THE GEORGE WASHINGTON UNIVERSITY
CYBER SECURITY POLICY AND RESEARCH INSTITUTE
*Thoughtful Analysis of Cyber Security Issues*

# GW CSPRI Newsletter

February 7, 2011

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



# Upcoming Events

-Feb. 8-9, **DOJ Cybersecurity Conference** - The theme of this annual event, now in its third year, is "Leveraging a Collaborative Defense," and will offer component chief information officers, security professionals, developers, and network operations staff a chance to learn firsthand about the emerging cyber threats and ways to defend against them. Registration is free but is open only to DOJ employees and DOJ contractors. More information.

-Feb. 9, 2:00 - 3:00 p.m., **Cyber Security: How to Protect Sensitive Client Information** - Sponsored by the SMB Cyber Security Alliance, this presentation focuses on the risk to customer personal confidential information and basic steps that should be taken to better protect your business and the privacy of your customers. The SMB Cyber Security Alliance is a volunteer-run initiative by leading industry cyber security

professionals, college professors, and cybercrime researchers seeking to increase cyber security awareness in small business communities through education, awareness training, free resources, and active engagement between local information security professional and small businesses. 113 South Columbus St., Suite 100, Alexandria, Va. More information.

-Feb. 15, 7:30 a.m. - 4:45 p.m., **ISACA National Capital Area Chapter Conference for DoD Community** - This all-day conference will focus on topics of interest to the Department of Defense community and to those who provide support to the DoD. This event, however, is not restricted to those with a current DoD affiliation as there are opportunities to learn about how to engage with DoD, obtain a clearance sponsored by a DoD organization, as well as many lessons to learn about the cyber threats impacting the nation's infrastructures and applying practical applications, cyber defense mechanisms, and counter measures. Holiday Inn Rosslyn @ Key Bridge, 1900 North Fort Myer Drive, Arlington. More information.

-Feb. 16, 6:30 - 8:30 p.m., **Cyber-Security and Cyber-Deterrence - Dr. Martin Libicki**, senior management strategist at The Rand Corporation, discusses the increasing connectivity of systems and passing of information, vulnerabilities to information systems, and whether it is possible to have cyber deterrence versus playing the constant measure-countermeasure game. Marriott Residence Inn, Pentagon City, 550 Army-Navy Dr., Arlington. More information.

-Feb. 24, 8:00 a.m. - 12 noon, **FedScoop's 2nd Annual CyberSecurity Summit** - The summit will host discussions on topics such as "Securing the Cloud," and "Law Enforcement's Perspective on Cyber Crime," and feature talks from U.S. Defense Command and Control Infrastructure Admiral (Ret.) **Betsy Hight**; Justice Dept. CIO **Vance Hitch**; Dept. of Defense Deputy CIO **Robert Carey**; and Symantec Vice President **GiGi Schumm**, among others. Newseum, 555 Pennsylvania Ave, NW. More information.

# Legislative Lowdown

-At least two consumer and Internet privacy measures are expected to be introduced in Congress this week. **Rep. Jackie Speier** (D-Calif.) plans to offer a privacy bill this week directing the Federal Trade Commission (FTC) to begin a "do-not-track" program for online advertisers, according to The Hill. The publication says the program would enable consumers to "opt out" of tracking by online advertisers; that the bill is narrowly tailored to address tracking issues only, rather than the broader question of online privacy; and that it provides a floor, rather than a ceiling, for privacy law, so it does not preempt additional legislation in the future.

Rep. Bobby Rush (D-Ill.) has said that this week he will introduce his online privacy bill, last year's version of which had the backing of eBay, Intel, and Microsoft, The Hill writes. Few details of the new bill are available yet, but **David Navetta**, a privacy expert

with the **Information Law Group**, has this analysis of Rush's bill from the 111th Congress -- memorably named the Building Effective Strategies to Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards (BEST PRACTICES) Act (PDF).

-Republican lawmakers on the Senate Judiciary Committee have put off a vote on extending controversial surveillance provisions in the USA PATRIOT Act, a contentious national security law that is set to expire in about three weeks. The legislators are trying to introduce a new bill that would make permanent and provide greater judicial oversight of the sections that are about to sunset, reports NextGov. The current extension would extend by two years provisions that allow roving wiretaps of suspects who switch computers or phone numbers to avoid monitoring; tracking of "lone wolves" -- persons of interest with no known links to terrorist organizations; and retrieval of records and other tangible evidence from organizations with a court order. The renewal, which was introduced Jan. 26 by **Chairman Patrick Leahy**, D-Vt., also would heighten judicial scrutiny of such actions, NexGov writes.

