US official: Difficult to alter US elections through hacking

September 14 2016, by Eric Tucker

In this Feb. 13, 2015 file photo, Assistant to the President for Homeland Security and Counterterrorism Lisa Monaco speaks at the White House Summit on Cybersecurity and Consumer Protection in Stanford, Calif. Monaco said Wednesday, Sept. 14, 2016, that it would be very hard for someone to hack into America's voting systems in a way that could alter an election outcome. Monaco, speaking at an event commemorating the 10-year anniversary of the Justice Department's national security division, said election systems by and large are not hooked up to the Internet and are diffusely operated by state and local governments. (AP Photo/Jeff Chiu, File)

President Barack Obama's homeland security adviser said Wednesday that it would be very hard for someone to hack into America's voting systems in a way that could alter an election outcome.

Lisa Monaco, speaking at an event commemorating the 10-year anniversary of the Justice Department's national security division, said election systems by and large are not hooked up to the Internet and are diffusely operated by state and local governments.

"That makes it extremely disparate, extremely diffuse and, as a consequence, extremely difficult to have an effect across the board that would result in a change in results," Monaco said during a question-and-answer session.

The bigger worry, she said, involves efforts to sow "concern or confusion" about the resilience of the system.

To help counter that, the federal government is pushing out to states a set of tools, such as the ability to scan for vulnerabilities and quickly patch them, and best practices that they should apply—including encrypting their voter registration data, she said.

The comments come amid ongoing concern about the ability by hackers from Russia or other nations to breach voting systems. The FBI last month warned state elections officials to boost their election security in light of evidence that hackers targeted related data systems in at least two states, Illinois and Arizona.

"The efforts of malicious actors to intrude upon voter registration databases and other elements of our critical infrastructure, as well as our voting infrastructure, are of concern," she said.

A Homeland Security Department official who is very involved in

efforts to secure local elections but wasn't authorized to speak publicly said the department was not looking at designating election systems critical infrastructure now because of how little time there is until the elections. The official said the focus has been on providing information to states on technical assistance the department can provide to secure their systems as well as existing vulnerability reports it sends out.

A Presidential Policy Directive released in 2013 details 16 sectors that are considered critical infrastructure, including energy, financial services, healthcare, transportation, food and agriculture, and communications. The designation places responsibilities on the Homeland Security Department's secretary to identify and prioritize critical infrastructure, considering physical as well as cyber threats.

The official said the department was looking at designating election systems as critical infrastructure in the future.

Monaco's remarks echoed those of FBI Director James Comey, who told an audience last week that "the vote counting in this country tends to be kind of clunky, which is a blessing because it makes it harder for hackers to infiltrate."

Besides hacks of election systems, the federal government is continuing to investigate a hack of the Democratic National Committee and the subsequent disclosure of internal DNC emails on WikiLeaks. The U.S. hasn't formally blamed Russia for the hack of Democratic National Committee emails over the summer, but the party has, and the White House has pointed publicly to outside investigators who have determined Russia is to blame.

Those investigators have been less clear about whether Russia was also responsible for disseminating those emails through the website WikiLeaks. Determining Russia's involvement in the public disclosure of

the emails is seen as a prerequisite to any sanctions the U.S. might levy on Russia in response to the hack.

Monaco on Wednesday replied "stay tuned" when asked whether the U.S. might respond. The Obama administration in the last two and a half years has publicly accused Chinese hackers in breaches of American corporations, North Korea in a punishing hack of Sony Pictures Entertainment, and Iranian hackers in digital breaches of banks and a small dam outside New York City.

Comey, appearing later at the same event, said not all tools that the government can respond with are visible to the public.

"Just because you can't see something doesn't mean your government's not doing something," he said.

Citation: US official: Difficult to alter US elections through hacking (2016, September 14) retrieved 26 April 2024 from https://phys.org/news/2016-09-difficult-elections-hacking.html