Denver Post

Colorado elections system may have been scanned for weaknesses by Russians, federal officials tell Secretary of State's Office

Colorado election officials feel strongly that their system was not compromised

Seth Perlman, Associated Press file
In this March 15, 2016, file photo, people line up to vote in the primary at a precinct in Bradfordton, Il. State election officials from across the U.S. are gathering this weekend in Indianapolis amid an uproar over a White House commission investigating allegations of voter fraud and heightened concern about Russian attempts to interfere with last fall's election.

By Jesse Paul | jpaul@denverpost.com and John Frank | jfrank@denverpost.com | The Denver Post

PUBLISHED: September 22, 2017 at 3:21 pm | UPDATED: September 22, 2017 at 3:51 pm

Colorado may have been among nearly two dozen states whose election systems were scanned for weaknesses by Russian-linked actors leading up to the 2016 election, the Colorado Secretary of State's Office said Friday, though officials feel strongly that there was no breach.

Trevor Timmons, chief information officer for the Secretary of State's Office, says information that a Department of Homeland Security agent passed along Friday didn't explicitly mention Russia but that it otherwise mirrored a warning federal officials gave Congress over the summer that did.

"Colorado is considered by DHS to be on that list of 21 states that were impacted. He said that Colorado systems were scanned," Timmons said. "He said there's no evidence of penetration or compromise but scanned."

Colorado was one of 21 21 states DHS contacted Friday to say their election systems were targeted by hackers last year, mostly without success. By contrast, DHS told Congress over the summer that 21 states' elections systems were targeted by hackers linked to the Russian government.

"We've reached out to local DHS resources as well as federal DHS resources to get more detail on what exactly they are talking about," Timmons said. "Are they attributing the scanning that they saw or that they are aware of to Russian-based actors or Russian-affiliated actors? I do not know the answer to that."

The Colorado Secretary of State's Office says it is routinely scanned by potential bad actors and that it has a robust security system to block any kind of infiltration.

Rich Schliep, chief information security officer for the secretary of state, said it's possible that DHS found out about the suspicious scanning linked to the 21 states because of data state officials turned over to federal investigators.

"There is a strong possibility that the reason we are on the list is we notified them in the first place," Schliep said, adding that it shows the office is ahead of the ball.

In Colorado, DHS told state officials, the scanning likely happened in September and October.

The Secretary of State's Office took in-depth steps on Election Day in November to ensure that the state's voter systems were safe. That included having the contest monitored by two teams of three cybersecurity experts from the Colorado National Guard and a local FBI special agent who focuses on election issues.

The Colorado Secretary of State's Office said in June that it does not think it was targeted by Russian-backed hackers.

Officials say they block anywhere from 10 to 15 IP addresses daily that it finds are linked to suspicious behavior toward the office's systems.

“According to Homeland Security, we were not attacked, probed, breached, infiltrated or penetrated,” Secretary of State Wayne Williams said in a written statement. “This was a scan and many computer systems are regularly scanned. It happens hundreds if not thousands of times per day. That’s why we continue to be vigilant and monitor our systems around the clock.”

Earlier this week, the state’s budget writers approved diverting money from an unused election account to spend an additional $1.2 million to upgrade the office’s cybersecurity measures for its voter registration system and business database.

The new funding, approved unanimously by the Joint Budget Committee, will cover the cost to add a centralized risk management platform to protect and monitor who accesses the state’s voter registration system, as well as upgrade the existing firewalls to allow real-time threat intelligence.

Other new cybersecurity measures will help minimize the potential impact of hackers and add masking tools to create multiple layers of defense for voter registration and elections data.

In an interview earlier this week, Williams said the current system was secure but the office “continues to work to harden the process.”