

[Click here to receive FCW magazine for FREE!](#)



Elections

Former DHS chief feared catastrophic attack on election systems

By Mark Rockwell Sep 28, 2017

Russian interference in U.S. institutions reaches further than the interference in the election infrastructure in 2016 and requires a strong strategy to counter a sustained effort by that country to undermine the integrity of the vote, former DHS leaders told a congressional task force.

Russian probes and alleged attempted hacks of state election systems in the last election are "a wake up call" for upcoming state and congressional elections in 2018, former Secretary of Homeland Security Jeh Johnson told House Democrats on the Election Security Task Force in a Sept. 28 public meeting.

House Democrats created the Election Security Task Force in June to study ways to keep Russian interference out of 2018 elections.

While Johnson told the panel that he found no evidence that Russian probes of state systems, including voter registration systems, altered ballots or election results, he said those efforts "exposed cyber vulnerabilities."

Johnson said that as his department initially uncovered the Russian probes he worried about the ramifications.

"Last year, when we saw these voter registration databases being targeted, I was very worried it was the run-up to a huge catastrophic attack," that would result in the deletion of voter



Former DHS chief Jeh Johnson said he worried about a catastrophic attack against U.S. voting systems in the 2016 elections.

ADVANCED SEARCH

New from FCW

The 20-year climb to an elevated CyberCom

Audit chides FDIC for sloppy breach protocols

FBI data center consolidation takes shape

NAACP sues Commerce amid concerns over census prep, funding

The CIO and government IT

Most Popular Articles

Audit chides FDIC for sloppy breach protocols

What should the military do when the lights go out?

How cyber impacts the full spectrum of terror threats

Keep FITARA going

FBI data center consolidation takes shape

FEATURED

Rising Stars

Meet 21 early-career leaders who are doing great things in federal IT.

[See all this year's winners](#)

registration information, he said. "We were very worried about that and we continue to worry about the ability of bad cyber actors to compromise voter registration data."

The feared catastrophic attack didn't materialize, but Johnson said the fate of national elections still can rest on key precincts in key states. Elections can "dance on the head of a pin," he said. "If writers of the TV series 'House of Cards' can figure that out, then a lot of other people could do the same."

The issue of an alleged Russian role in probing election data and systems continues to be controversial. DHS recently supplied information to state officials about attempts to probe systems in 21 states. However, officials in California and Wisconsin so far have **disputed** those claims.

DHS spokesman Scott McConnell said the agency "stands by its assessment that Internet-connected networks in 21 states were the target of Russian government cyber actors seeking vulnerabilities and access to U.S. election infrastructure."

Judd Choate, president of the U.S. National Association of State Election Directors, **told Reuters**, "there remains no evidence that the Russians altered one vote or changed one registration."

Former National Protection and Programs Directorate Undersecretary Suzanne Spaulding spoke alongside Johnson at the Sept. 28 forum, warning that the alleged Russian interference was part of a broader effort by that country to destabilize and sow discord in the U.S.

That broader effort should be addressed in Congress and in the White House, Spaulding said. "We can't wait for the outcome of investigations," she told the legislators. "We know enough now. It's time to act."

Johnson's DHS scrambled to follow up on intrusions in two states as the election drew near, as well as to respond to an increasing number of states' requesting his agency scan their systems for signs of attempted break-ins.

In his remarks to the task force, Johnson said 33 states and 36 cities and counties across the country sought cyber assistance from DHS as the 2016 election approached.

Despite those requests, there was friction between fiercely independent state election agencies and DHS when Johnson formally declared early this year that election systems were "critical infrastructure," eligible for federal protections.

Federal and state agencies, said Spaulding, can take several lessons from the incidents in 2016.

She said having cyber and infrastructure experts sit next to each other can help define and blunt hacks on critical infrastructure. DHS infrastructure experts, she said, had developed relationships with state officials that can be valuable in such situations.

In the run-up to the 2016 election and the mounting evidence of Russian probes, Spaulding said DHS "didn't appreciate" some of the finer points of how state election systems were administered, with governors and secretaries of states responsible for different aspects in different states.

Accordingly, Johnson urged congressional caution in moving possible legislation aimed at protecting state voting systems. He and Spaulding noted the valid sensitivities of states in dealing with federal agencies over their systems.

Mark Rockwell is a senior staff writer at FCW, whose beat focuses on acquisition, the Department of Homeland Security and the Department of Energy.

Before joining FCW, Rockwell was Washington correspondent for Government Security News, where he covered all aspects of homeland security from IT to detection dogs and border security. Over the last 25 years in Washington as a reporter, editor and correspondent, he has covered an increasingly wide array of high-tech issues for publications like Communications Week, Internet Week, Fiber Optics News, tele.com magazine and Wireless Week.



Rockwell received a Jesse H. Neal Award for his work covering telecommunications issues, and is a graduate of James Madison University.

[Click here](#) for previous articles by Rockwell. Contact him at mrockwell@fcw.com or follow him on Twitter at [@MRockwell4](https://twitter.com/MRockwell4).

E-MAIL THIS PAGE

PRINTABLE FORMAT

REGISTER NOW Become CUI Compliant Before It's Too Late

FEATURED



The 20-year climb to an elevated CyberCom



The CIO and government IT



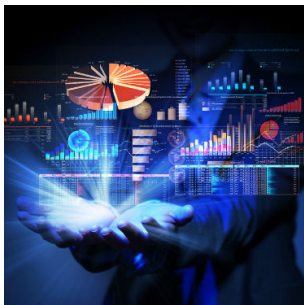
Oracle rips innovation shops



Is USPS prepping for driverless mail trucks?



What to look for in agency reorg plans



DHS moves ahead on financial system amid questions from Congress

Reader Comments

Please post your comments here. Comments are moderated, so they may not appear immediately after submitting. We will not post comments that we consider abusive or off-topic.

Name: (Optional)

Email: (Optional)

Location: (Optional)

Your Comment:



Please type the letters/numbers you see above

SUBMIT MESSAGE

Marketplace: Products

ADVERTISEMENT



Free List of \$231B Top Federal Contracts...

solarwinds

Provides the methodology an IT



Options buyers lose money 7 out of 10...



Jim Fink wasn't a professional investor,



Solving the challenges of meeting FISMA &...

More from 1105 Public Sector Media Group

Federal  **SOUP**

FEHBP expert: Feds have a good deal despite higher premiums

Committee OKs hiring boost at CBP

House passes budget that targets feds' retirement, health benefits

GCN

Standardizing and securing Navy systems in the cloud

At long last, a common login?

A one-stop shop for out-of-this-world multimedia

Washington
Technology

CMS signs onto GSA's OASIS services vehicle

Alion names new chief strategy, tech officers

SAIC wins \$980M Army 'Battlefield Systems' recompile

**DEFENSE
SYSTEMS**

Navy cyber director amps use of AI and computer automation

New radar technology lets aircraft sensors penetrate clouds, dust

Air Force, Navy team up to acquire new counter radio-controlled explosive technology

©2017 1105 Media, Inc.

Policy
Management
Who & Where
The Hill
Agencies
Opinion
Resources

Mobile site
FCW App
Digital Edition
List Rental

About Us
Contact Us
Advertise
Reprints
Subscribe
Terms of Use
Privacy Policy

 **PUBLIC SECTOR
MEDIA GROUP**

8251 Greensboro Drive, Suite 510
McLean, VA 22102
703-876-5100