

RECOMMENDED READING

The State of
Cybersecurity
Awareness

IRS Explains Why It
Gave Equifax a \$7
Million Contract After
Breach

What CIO Vacancies
Mean For Modernizing
Government

SPONSORED
The Need for Speed in the
Federal IT Lifecycle

TRENDING

DOD CLASSIFIED CLOUD // LPTA CONTRACT BILL //
MOBILE GOV SITES // SUICIDE PREVENTION // DATA REFORM //
DATA CENTERS

Search Nextgov ...

NEWS CIO BRIEFING EMERGING TECH CLOUD CYBERSECURITY MOBILE HEALTH DEFENSE BIG DATA

DHS CHIEF: WE'LL DO BETTER NEXT TIME ON ELECTION MEDDLING



Mark J. Terrill/AP File Photo

- 17 The Homeland Security Department didn't go high enough up the chain when it notified state officials about Russian attempts to penetrate election systems during the 2016 campaign, the Homeland Security Department's top official told lawmakers Wednesday.

Print this article
Email this article
Increase size

"We notified the states back when the intrusion occurred," acting Homeland Security Secretary Elaine Duke said. "What we learned from that and what we're correcting is we notified the systems' owners and didn't necessarily notify the right senior officials that need to take action."

The department won't make the same mistake during the 2018 election cycle, Duke told members of the Senate Homeland Security Committee.

» **Get the best federal technology news and ideas delivered right to your inbox. [Sign up here.](#)**

Russian government-linked hackers attempted to penetrate election systems in **either 20 or 21** states during the 2016 campaign, according to Homeland Security officials. Investigators have found no evidence that those hackers were able to actually change vote tallies or voter information, officials have said.

By **Joseph Marks**
September 27, 2017
3 Comments

**NEXTGOV
NEWSLETTER**
SUBSCRIBE

RELATED STORIES

**Congress Should
Consider Election
Security Standards,
Obama DHS Officials
Say**

**Trump
Administration
Orders Russian Anti-
virus Off All
Government Systems**
4 Comments

**Trump's Lack of
'Moral Infrastructure'
Causes Cyber
Advisers to Resign**
23 Comments

**Washington, Not
Silicon Valley, Leads
the Way in
Cybersecurity**
1 Comment

PROMOTIONS



**SPECIAL REPORT The Evolution of
Digital Government** // Transforming
services started with launching
websites. Now federal agencies are
thinking of how to put citizens' needs
first.

IT Modernization



**The White House's Cyber Tool
Wish List**
[SEE ALL COVERAGE](#)

UNDERWRITTEN BY **DELL EMC** | **intel**

FREE NEWSLETTERS

- ☐ Nextgov Today
☐ CIO Briefing
☐ Nextgov Data
☐ Emerging Tech
☐ Cybersecurity

[SEE ALL](#)

Enter your email address here...

SUBSCRIBE

BLOGS



Nextgov Event: Tech Refresh Thursday
Emerging Tech by Frank Konkel



**Without Automation, There is No
Federal IT Modernization**
Tech Insider by Bob Osborn

**For a Long, Successful Career,
LinkedIn Says Nothing Beats a Liberal
Arts Major**
Wired Workplace by Dan Kopf

SPONSORED LINKS

10 Things to Start Doing
You could become more successful by doing these
10 things each day.
[Newszoom](#)

DHS **shared details** with affected states about that hacking campaign for the first time last week.

Homeland Security has the resources to help protect voting systems from digital meddling during the 2018 election cycle, but some states are refusing federal aid, said Duke who became acting secretary when her predecessor John Kelly left to become President Donald Trump's chief of staff.

State election officials have been broadly wary of federal attempts to assist with or monitor election security in the wake of Russia's 2016 digital meddling campaign. The National Association of Secretaries of State, the officials who run state elections, severely **criticized** a late-Obama administration decision by Homeland Security to designate election systems as critical infrastructure.

That designation effectively helps the federal government devote resources to election security.

The association **also criticized** the Homeland Security Department Monday for waiting nearly a year to share information about Russian efforts to penetrate their voting systems.

Duke is also concerned that some states aren't taking digital threats to their election systems seriously enough.

"I'd like to see more sense of urgency," she told committee members.

Also during Wednesday's hearing:

- Cyberattacks against energy plants and other critical infrastructure represent both the greatest cyber threat to the U.S. and the place where Homeland Security has the most room for improvement, Duke said.
- Asked to grade cooperation on cybersecurity issues between executive branch agencies, Duke gave the government a B. FBI Director Christopher Wray gave the government a B or B minus.
- Duke urged Senators to pass a Homeland Security Department reauthorization bill that **passed the House** in July.
- Wray renewed his predecessor James Comey's call for a compromise between the tech industry and law enforcement on warrant-proof encryption systems that law enforcement leaders say allow criminals and terrorists to "go dark" in recruiting and communication. Tech leaders say any compromise on encryption would make ordinary citizens' information less secure.

RECOMMENDED FOR YOU

Intel Exec: Internet of Things Isn't Scaling As Fast As We Thought

Report: Russian Hackers Used Kaspersky Anti-virus to Steal NSA Hacking Tools

Pentagon: We'll Keep Buying Software That Russian Spies have Looked Through

Top Vacations

8 Must See Vacation Spots. This is where your next vacation needs to be...

[Newszoom](#)

Credit Score Myth

Do you know what the most common credit score myths are?

[Credit Score](#)

Unbelievable Homes

The outside of these homes may be eye-catching, but wait until you see the inside!

[Newszoom](#)

THREATWATCH ALERT

Thousands of cyber attacks occur each day

[SEE THE LATEST THREATS](#)

[ADD A COMMENT](#)



**Federal Payments
Technology Trends:
Virtual Cards**



**Infrastructure
Management and
Operation—Freeing
Agencies to Execute
Critical Missions**



**Federal Payments
Technology Trends:
Digital/Tokenization**



**Digital Briefing
Center: Intelligent
Automation**

SPONSORED

Get Smart. Get The D Brief. Subscribe to Defense One's new national security newsletter.

JOIN THE DISCUSSION

By using this service you agree not to post material that is obscene, harassing, defamatory, or otherwise objectionable. Although Nextgov does not monitor comments posted to this site (and has no obligation to), it reserves the right to delete, edit, or move any material that it deems to be in violation of this rule.

3 Comments

Nextgov

Login

Recommend

Share

Sort by Newest



Join the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

JackChanse • 11 days ago

"California Secretary of State Alex Padilla said in a statement that homeland security officials told him the scanning activity took place on the state technology department's network and not on the Secretary of State website, as the state was told last week.

"Our notification from DHS last Friday was not only a year late, it also turned out to be bad information," Padilla said in a statement."

<https://www.usnews.com/news...>

^ | v • Reply • Share ›

uncaherb • 11 days ago

So The State Department is done interfering with other nations elections?

1 ^ | v • Reply • Share ›

Thirtyeightspecial • 12 days ago

This is a point that has been lost in all of the Obama oversight of the election and the accusations of Trump Campaign collusion with the Russians...he didn't want any. How else would you get thousands of illegal ballots counted?

HRC "won" the popular vote? Hahaahahahaahhahahahaahhahahahaahhahhaaaaa!

1 ^ | v • Reply • Share ›

Subscribe Add Disqus to your siteAdd DisqusAdd Privacy

About // Contact Us // Events // Advertise // List Rentals // Site Map // Privacy Policy // Terms & Conditions

GovExec // Defense One // Route Fifty // Quartz // National Journal // The Atlantic // CityLab

© 2017 by National Journal Group, Inc. All rights reserved.

