Cyber Security Policy and Research Institute

THE GEORGE WASHINGTON UNIVERSITY

The Weekly Newsletter of The George Washington University Cyber Security Policy and Research Institute

Quick Links

About CSPRI

Contact Us

Newsletter Archive

Blog: The CSPRI Byte

Scholarship portal is open

The GW CyberCorps Program is accepting applications for the upcoming 2016 - 2017 academic year.

The scholarship includes fully funded tuition and fees, a living stipend, book allowance, and a professional development fund.

Completed scholarship packages are due byJanuary 31, 2016.

Click **here** for more information.

December 7, 2015

Nine (9) events scheduled in the Greater Washington Area in the next few weeks.

Legislative Lowdown

-A majority of House lawmakers favor legislation that would end warrantless wiretap authority for email, and yet the legislation has failed to pass thus far. National Journal explores some of the reasons why. Spoiler alert: A big part of it has to do with law enforcement agencies who've been lobbying that the bill could damage several ongoing investigations. More here.

Morning Consult looks a little closer, noting that The Email Privacy Act, H.R. 699, would require a warrant before an enforcement agency can compel a provider to disclose the contents of any electronic communication. "The bill would clarify that a warrant is required for emails and other forms of communication older than 180 days old, and if they are stored on a cloud service,"writes Amir Nasr. "When the law was written, it was assumed that any email stored for longer than 180 days was considered to be abandoned. But now, with cloud computing and the ability to store more information for longer periods, this interpretation of email storage no longer makes sense. Agencies are against the bill because they believe it would hamper their ability to investigate crimes."

-A Republican-backed bill overhauling federal

Events

December 8
Cybersecurity Initiative Business-Policy Roundtable

December 9
ISACA CM Meetup

December 9
Cyber RiskWednesday

December 10
OWASP NoVA & DC Holiday Party

December 15
ISSA Baltimore Meetup

December 16
Crafting a National Strategy for the Internet of Things

December 16
NovaInfosec Meetup

December 17
CharmSec

December 18
International Norms in Cyberspace

Click here for detailed descriptions

Follow Us

Follow us on Twitter:
@gwCSPRI

Follow CSPRI Director, Lance Hoffman:
@lancehoffman1

Follow CSPRI Associate Director, Costis Toregas:
@DrCostisToregas

energy policy that passed the House last week includes several significant provisions aimed at defending the nation's power supply against cyberattacks, The Hill reports. "Included in Rep. Fred Upton's (R-Mich.) legislation is the creation of a "Cyber Sense" program that would require the Department of Energy (DOE) to identify and promote cyber-secure products intended for use in the bulk-power system," writes Katie Bo Williams. "The bill also requires that both the DOE and electrical utilities create plans to keep power flowing in the event of a cyberattack. In addition, it establishes a grant program for state and local governments to prepare to mitigate power disruptions resulting from a cyberattack."

Cyber Security Policy News

OPM update
-The Chinese government recently arrested a handful of hackers it says were connected to the breach of Office of Personnel Management's database this year, a mammoth break-in that exposed the records of more than 22 million current and former federal employees, according to The Washington Post. "The arrests took place shortly before a state visit in September by President Xi Jinping, and U.S. officials say they appear to have been carried out in an effort to lessen tensions with Washington," writes Ellen Nakashima. "The identities of the suspects - and whether they have any connection to the Chinese government - remain unclear."

DHS update
-The U.S. Department of Homeland Security (DHS) has been quietly launching stealthy cyber attacks against a range of private U.S. companies - mostly banks and energy firms. These digital intrusion attempts, commissioned in advance by the private sector targets themselves, are part of a little-known program at DHS designed to help "critical infrastructure" companies shore up their computer and network defenses against real-world adversaries. Read more at KrebsOnSecurity.com.

Kazakhstan's new internet law
-Before the end of the year, Kazakhstan will begin enforcing a new law that requires every internet user in the country to install a backdoor, allowing the government to spy on its citizens. The New York Times reports that the "move to intercept encrypted communications - which is scheduled to begin in January - will effectively allow Kazakh officials to monitor, or even block, vast swaths of digital content for Kazakh Internet and mobile users," writesNicole Perlroth. "Kazakhstan's largest telecommunications company said in a news release that it and other operators were 'obliged' by law to intercept encrypted web and mobile connections flowing into its borders, beginning Jan. 1. The company advertised the move

as a way to 'secure protection of Kazakhstan users' who have access to encrypted content from 'foreign Internet resources.' But, in effect, it will do the opposite, exposing Kazakh users' private communications to snooping."

Lockheed Martin IT Unit

-Forbes reports about how Lockheed Martin has been trying to sell off its $4 billion information technology unit - including its cybersecurity division. "Lockheed announced plans this past September to lay off about 500 peopleacross its information systems and government services division," reports Steve Morgan. "The Lockheed cyber business is a valuable asset, perhaps more so than any other part of the government IT services business."

About this Newsletter

This newsletter is a weekly summary of events related to cyber security policy and research, with a special focus on developments and events in the Washington, DC area. It is published by the Cyber Security Policy and Research Institute (CSPRI) of the George Washington University. CSPRI is a center for GW and the Washington area that promotes technical research and policy analysis of topics in or related to cybersecurity. More information is available at our website, http://www.cspri.seas.gwu.edu

CSPRI

202 994 5613, **cspri@gwu.edu**
Tompkins Hall, Suite 106
725 23rd Street NW
Washington DC, DC 20052