Public, election officials may be kept in the dark on hacks

October 21 2019, by Colleen Long and Christina A. Cassidy

In this Nov. 1, 2017, file photo, traffic along Pennsylvania Avenue in Washington streaks past the Federal Bureau of Investigation headquarters building. Federal policies emphasizing privacy over disclosure and a complex web of government officials could undermine improvements in communication and coordination if another cyberattack on U.S. election systems occurs. (AP Photo/J. David Ake, File)

If the FBI discovers that foreign hackers have infiltrated the networks of your county election office, you may not find out about it until after voting is over. And your governor and other state officials may be kept in the dark, too.

There's no federal law compelling state and local governments to share information when an electoral system is hacked. And a federal policy keeps details secret by shielding the identity of all cyber victims regardless of whether election systems are involved.

Election officials are in a difficult spot: If someone else's voting system is targeted, they want to know exactly what happened so they can protect their own system. Yet when their own systems are targeted, they may be cautious about disclosing details. They must balance the need for openness with worries over undermining any criminal investigation. And they want to avoid chaos or confusion, the kind of disruption that hackers want.

The secrecy surrounding foreign hacks is not a hypothetical issue. The public still doesn't know which Florida counties were breached by Russian agents in the 2016 election. Rick Scott, Florida's governor in 2016 and now a U.S. senator, was not told at the time and didn't learn most of the details until this year.

And the threat to electoral systems is real. Federal officials believe Russian agents in 2016 searched for vulnerabilities within election systems in all 50 states. And the nation's intelligence chiefs warn that Russia and other nations remain interested in interfering in U.S. elections.

Meanwhile, experts worry the White House hasn't highlighted the threat as President Donald Trump argues it's OK for foreign countries to provide damaging information on his political rivals, a matter now the

subject of an impeachment inquiry led by House Democrats.

In general, it's up to electoral agencies to disclose when they've been hacked. That, plus the federal policy protecting the identity of cyber victims, could mean that state election officials might not be told immediately if one of their local election offices experiences a breach. In addition, the whole situation could be considered classified as part of a federal investigation.

At least two states—Colorado and Iowa—have implemented policies to compel local officials to notify the state about suspected breaches involving election systems.

"Every American in this nation deserves to have a democracy they can believe in, and when there is not good communication on cyber incidents ... it does create a lack of confidence in the system," said Colorado Secretary of State Jena Griswold. "Luckily we have been able to work around the void of federal policy that has been leaving our nation in a precarious spot."

But Department of Homeland Security officials say privacy is needed to ensure that officials come forward and share valuable threat information, such as suspect IP addresses.

Some election officials could be hesitant about public disclosures, concerned their agencies would be portrayed in a negative light. They could opt to handle any breach alone.

That could create dangerous delays in sharing information, said Jeanette Manfra, assistant director for cybersecurity at Homeland Security's new cyber agency.

Homeland Security acts as the middleman between the intelligence

community and the states. In general, communication and coordination on election security have improved in the last two years.

"We've worked over the years to be able to declassify even more and to do it faster," Manfra said. "It's still not a perfect process."

Due to the criminal nature of cyber breaches, law enforcement officials may seek to withhold releasing certain information long after the incident. When Florida's current governor, Ron DeSantis, was briefed this year on the 2016 cyber breaches, he said he signed an agreement preventing him from identifying the affected counties.

The secrecy surrounding Florida helped spur bipartisan legislation that would compel reporting among federal, state and local officials and to voters potentially affected by a breach. Rep. Stephanie Murphy, a Florida Democrat, co-sponsor of the bill, said she believes voters are the victims, not the election office, and that not disclosing information about election-related breaches could undermine public confidence.

In June, a majority of Americans expressed at least some concern that voting systems are vulnerable to hackers, according to a poll from The Associated Press-NORC Center for Public Affairs Research.

"It's hard for me to assess if what people are doing in response is sufficient when I don't know the full scope of the problem," Murphy said. "And I think that's the same issue with voters: How can they feel comfortable or confident that this next election will be free and fair?"

Yet election officials want to ensure they have a good understanding of what happened before going public so they don't contribute to the confusion that the hackers may be trying to achieve.

Cyber intrusions are inherently complicated, taking time to understand

and contain. There is also a concern of inadvertently releasing information that could invite further compromises or undermine an investigation.

"It is important to be as transparent as possible, but as with any crime, the full details of an investigation are not discussed," said Paul Pate, Iowa's Republican secretary of state. "It's a balancing act that needs to be measured on a case-by-case basis."

In 2017, California election officials quickly disclosed the state had been notified by federal officials that its election systems were among those scanned by Russians the year before. Five days later, they had to correct the announcement after discovering the scans involved a non-election system. Secretary of State Alex Padilla, a Democrat, said it was an important lesson in making sure all the facts were there, especially considering the public is not familiar with cybersecurity terminology.

In the summer of 2016, hackers accessed Illinois' voter registration database, and officials moved fast to shut down the system and isolate the threat. State officials knew the move wouldn't go unnoticed and felt it was important to notify the public.

It became clear only later that Russian agents were involved, and the breach was part of an unprecedented campaign to interfere in U.S. elections.

Matt Dietrich, spokesman for the Illinois State Board of Elections, said it would be hard to imagine that any election office would seek to keep something like that quiet today.

"In 2016, it was a story and then it was dealt with and then it kind of went away for a year," Dietrich said. "That is not going to happen this time. It will be a national and a worldwide story. We all know this. We

all know we are going to be under the microscope."