GW CSPRI Newsletter

February 27, 2012

From the **Cyber Security Policy and Research Institute** of **The George Washington University**, www.cspri.seas.gwu.edu.

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.

Faculty and student readers of this newsletter with new and important cyber security research to report (especially new papers or results by GW faculty and students) are encouraged to send notifications of this to cspriaa@gwu.edu. A short (up to three sentences) description of why you think the research is important is required.

Contents

Events

-Feb. 28, 10:15 a.m., **Critical Infrastructure Cybersecurity: Assessments of Smart Grid Security** - The House Commerce Committee's Subcommittee on Oversight and Investigations will hold a hearing. Room 2322, Rayburn Building. More information.

-Feb. 28, 12:00 noon - 1:30 p.m., **Privacy by Design: What All Companies Need to Do Now** - FTC Commissioner Julie Brill and Anne Cavoukian, commissioner of Canada's Office of the Information and Privacy Commissioner, will speak at a Webinar event hosted by the American Bar Association. More information (PDF).

-Feb. 28, 2:00 p.m. - 3:15 p.m., **NSTAC Meeting** - The President's National Security Telecommunications Advisory Committee will meet by teleconference. The agenda includes an update from Gregory Schaffer, DHS Assistant Secretary for Cybersecurity and Communications; an update on cloud computing from Mark McLaughlin; and an update on the national public safety broadband network scoping effort from Scott Charney and Michael Laphen. More information.

-Feb. 28, 10:00 a.m. - 11:00 a.m., **Where Do We Go From Here? Building a Plan** - This is the final Webinar in a three-part series on the threat to the nation's vital infrastructures from severe space weather and electromagnetic pulse (EMP) weapons. The presenter will be Avi Schnurr,

coordinator of the International Electric Infrastructure Security Summit Series, and CEO and chairman of the Electric Infrastructure Security (EIS) Council. More information.

-Feb. 29, 2:00 p.m., **NASA Cybersecurity: An Examination of the Agency's Information Security** - The House Science Committee's Subcommittee on Investigations and Oversight will hold a hearing, which will also be Webcast. Room 2318, Rayburn Building. More information.

Legislative Lowdown

-The Cybersecurity Act of 2012, introduced by three senior senators last week, was supposed to be one that everybody could agree on. But some high-profile Senate Republicans, including Sen. John McCain (R-Ariz.) and industry representatives cite concerns about "unelected bureaucrats" being granted too much power, Federal News Radio writes. McCain also said technology-company lobbyists may have unduly influenced the legislative process. This Act would give the Homeland Security Department power to identify vulnerabilities in critical infrastructure and set regulations requiring private companies who operate critical networks to improve security or face penalties. It also requires the State Department to identify cyber threats and award foreign aid to cooperative governments while issuing sanctions against those governments that do nothing to stop cyber attacks.

(Vice Admiral Mike McConnell, USN (ret.), former Director of National Intelligence, Michael Chertoff, former U.S. Secretary of Homeland Security, and several Hill staffers discussed it at a GW Homeland Security Policy Institute event on February 22. See the event at http://www.c-span.org/Events/Michael-Chertoff-Mike-McConnell-Discuss-Cybersecurity-Bill/10737428454-1/.)

-Reps. Joe Barton (R-Texas) and Ed Markey (D-Mass.) on Thursday vowed to push ahead with their Do Not Track Kids Act, despite voluntary privacy commitments from Web companies, The Hill reports. The lawmakers stuck to their plan even after Google, Microsoft, Yahoo and hundreds of other companies in the Digital Advertising Alliance promised to work with the major Web browsers to create a "Do Not Track" button that will allow users to opt out of tracking by Internet advertisers with a single click.

Cyber Security Policy News

-The White House last week called on Congress to pass a "privacy bill of rights," that will give people greater control over the personal data collected about them. Computerworld reports that the administration will push for online businesses to adopt new privacy codes of conduct, including consumer rights to control what information websites collect about them and a right to see what data is being collected, officials there said. While the Obama administration will propose privacy legislation to the U.S. Congress, the U.S. Department of Commerce will move ahead with voluntary codes of conduct that could be implemented without congressional action. Legislation would put consumer privacy rights into law. If a company commits to following a privacy code of conduct, that commitment will be enforced by the U.S. Federal Trade

Commission, said Daniel Weitzner, the White House's deputy CTO. While adopting the privacy codes will be voluntary, many online businesses will want to consider them in an effort to retain the trust of their customers, officials said. The Obama administration's statement on the matter is available here.

-Internet service providers need to work harder to prevent hacks, data theft and other fraud, including contacting customers whose infected computers have been hijacked by organized crime, and help them clean out viruses, the head of the Federal Communications Commission said on Wednesday. According to Reuters, FCC Chairman Julius Genachowski said he sought "smart, practical, voluntary solutions" to the massive problem of Internet fraud and data theft. He estimated that 8.4 million credit card numbers are stolen online each year.

-The Obama administration is urging the Supreme Court to halt a legal challenge weighing the constitutionality of a once-secret warrantless surveillance program targeting Americans' communications that Congress eventually legalized in 2008. Wired.com reports that the FISA Amendments Act, the subject of the lawsuit brought by the American Civil Liberties Union and others, allows the government to electronically eavesdrop on Americans' phone calls and e-mails without a probable-cause warrant so long as one of the parties to the communication is outside the United States. The communications may be intercepted "to acquire foreign intelligence information." The administration is asking the Supreme Court to review an appellate decision that said the nearly 4-year-old lawsuit could move forward. The government said the ACLU and a host of other groups don't have the legal standing to bring the case because they have no evidence they or their overseas clients are being targeted.

-On Thursday, mysterious signs began popping up in metropolitan areas nationwide, accompanied by a challenge from the Defense Advanced Research Projects Agency: Be the first person to track down and report the square quick response codes on all the signs across the country and win $40,000. NextGov writes that the signs displaying the codes, also known as QR codes, were to remain in prominent public spaces until 3 p.m. Sunday, Feb. 26. For a chance to win the promised $40,000, prospective participants (sorry federal workers, you're not eligible to play) needed only a cell phone and an online social network. DARPA's unannounced contest, a successor to its similarly themed 2009 nationwide balloon hunt, is intended to study how people use social media during times of crisis.

-A federal judge last week dismissed a lawsuit from the Electronic Privacy Information Center (EPIC) that sought to force the Federal Trade Commission (FTC) to block Google's planned privacy changes. EPIC argued that Google's privacy changes, scheduled to go into effect March 1, would violate a settlement the Web company reached with the FTC last year. But in her decision, Judge Amy Berman Jackson concluded that the courts cannot review whether the FTC chooses to enforce its legal settlements.

-Millions of computers infected with the stealthy and tenacious DNSChanger Trojan may be spared a planned disconnection from the Internet early next month if a New York court approves a new request by the U.S. government. Meanwhile, six men accused of managing and profiting from the huge collection of hacked PCs are expected to soon be extradited from their native Estonia to face charges in the United States, computer security researcher Brian Krebs reports.

The Cyber Security Policy and Research Institute (CSPRI) is a center for GW and the Washington area to promote technical research and policy analysis of problems that have a significant computer security and information assurance component. More information is available at our website, http://www.cspri.seas.gwu.edu.