POLITICO

POLITICO
Morning Cybersecurity
A daily briefing on politics and cybersecurity

Can CISA beat the clock? — DARPA seeks attack-resilient software — An asymmetric approach to Chinese cybertheft

By **JOSEPH MARKS** | 08/04/15, 10:02 AM EDT

With help from David Perera and Adam Sneed

CAN CISA BEAT THE CLOCK? — The Cybersecurity Information Sharing Act of 2015 appears on its way to the Senate floor at long last, but the big question is whether it will beat the Senate calendar. Senate Majority Leader Mitch McConnell took the upper chamber one step closer to considering the bill when he filed for cloture Monday evening. But McConnell didn't have unanimous consent to proceed, which means the bill likely won't reach the floor before Wednesday. That leaves proponents a tight window to get the bill through, as many senators want to bolt town for the summer break ahead of the GOP presidential debate Thursday evening in Cleveland.

"We'd like to get that done," said McConnell spokesman Don Stewart. Opponents, however, say the bill may be too controversial to handily dispose of this week. "You're looking at Friday or the weekend before final passage," a Senate Democratic aide said, adding that a Thursday deadline "just seems like an unrealistic time frame."

The broad strokes of the debate began to come into focus Monday. On one side is a manager's amendment aimed at placating CISA opponents. That amendment would limit information sharing to data with a "cybersecurity purpose" and bar the government from using cyberthreat data shared by outside entities for investigation of "serious violent felonies," according to a draft shown to MC. Investigation of other crimes, such as identity and trade secret theft, would still be allowed. On the other side is an amendment proposed by Sen. Tom Cotton that would grant liability protection to companies that share cyberthreat indicators directly with the FBI and Secret Service.

CISA foes were quick to condemn the manager's amendment. "Any senator who values privacy and security must reject this attempt to sacrifice both at the altar of increased surveillance and corporate liability protections," said Amie Stepanovich, U.S. policy manager at human rights group Access. Proponents sounded a welcoming note. "The Senate was wise to make CISA a priority before recess," said Victoria Espinel, CEO of BSA | The Software Alliance. Retail industry associations also expressed support for the Cotton amendment. The letter: http://politico.pro/1HnbH5V

HAPPY TUESDAY! Welcome to Morning Cybersecurity, where Joe's your host today, back from a great weekend in the Twin Cities, including a fantastic introduction to Lowertown St. Paul. Thanks to Faces, Pazzaluna, The Bulldog and the Gopher Bar. And thanks to "Pig's Eye" Parrant, the "coarse, ill-looking, low browed fellow" who set the whole thing in motion: http://bit.ly/1M8oTQY. Wherever you're staking your claim today, drop us a line. Send your thoughts, tips and feedback this week to jmarks@politico.com and follow @ joseph_marks_, @ POLITICOPro and @ MorningCybersec. Full team info is below.

DARPA SEEKS ATTACK-RESILIENT SOFTWARE — The Defense Advanced Research Projects Agency's information innovation office is looking for research proposals that can guarantee the U.S. military a long-term information advantage, according to an agency announcement out Monday. At the top of the office's wish list: research aimed at developing "software that is inherently resilient to attack and computing architectures that can be rapidly restored following an attack."

The office plans to support "research in areas such as formal methods, software diversity, transparency/causality/information flow tracking, and automated cyber response," according to the notice. This research could span "military systems, embedded systems, critical infrastructure, industrial systems, vehicular systems, the Internet of Things, and enterprise networks." DARPA expects to fund a "limited number of proposals" resulting from the solicitation and hasn't determined the total funding dollar amount, the notice states. Take a look: http://1.usa.gov/1KMQpGf

AN ASYMMETRIC APPROACH TO CHINESE CYBERTHEFT — If the U.S. wishes to stem China's cyber theft of U.S. companies' intellectual property, it should start launching asymmetric counterattacks, author and scholar Abe Shulsky argues in a Hudson Institute primer on "Cyber-Enabled Economic Warfare" released Monday. "One possibility might to be to exploit the Chinese sensitivity to the free flow of information," says Shulsky, who wrote one of five chapters in the report. "An information campaign that rendered part of the censorship apparatus ineffective might create sufficient pressure," he writes, or "the collection and judicious leaking of information about the assets of … key officials could serve the same purpose." To date, the U.S. response to Chinese cyber-economic espionage has focused on naming and shaming the Chinese and, in one case, indicting five members of the People's Liberation Army.

