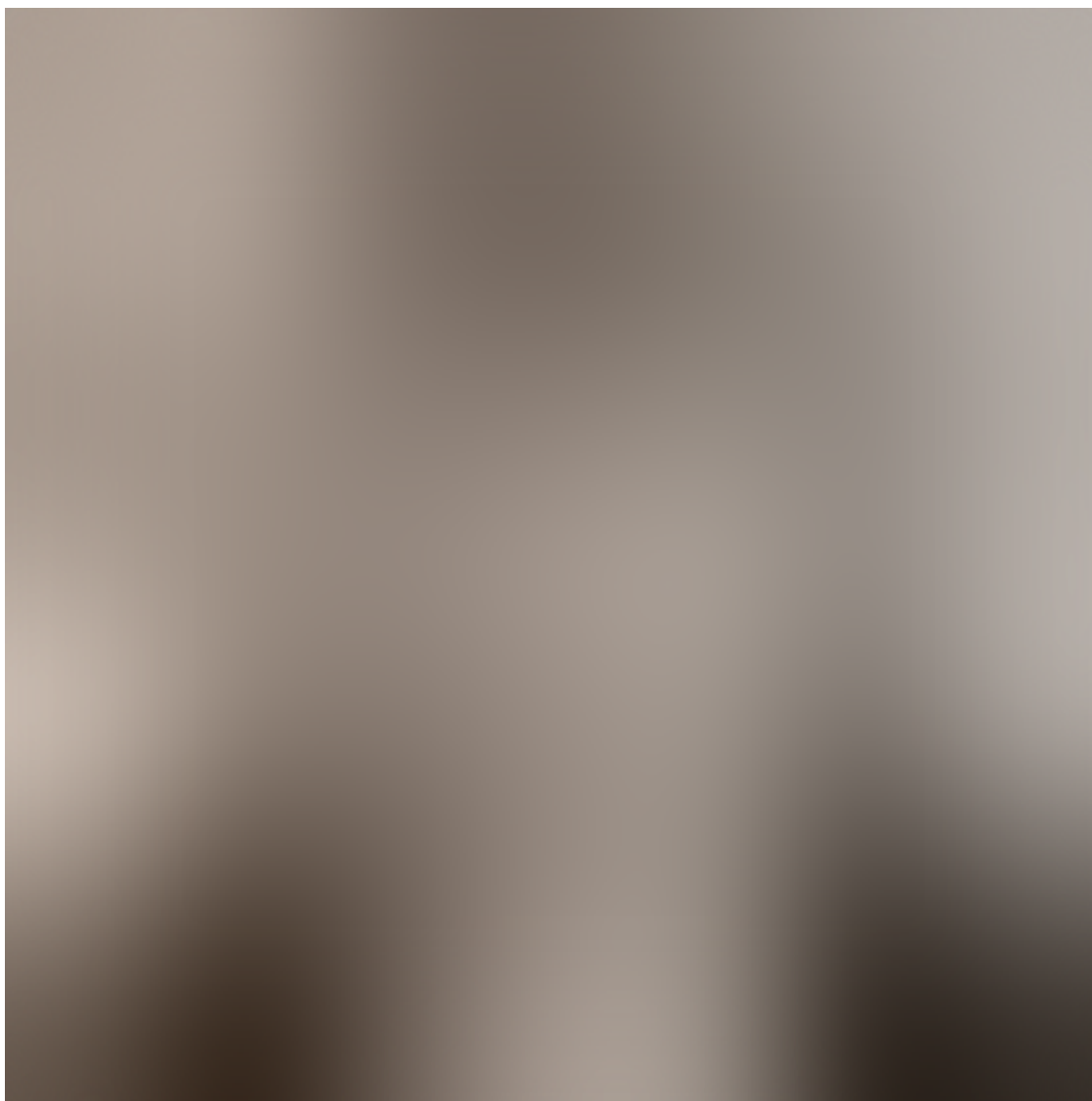
Cynthia McFadden

Cynthia McFadden is the senior legal and investigative correspondent for NBC News.

Didi Martinez

Didi Martinez is an associate producer with the NBC News Investigative Unit.