

Cyber Security Policy and Research Institute

THE GEORGE WASHINGTON UNIVERSITY

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

In This Issue

[Quick Links](#)

[Announcements](#)

[Cyber Security Policy News](#)

[Events](#)

Quick Links

[About CSPRI](#)

[Contact Us](#)

[Newsletter Archive](#)

[Blog: The CSPRI Byte](#)

November 3, 2014

Four (4) Cyber security Events are scheduled in the Greater Washington Area in the few weeks.

Of note this week...

NSF Scholarship for Service Program application to open again

CSPRI is pleased to announce that the scholarship application process is open once again for the National

Science Foundation's (NSF) Scholarship for Service program. This program aims to build a sustainable and interdisciplinary cyber workforce with candidates from across all of GW's Schools (but the application is not limited to just GWU students) - see more on www.cspri.seas.gwu.edu.

Please note that application process is only open to prospective applicants who are US citizens due to the scholarship terms of mandatory employment with the government following graduation from the program.

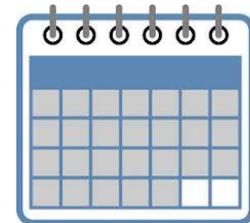
The scholarship fully funds a recipient's education at the undergraduate, graduate, or doctoral level - for a maximum of three years. It includes the cost



Events

Click [here](#) for descriptions of the upcoming events!

Click the Calendar to See Upcoming Events at a Glance!



Follow Us

Follow us on Twitter:
[@gwCSPRI](#)

Follow CSPRI Director,
Lance Hoffman:
[@lancehoffman1](#)

Follow CSPRI Associate
Director, Costis Toregas:
[@DrCostisToregas](#)

Follow CSPRI Research
Scientist, Allan
Friedman:
[@allanfriedman](#)

of tuition and related fees, a living stipend, a book allowance every semester, and a professional development fund. A signature seminar program brings students together with leaders in the cyber security space on a weekly basis and ensures alignment of academic accomplishments with ongoing realities of the cyber world. In exchange for this scholarship, the recipient agrees to work for a federal, state, local, or tribal government entity at least for the same number of years.



Each year, CSPRI awards these scholarships to a variety of students who demonstrate impressive academic performance, practical experience in their field, and unmatched personal drive to succeed. Prospective applicants from all academic disciplines are encouraged to apply. Keep an eye on our web portal and newsletter in the coming weeks for updates on the scholarship process.

Cyber Security Policy News

White House breached by Russian hackers

-The White House joined the ranks of organizations that have been hacked by Russian hackers last week. As The Washington Post reports, "hackers thought to be working for the Russian government breached the unclassified White House computer networks in recent weeks, sources said, resulting in temporary disruptions to some services while cybersecurity teams worked to contain the intrusion." Ellen Nakashima [writes](#) that "the breach was discovered two to three weeks ago, sources said. Some staffers were asked to change their passwords. Intranet or VPN access was shut off for awhile, but the email system, apart from some minor delays, was never down, sources said."

Fake Associated Press story sparks a call for more reliable accounting of events from the FBI

-Lawmakers in the House and Senate are clamoring for a clearer accounting of events from the FBI, after privacy activists revealed last week that the agency used a fake Associated Press story to plant malicious software on the computer of a bombing suspect in 2007. "Documents obtained by the San Francisco-based Electronic Frontier Foundation and publicized this week by Christopher Soghoian, the principal technologist for the American Civil Liberties Union, revealed that the FBI's Seattle office forged an AP story to help catch a 15-year-old suspect who had been making bomb threats at a high school near Olympia," [writes](#) the Associated Press. "The FBI obtained a warrant from a federal magistrate judge to send a 'communication' to a social media

account associated with the bomb threats." That "communication," the AP writes, actually contained a software tool that could verify Internet addresses.

Facebook is now compatible with Tor software

-Facebook is known for tracking its users down to every last click, but in a surprise move last week, the social networking giant launched a version of its site that is reachable via Tor, a network designed to protect the privacy and obscure the location of its users. "That new site, which can only be accessed by users running the Tor software, bounces users' connections through three extra encrypted hops to random computers around the Internet, making it far harder for any network spy observing that traffic to trace their origin," [writes](#) Andy Greenberg, for Wired.com.

Obama administration wants help from technology companies

-The Obama administration is gearing up a campaign to coax technology companies into helping the government spy on their users, according to The National Journal. "FBI and Justice Department officials met with House staffers this week for a classified briefing on how encryption is hurting police investigations, according to staffers familiar with the meeting," [reports](#) Brendan Sasso. "The briefing included Democratic and Republican aides for the House Judiciary and Intelligence Committees, the staffers said. The meeting was held in a classified room, and aides are forbidden from revealing what was discussed."

Fingerprint vs. passcode

The campaign comes as a Virginia court has ruled that a criminal defendant can be compelled to give up his fingerprint, but not his pass code, to allow police to open and search his cellphone. "The question of whether a phone's pass code is constitutionally protected surfaced in the case of David Baust, an Emergency Medical Services captain charged in February with trying to strangle his girlfriend," [writes](#) Elisabeth Hulette, for the Virginian-Pilot. "Judge Steven C. Frucci ruled this week that giving police a fingerprint is akin to providing a DNA or handwriting sample or an actual key, which the law permits. A pass code, though, requires the defendant to divulge knowledge, which the law protects against, according to Frucci's written opinion."

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

304 Staughton Hall

707 22nd St., NW

Washington DC, DC 20052