# Cyber Security Policy News

-Hackers breached security systems at the NASDAQ stock exchange, the Wall Street Journal reported late last week. The WSJ story is light on details. A statement published by NASDAQ says the attackers didn't affect its trading systems, but instead appeared to be interested in an application called Director's Desk, a suite of applications that facilitates Web-based conferencing and makes it easier for companies to share documents with directors between scheduled board meetings.

-Egypt's decision to shut down the Internet for its 80 million citizens last week (it has since lifted that virtual blockade) has reignited discussion about a claimed "Internet kill switch" component of cybersecurity legislation being offered in the U.S. Congress. In the previous congressional session, Sens. Susan Collins (R-Maine) and Joseph Lieberman (I-Conn.) offered the Protecting Cyberspace as a National Asset Act, designed to provide incentives for national infrastructure providers to beef up the security around their cyber assets. The two senators have yet to reintroduce their measure, but already that effort has drawn fire from those who say it would give President Obama power to shut off the Internet, if the President determined a concerted cyber threat warranted immediate action. In joint statement issued last week, both lawmakers sought to put to rest the rumor. "We would never sign on to legislation that authorized the President, or anyone else, to shut down the Internet. Emergency or no, the exercise of such broad authority would be an affront to our Constitution," the Senators said.

In related news, the U.S. Bureau of Reclamation is shooting down a key legislative talking point for proponents of the Collins-Lieberman bill. The agency weighed in on the bill after legislative aides to the Homeland Security and Governmental Affairs Committee offered a Wired.com reporter examples of why the bill was needed. "The bill, one aide said, would give the president the power to force 'the system that controls the

floodgates to the Hoover Dam' to cut its connection to the 'Net if the government detected an imminent cyberattack." The Bureau of Reclamation, which runs the power-generating facility on the Arizona-Nevada state line, rebutted those claims, saying the control systems for the landmark dam weren't even connected to the Internet. "I'd like to point out that this is not a factual example, because Hoover Dam and important facilities like it are not connected to the internet," Wired.com quoted Peter Soeth, a spokesman for the bureau, saying in an e-mail. "These types of facilities are protected by multiple layers of security, including physical separation from the internet, that are in place because of multiple security mandates and good business practices."

Meanwhile, a recent internal test by a federally-funded broadcaster shows that the U.S. government has the power to bypass foreign Internet censors by feeding news over a special e-mail system, writes NextGov. Between March and June 2010, the Broadcasting Board of Governors successfully used the tool in China to transmit news feeds from broadcasters Voice of America, CKXX and China Weekly, a report (PDF) that the nonprofit Governmentattic.org obtained through Freedom of Information Act requests from the U.S. State Department.

-A new audit report (PDF) from the U.S. Department of Energy's inspector general offers an unflattering picture of efforts to secure the nation's power grid from cyber attacks. eWeek's **Brian Prince** writes that the audit, which was conducted between October 2009 and November 2010, found existing critical infrastructure protection standards do not always include controls commonly recommended for protecting critical information systems. But another problem was much more basic – the standards did not include a clear definition of what constitutes a critical asset. In fact, the auditors' findings mirror those reported in 2009, when then-NERC Chief Security Officer Michael Assante reported that only 29 percent of power generation owners and operators – and less than 63 percent of power transmission owners – identified at least one critical asset on a self-certification compliance survey.

-In late December, spoofed emails claiming to come from the White House bypassed filters and infected U.K. government systems with a variant of the Zeus information-stealing Trojan, **Foreign Secretary William Hague** told the Munich Security Conference on Friday. ZDNet UK writes that in his speech, Hague called for new rules to establish how countries should behave in cyberspace. "In Britain, we believe that the time has come to seek international agreement about norms in cyberspace," Hague said. "We believe there is a need for a more comprehensive, structured dialogue to begin to build consensus among like-minded countries and to lay the basis for agreement on a set of standards on how countries should act in cyberspace."

Recent cyberattacks are adding new momentum behind a push to have the United Kingdom sign the European Commission's cybercrime directive, which tends the borders between European Union member countries' law enforcement domains by requiring each of them to establish a central cyber-security operation which can be contacted by other states, contacts that would have to be responded to within eight hours under the ruling. But tensions have broken out in the U.K. House of Commons over the plan, with critics

charging that the directive involved changing UK law and creating new criminal offences without a prior debate in parliament.

*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.*