State elections officials around the country are expressing confidence that they’re ready to protect the November 2018 vote from potential cyber threats and, if necessary, deploy new tools and communications protocols put in place since the 2016 election, which saw 21 states targeted by Russian hackers.

“Yes, we feel confident that we’re in good shape,” said Vermont Secretary of State Jim Condos. “But I will also say that cybersecurity ... is like the race without a finish line. It’s a never-ending proposition. This is the new normal. We will always be focused on cybersecurity.”

Condos was one of five dozen state and local elections officials, state legislators, executive branch staff and state technology directors from eight states who talked with CSG between early August and mid-October as part of an election cybersecurity initiative with The Democracy Fund, a Washington, D.C.-based, bipartisan foundation with the aim of improving the democratic process in the United States.

Condos believes it’s important for states to not only be ever-vigilant but adaptive as well.

“When a bad actor tried to get in yesterday and couldn’t, he’s going to try a different way today and if he can’t get in today, he’s going to try a different way tomorrow,” he said. “We have to be proactive and focus on defending our systems. We have to be able to adjust and evolve just like they will—the bad actors.”

Across the country in Washington state, there is cautious optimism as well.

“Of course, you never want to say that you’re 100 percent prepared because that’s when you get bit by the thing you didn’t plan for,” said Washington Secretary of State Kim Wyman. “But I really think that we’ve used the last six months well in terms of time and really reaching out to all of the players that we can foresee being ones that need to be (part of our) communication plans.”

Wyman said the county auditors who actually administer elections in Washington are well-prepared thanks in part to months of tabletop exercises and training with the Department of Homeland Security and the National Guard. Her team also has worked to get nearly every county in the state registered with the Elections Infrastructure Information Sharing & Analysis Center (EI-ISAC), which allows them to access threat notifications, vulnerability assessments and incident response services without requiring the secretary of state’s office to act as intermediary with the federal agencies.

Washington state is also working towards a goal of getting intrusion detection sensors, known as Albert sensors, installed on all 39 county systems, Wyman said. Reuters reported this summer that 36 states had installed the $5,000 sensors that make use of open source software at the elections infrastructure level. Overall, Reuters reported, 74 sensors have been installed in 38 local jurisdictions around the country. Only 14 of the sensors were installed nationwide prior to the 2016 election.
Washington and other states also have taken advantage of $380 million in federal dollars made available as part of the 2018 Help America Vote Act (HAVA) Election Security Fund included in the omnibus appropriations bill signed by President Donald Trump in March. Wyman’s office is using Washington’s share of those dollars to build an in-house IT support team.

But there may be another reason Washington is feeling confident it can avoid cyber threats that could impact other states. RaShelle Davis, a senior policy advisor to Gov. Jay Inslee, noted that Washington is one of three completely vote-by-mail states—Colorado and Oregon are the others. That means they have records of every ballot cast and they retain those records. If there is ever a question about the validity of the count, the vote tabulation or if there’s a need for an audit or recount, they have the ballots, Davis said.

“What we’re seeing is some (other states)—the five states that have touchscreen voting, for example—I think they’re going to have a little tougher road,” said Wyman. “On the national level there is some chatter about how the touchscreen devices are not secure and they can be hacked and there’s no paper trail. … But I think we’re well positioned because of the paper ballot parts of vote-by-mail and just the system’s accessibility across the board.”

Assistant Secretary of State Mark Neary said that doesn’t mean Washington’s election systems are completely invulnerable to attack, however.

“Where I think our risk is is our voter registration database,” he said. “That’s where we actually keep all of the detailed information about how we get those mailed ballots to individuals who are registered to vote here in Washington state.”

Condos, the Vermont secretary of state, noted that of the 21 states that were targeted by hackers in 2016, just one—Illinois—was actually breached.

“It was their voter registration database,” he said.

But Condos is also quick to point out something else about 2016.

“What the press doesn’t focus on or doesn’t mention much is that there were 20 states that actually defended and defended well and did their job,” Condos said. “That’s kudos to the states. We actually did our work. We did what we were supposed to do.”

Indeed, Secretary Wyman in Washington said, one could argue the biggest lesson from 2016 was not necessarily what happened but what elections officials prevented from happening.

“I think it renewed my confidence in our safeguards and our controls that we have in place because my team—the IT folks and the elections folks—started noticing the (cyber) activity very early,” she said. “They were on it before we ever involved Homeland Security or the FBI or any of those entities. So I think our lesson learned was just continue on the track we are with our controls and our safeguards and probably beefing them up and really working with the counties … that just don’t have the depth of resources that they need to have to be successful and really trying to shift our emphasis more on giving them the tools and giving them access to training and things that will help them take their system to that level of security as well.”

Others are similarly concerned that the underfunded and under-resourced counties and other local jurisdictions that conduct elections around the country could prove to be the weakest links in the efforts to protect election systems and processes.

“I think (the counties are) probably our biggest concern,” said Kim Strach, executive director of the
North Carolina State Board of Elections. “What we’re doing is we’re trying to give them guidance on everything that we can think of they need to do to harden their systems and make sure they’re prepared. ...That’s going to be a daily battle because the resources in the counties are very different from county to county.”

For many elections officials around the country that battle will continue well past Nov. 6.

“We don’t stop today and say ‘okay, we’ve got this, we’re secure,’” said Washington Director of Elections Lori Augino. “You have to continue to identify the threat, analyze those threats and identify what new ways they might be looking at a threat vector and how can we adapt to protect to those. So yeah, definitely no finish line and it’s something that we will continue to fight every single day.”

CSG will release the CSG Elections Cybersecurity Report for state and local officials at the CSG 2018 National Conference Dec. 7 in Northern Kentucky-Greater Cincinnati.

By:
Friday, October 26, 2018 at 10:23 AM
Tags:

© 2016 The Council of State Governments. All Rights Reserved.

Source URL: http://knowledgecenter.csg.org/kc/content/state-elections-officials-say-theyre-ready-deal-cyber-threats

Links