Cyber Security Policy and Research Institute

THE GEORGE WASHINGTON UNIVERSITY

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

Follow Us

Follow us on Twitter:
@gwCSPRI

Follow CSPRI Director,
Lance Hoffman:
@lancehoffman1

Follow CSPRI Associate
Director, Costis Toregas:
@DrCostisToregas

November 2, 2015

Thirteen (13) events scheduled in the Greater Washington Area in the next few weeks.

Announcements

CSPRI Associate Director, Dr. Costis Toregas is attending two conferences that are shaping the role of academic institutions in Cybersecurity education: the CAE 2015 conference and the **NICE 2015 conference.**

CSPRI is managing the SFS program which provides strong Cybersecurity talent to government agencies. This is open for 2016 applicants. **Apply here.**

Legislative Lowdown

-The U.S. Senate approved a controversial cybersecurity bill last week, despite objections from privacy experts. By a vote of 74-21, the Senate approved the Cybersecurity Information Sharing Act (CISA). "Since the House earlier this year passed two different versions of a cyber-in-formation-sharing bill, lawmakers from the Senate and House will have to come togeth-er in a conference to align their versions of the legislation into a final, unified version of the bill that will need to be passed again by both chambers before it can be signed into law," writes Kaveh Waddell for National Journal. Security expert Brian Krebs last week published a comprehensive

Events

November 3
EU Safe Harbor Decision

November 3
International Data Flows

November 3
Data Brokers

November 3
Demise of EU-US Safe Harbor

November 3 - 4
SINET Showcase 2015

November 4
Federal Information Technology Act's Role in Reducing IT Acquisition Risk, Part II

November 4
The State of US Cybersecurity

November 4 - 6
International Cryptographic Module Conference

November 5
After the Shift: Securing Tomorrow'sPayment Technology

November 5
Always On: Security and Privacy in the Connected Generation

November 5
Cybersecurity Initiative Business-Policy Roundtable #3

breakdown of the positions on both sides of the bill.

Cyber Security Policy News

New White House cybersecurity plan
-The White House last week issued a broad new plan designed to better respond to cybersecurity incidents such as those that exposed secrets on millions of citizens as well as government operations, reports NextGov. "The new guidance, which aims to protect the most high-value information assets the federal government holds, is the latest step in the months-long fallout from the devastating hack of sensitive federal employee files from the Office of Personnel Management revealed this summer," write Aliya Sternstein and Jack Moore for NextGov.

EU & US on trans-Atlantic data-transfer
-The European Union on Monday said it had agreed in principle with the U.S. on a new trans-Atlantic data-transfer pact, as both sides race to complete the deal after the bloc's highest court junked a previous framework used by thousands of firms. The Wall Street Journal has the lowdown.

The agreement comes as German privacy regulators have announced an investigation into data transfers from the European Union to the U.S. from companies such as Google and Facebook. "The decision follows a bombshell court ruling that invalidated a key data-flow agreement between the United State and EU," reports The Hill. "The surprise move come just as the EU said it had struck a deal in principle with the United States on a new agreement to allow companies to legally transfer information between borders."

NSA Update
-A panel of federal judges decided Thursday that the National Security Agency can continue its phone surveillance program in the period before a formal ban enacted by Congress takes effect, according to National Journal. "The decision from the Second U.S. Circuit Court of Appeals, a small victory for the government, allows the NSA to maintain its bulk surveillance program throughout a 180-day transition period," NJ's Waddellreports. "The transition was enacted in the USA Freedom Act, which President Obama signed on June 2 of this year."

FBI uses new technology to monitor protesters
-The Baltimore Sun reports that the FBI used advanced technology on airplanes to monitor protesters in Baltimore in the week after Freddie

Gray's funeral. "Authorities see such flights as a useful way to monitor a city during unrest, but privacy advocates have expressed concern," writes Ian Duncan for The Sun. "There undoubtedly are times when aerial surveillance is an appropriate law enforcement tool for public safety or investigative purposes," Duncan quotes Nathan Freed Wessler, an ACLU attorney. "But it is essential that accurate information about such surveillance be available to the public, and that strict rules be in place to protect against unjustified mass surveillance or warrantless collection of private information." Read more here.

New exemptions to the Digital Millennium Copyright Act
-The Library of Congress has adopted new exemptions to a portion of the Digital Millennium Copyright Act (DMCA) that prohibits circumventing technology that controls access to copyrighted works. The new carve-outs include vehicle software for the purposes of diagnosis, repair, or modification and certain networked medical devices. Read more at Ars Technica.