
From: CyberScoop <news@cyberscoop.com>
Sent: Thursday, January 12, 2017 12:12 PM
To: Haley, Nikki
Subject: Rudy Giuliani will do something cybersecurity-related for Trump, we just don't know what

Congressmen talk about cybersecurity backdoors, and an expert on the laws of war talks about the rules of cyber-response.

Not rendering correctly? View this email as a web page [here](#).



THURSDAY
January 12, 2017

So Rudy Giuliani is going have a role in Trump's administration after all. Congress' tech experts see more money for government hacking in the near future. And countries have the legal recourse to come up with any ol' reason to respond to a cyberattack. Fun times all around! This is CyberScoop for Thursday, January 12.

SO MUCH CYBER: Fresh off of taking credit for the RNC's cyber defenses during a Wednesday press conference, Rudy Giuliani "will be sharing his expertise and insight" on private cybersecurity matters for President-elect Trump. Any more details on what exactly that will entail are extremely vague. Trump made some hints at a cybersecurity panel being stood up within the first 90 days of his administration, but again, anything beyond that is vague. Giuliani is the chairman of the global cyber security practice at Greenberg Traurig and the Chairman and CEO of Giuliani Partners, an international security consulting firm. You can read the full announcement on [the transition website](#).

SO MUCH MONEY: With a bipartisan congressional consensus building against backdoors, the focus will move significantly toward giving law enforcement and intelligence agencies more resources, tools and legal means for offensive hacking in order to access whatever encrypted data comes into their crosshairs. [Congressmen from both sides of the aisle](#) said over the weekend at CES that more money is needed in order to fend off the myriad global targets and threats. The congressmen also said President-elect Trump had no idea what he was talking about when it came to the most important technology issues facing Washington, but is building an administration filled with advisers who possess the right pedigree. Those people will help get the resources law enforcement needs.

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](#).

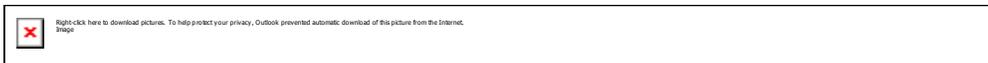
SO MUCH FOR NORMS: There is no requirement in international law for the U.S. or any other state that has been attacked to show any evidence it may have that justifies any response it may make, the leading expert on cyber and the laws of war said Wednesday in Washington. “Our position was, states may respond without providing the evidence based upon which they act,” said Michael N. Schmitt, lead author of the Tallinn Manual, widely regarded as the definitive guide to cyberwarfare and international law. It’s an issue that’s complicated by the always-tricky issue of attribution in

cyberspace, where hackers can easily hide their identity or masquerade as someone else. [Shaun Waterman has more.](#)

SO ABOUT THAT FRAMEWORK: Federal scientists at the government's technology laboratory have issued a draft update to their widely adopted Cybersecurity Framework, adding for the first time a way of quantifying risk and security outcomes. At the direction of an executive order from President Obama, NIST published version 1.0 of the framework back in February 2014 following consultations with industry, academia and government agencies. They've been collecting feedback and suggestions for changes and enhancements almost ever since. [Shaun has more.](#)

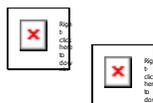
SO WHERE ARE THEY NOW?: A couple moves to note over the past few days...[Rohit Ghai was named](#) President of RSA, replacing Amit Yoran, who recently left to become CEO at Tenable...Fortinet has named Phil Quade, previously chief of the NSA Cyber Task Force, as its CISO...John P. Carlin, former Assistant Attorney General for Justice's National Security Division [will now be a partner](#) at Morrison Foerster.

TWEET OF THE DAY



"Going Dark" was supposed to be a problem, right?

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.





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

CyberScoop News 1150 18th Street NW Suite 850 Washington District of Columbia 20036 United States

You received this email because you are subscribed to CyberScoop | Newsletter from CyberScoop News.

Update your [email preferences](#) to choose the types of emails you receive.

[Unsubscribe from all future emails](#)