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](#)

Follow Us

**Follow us on Twitter:
@gwCSPRI**

**Follow CSPRI Director,
Lance Hoffman:
@lancehoffman1**

**Follow CSPRI Associate
Director, Costis Toregas:
@DrCostisToregas**

October 5, 2015

Ten (10) events scheduled in the Greater Washington Area in the next few weeks.

Legislative Lowdown

-Two weeks after a watchdog report uncovered a lack of coordination in the Department of Homeland Security's cybersecurity efforts, a key House committee voted to require the agency to report to Congress on a new cybersecurity strategy, NextGov reports. "The House Homeland Security Committee on Sept. 30 approved a bipartisan measure sponsored by Rep. Cedric Richmond, D-La., requiring DHS to report on its strategic goals, its capability to conduct cybersecurity investigations and how it engages with international partners, among other areas," [writes](#) Jack Moore. "The DHS inspector general's review, [issued publicly](#) earlier this month, found the agency struggles to coordinate its cyber-response activities and lacks an automated information-sharing tool to share cyberthreat data among its components."

-Tired of the government losing your Social Security number amongst a rash of recent data breaches affecting federal agencies? A new bill introduced this month would truncate Social Security numbers on common tax forms. The National Journal has [the story](#).

Events

October 5-6
[ACFCS Cyber Financial Crime Summit](#)

October 7
[The EMV Deadline and What it Means for Small Businesses](#)

October 7
[OWASP DC Meetup: Building Modern Identity Systems](#)

October 8
[Protecting Maritime Facilities in the 21st Century: Are Our Nation's Ports at Risk for a Cyberattack?](#)

October 9
[The Role of US Military in Cyberspace](#)

October 14
[ISACA CM Meetup](#)

October 15
[ISSA NoVa Meetup: Trends in DDoS Attacks](#)

October 15
[Fall 2015 Cybersecurity Summit](#)

Cyber Security Policy News

Pentagon's lack of cybersecurity policy
-Sen. John McCain (R-Ariz.) says the Pentagon's lack of a cybersecurity policy is illegal. In a hearing last week, McCain pressed defense and intelligence officials on the rules of war for cyberspace, the National Journal tells us. "In a heated exchange, McCain pressed Deputy Defense Secretary Robert Work on his department's progress in developing an 'integrated policy' for cybersecurity, a task Congress assigned the department in the fiscal year 2014 Defense reauthorization bill," writes Kaveh Waddell. "Work began responding, haltingly, 'The first is to try-first we deny and then we first find out, we do the forensics' - McCain cut him off, and asked repeatedly whether it is Pentagon policy to counterattack after such a breach. Work said a counterattack is 'one of the options.'" Read more here.

Experian breach
-Kicking off National Cybersecurity Awareness Month with a bang, credit bureau and consumer data broker Experian North
America disclosed Thursday that a breach of its computer systems exposed approximately 15 million Social Security numbers and other data on people who applied for financing from wireless provider T-Mobile USA Inc.

KrebsOnSecurity.com has the story, along with some helpful tips for warding off identity thieves.

Reuters reports that Massachusetts Attorney General Maura Healey is expecting that a multi-state probe will be launched into the breach.

FISC & the USA Freedom Act
-The shadowy Foreign Intelligence Surveillance Court has appointed its first "friend of the court" to add an outsider's perspective to the highly secretive process of approving surveillance requests from the government, according to The Intercept. "Preston Burton, a criminal defense attorney known for his work with accused spies, is the first of at least five *amici curiae* the court must appoint due to a provision in the USA Freedom Act, the surveillance-reform legislative package passed in June," writes Jenna McLaughlin. Read more here.

Automotive computer security: legality update
-Federal regulators are trying to use copyright law to quash dangerous tampering with automobile computers, sparking fears that they will stymie needed cybersecurity research, The Hill reports. The hubbub started this summer, when security researchers demoed how they could seize control over a new Jeep remotely in a live stunt on the highway, sparking concerns about how researchers go about disclosing vulnerabilities to manufacturers and the public. "Critics - including car manufacturers

- suggest that researchers who go public with their findings both recklessly expose vulnerabilities to the bad guys and give manufacturers no time to resolve concerns," writes Katie Bo Williams. "Others say silencing researchers has dangerous implications for both public safety and national security. Last month, the Department of Transportation joined a chorus of agencies petitioning the U.S. Copyright Office to stop researchers from circumventing protected technology."