From: CyberScoop <news@cyberscoop.com>
Sent: Friday, January 6, 2017 12:07 PM
To: Haley, Nikki
Subject: The fast-spreading lie about John Podesta’s hacked email password

The DNI can't stop counting down to Jan. 20. And we could have an inspector general's office full of penetration testers.

Not rendering correctly? View this email as a web page here.

Right-click here to download pictures. To help protect your privacy, Outlook prevented automatic download of this picture from the Internet.
CyberScoop

FRIDAY

January 6, 2017

From sea to shining sea, people seem to be comfortable in believing any ol' lie about John Podesta's email account. The Director of National Intelligence can't stop counting down to Jan. 20. And we could have an inspector general office that's full of penetration testers. (We didn't see that coming.) This is CyberScoop for Friday, January 6.

STOP MAKING US DEBUNK FAKE NEWS: It's not everyday that Ann Coulter, Julian Assange and cybersecurity experts on stage at CES all agree on the same lie. But from TV to social media, the debate over the hacking of John Podesta's emails now includes the assertion that his Gmail password was "password." If that's the case, the argument goes, anyone could have hacked him — Russia, maybe, or a 14-year-old kid (Man, we just don't know!) Yet, actually, that wasn't Podesta's password at all. Google doesn't even allow users to enter that as a password. Call it a lie, fake news, or the confused ramblings of the security and politically illiterate — either way, it's being repeated loudly and often**.** Patrick O'Neill has more.

DUDE, WE GET IT, YOU DON'T LIKE YOUR JOB: In Congress, as in comedy, timing is almost everything. So it seems unlikely to be an accident that Sen. John McCain's Armed Services Committee hearing on foreign cyber threats (aka Russian election hacking) with Director of National Intelligence Jim Clapper was scheduled a few days *before* the release of the intelligence community's much anticipated report on the issue. As Shaun Waterman reports, Clapper complained about the timing but still gave some hints about the conclusions to be unveiled next week. Oh, and being Clapper, he mentioned how much longer he still has to serve — 15 days and counting!

EVENT

DATA SECURITY IN FOCUS: The need for agencies to meet regulations and fulfill unfunded mandates will continue into the next administration. Federal IT shops are going to be saddled with protecting their data, which is only going to grow in volume. During this webinar on Jan. 18, experts will explain how agencies can embrace new forms of encryption without the worry that it will break their systems. Experts from government and HPE will take a look at how format-preserving encryption can allow for agencies to conduct their work without systems slowing down or breaking altogether. **REGISTER HERE**.

ON THE DEFENSIVE: House Homeland Security Chairman Rep. Michael McCaul is pushing back against Donald Trump's plan to increase the Defense Department's role in defending domestic computer networks. Trump's proposal, originally announced in late November, would see the Homeland Security Department take a backseat with regard to the federal government's private sector cybersecurity efforts. On Thursday, McCaul warned that shifting cyber defense authorities from a civilian to militaristic agency would be a "grave mistake" because of privacy interests and civil liberties concerns. Chris Bing has more.

HACKING TEAM, FEDERAL EDITION?: Sen. Sheldon Whitehouse is proposing the creation of an independent inspector general's office that would actively test the cybersecurity of federal, civilian agencies. The office would be staffed with “red team” operators that could penetrate or “pen test” agency computer networks, thereby providing information about existing vulnerabilities to federal executives. Whitehouse proposed the idea as part of a larger policy recommendation package that he co-authored with Rep. Michael McCaul, R-Texas, and Washington-based think tank the Center for Strategic and International Studies. Chris has more on what Whitehouse & Co. is envisioning.

A MESS IN TEXAS: Nearly 23,000 students and faculty at the largest school district in San Antonio may have had their personal information compromised in a data breach that occurred last summer, according to a district official. Northside Independent School District officials realized just a month ago how extensive the Aug. 12 cyberattack was, Executive Director of Communications Barry Perez told EdScoop. There is an ongoing investigation into the incident, he said.

TWEET OF THE DAY

☒ Right-click here to download pictures. To help protect your privacy, Outlook prevented automatic download of this picture from the Internet.
Image

We did it, we encapsulated the state of cybersecurity in one tweet.

In the meantime, how about tossing your favorite new website a follow on Twitter and a like on Facebook? Click those shiny social buttons below to get the best we have to offer across the social web.

☒ Right-click here to dow

☒ Right-click here to dow

This newsletter is produced by Scoop News Group.
Visit cyberscoop.com to read this newsletter on the web.