In another report chapter, former Deputy National Security Adviser Juan Zarate argues the government should consider giving companies limited licenses to "hack back" against foreign cyber thieves. The report: http://bit.ly/1KNhFSo

GERMANY'S NETZPOLITIK DRAWS DEFENDERS ONLINE AND OFF — Hackers were responsible for taking part of the German federal prosecutor's office offline earlier this month, a day after the office announced an investigation into alleged treason by the Netzpolitik blog, a spokeswoman told Reuters on Monday. The blog drew prosecutors' ire when it published documents earlier this year about secret plans for launching bulk surveillance programs. Prosecutors have since backed off and are expected to officially find the blog's reports aren't treasonous, as they originally claimed, according to German media (http://bit.ly/1P1OFrm). The office's spokeswoman didn't give Reuters any details about the scope of the attack or its perpetrators (http://reut.rs/1eOSvHf). Civil libertarians, meanwhile, have rallied around Netzpolitik. An open letter that's currently seeking signatories calls the investigation "an attack against the free press" and against the German constitution.

A FRESH TAKE ON 'DO NOT TRACK' — A group of privacy advocates and Web services is banding together to revive online "Do Not Track" protections, and they've crafted a new set of standards to boost privacy protections and support advertising best practices. The Electronic Frontier Foundation worked with Disconnect, Medium, AdBlock, Mixpanel and DuckDuckGo to write and implement the new policy, which would let users opt out of online trackers that collect information that powers targeted ads. Do Not Track standards have had some trouble getting off the ground in the past. Do not tracks is an option built into the most popular Web browsers, but many websites simply ignore it. The new standard isn't an ad blocker, but works "in tandem" with ad-blocking technology, EFF says. More from EFF: http://bit.ly/1SXi3Q4

ICYMI: THERE'S A NEW BOSS AT IARPA — Dr. Jason Matheny is taking the helm as the next director of the Intelligence Advanced Research Projects Activity agency, Director of National Intelligence James Clapper announced Monday. Matheny is assuming the post as IARPA works on major projects to forecast cyberthreats using unconventional sensors such as social media (http://1.usa.gov/1MIQ9rb) and to root out insider threats by seeding employees with lures (http://1.usa.gov/1M1MxzV). Matheny was previously director of IARPA's office for Anticipating Surprise. He's succeeding Dr. Peter Highnam, the second IARPA director. Highnam moved to a position at the National Geospatial Intelligence Agency in July, according to his LinkedIn profile. More here: http://politico.pro/1IUIOFr

ON THE MOVE:

— Former Tor Project executive director Andrew Lewman will be joining the cyber intelligence firm Norse as vice president of data development, the company said in a press release. Tor co-founder Roger Dingledine is serving as the organization's interim executive director while the nonprofit searches for a permanent replacement, according to the company's website.

— Covington and Burling privacy attorney Jeff Kosseff is moving to the U.S. Naval Academy's cybersecurity department, where he will be an assistant professor of cybersecurity law, according to an email to colleagues. The Naval Academy will graduate its first class of cyber operations majors next year.

QUICK BYTES

— JPMorgan is speeding up its cybersecurity spending plan and aims to spend $500 million this year. The Wall Street Journal: http://on.wsj.com/1SXK2PD

— Yahoo acknowledges hackers exploited a Flash vulnerability in its ad network for a week. The New York Times: http://nyti.ms/1gFUSy2

— This firmware worm attacks Macs too. Wired: http://wrd.cm/Jwn9hk

— Hacktivists briefly seize Donald Trump's website to say goodbye to Jon Stewart. The Register: http://bit.ly/1gObgID

— The Electronic Frontier Foundation has a rundown on Arab government contracts with Hacking Team. EFF: http://bit.ly/1Ujhp1Y

— Your laptop or smartphone's battery life may be the next thing used to track you. The Guardian: http://bit.ly/1KLzt32

— Here are the winners of this year's U.S. Cyber Challenge Western Regional Cyber Camp competition. USCC: http://bit.ly/1OLSPmA

— Estonia is hosting a hackathon to develop apps for its e-residency program. Motherboard: http://bit.ly/1M7D77B

That's all for today. Hey, I'm no good at goodbyes. http://onion.com/1HnhhVC

Stay in touch with the team: Joseph Marks (JMarks@politico.com, @ Joseph_Marks_); David Perera (dperera@politico.com, @ daveperera); and Shaun Waterman (swaterman@politico.com, @ WatermanReports).