Cybersecurity: Washington Week in Review, Week of January 24

JANUARY 29, 2016

***H*omeland Security Committee Chairs Lay Out Cyber Agenda**

On Tuesday, January 26, House Homeland Security Chairman Mike McCaul (R-TX) published an essay on Bloomberg Government, in which he laid out an expansive cyber legislative agenda for the committee. “According to the essay, Rep. McCaul will hold “regular” hearings this year on the implementation of The Cybersecurity Act of 2015. Additionally, the panel will examine a proposed reorganization of the National Protection and Programs Directorate; assess an array of potential incentives for companies to bolster their defenses (including applying the lessons of the SAFETY Act to cyber, working on bolstering cyber insurance, and more effective use of the National Institutes of Standard and Technology framework); and look to help state and local governments protect their networks.

On the other side of the Hill, Rep. McCaul’s Senate counterpart, Ron Johnson (R-WI) spoke about his cyber agenda during a speech at the American Enterprise Institute on Thursday, January 28. Now that Congress has passed information-sharing legislation, the next order of business should be establishing a national standard for reporting data breaches, Senator Johnson said. He also said Congress needs to figure out how to deter future attacks.

Senate Judiciary Committee Passes Trade Secrets Bill

On Thursday, January 28, the Senate Judiciary Committee passed the Defend Trade Secrets Act (S. 1890), which would allow companies to sue trade secret thieves in federal court. The committee approved the bill by a voice vote, following the addition of an amendment by the Committee’s leaders, Chuck Grassley (R-IA) and Patrick Leahy (D-VT) protecting whistleblowers. While combatting foreign cyber espionage is not the main focus of the bill, it has been seen as a tool to go after current and former employees who steal trade secrets, and thus may address some cyber issues (such as insider threats).

House Oversight Committee Investigates Government Use of Juniper

The House Oversight Committee is asking government agencies for more information on a how a

recent hack of Juniper Networks firewalls has impacted federal agencies. On Thursday, January 21, the committee sent letters to 24 agencies, asking them to provide and inventory of affected Juniper products and the dates that they fixed the identified security flaws. The inquiry comes after it was revealed in December that many government agencies had been using a security tool for years with an unauthorized backdoor planted in it. The letter was followed by a Wall Street Journal op-ed from Representative Will Hurd (R-TX), Chair of the House Oversight IT subcommittee, about the breach and the letters.

OPM Shake-Up: DoD to Take Control of Background Check IT

In a pre-blizzard Friday news dump, OPM announced on Friday, January 22 that it will form a new agency to handle background checks, with IT systems controlled by DoD. The newly created National Background Investigations Bureau will replace OPM's Federal Investigative Services agency and will focus only on background checks.

Reactions to the news on the Hill were mixed. Representative Will Hurd (R-TX), Chair of the House Oversight IT subcommittee, is reserving judgment until he learns more. "This is another task that the Department of Defense has to take on. Most folks would think their level of sophistication is much higher," Rep. Hurd said. "But is this the right move for them? Technical capabilities aside, are these the folks that should be protecting this? I'm not saying it isn't, but these are the kinds of questions that should be asked."

Representative Jason Chaffetz (R-UT), chair of the full Oversight committee, was less conciliatory. "Simply creating a new government entity doesn't solve the problem," he said. "Today's announcement seems aimed only at solving a perception problem rather than tackling the reforms needed to fix a broken security clearance process."

Representative Adam Schiff (D-CA), ranking member of the House Intelligence Committee, applauded the change. "OPM was never designed, nor intended to be, an intelligence or national security agency," Rep. Schiff said. "By entrusting the cybersecurity of this new bureau to the Pentagon, we will be better able to ensure that the personal information of those who work to secure all of us is protected."

US, Australia Announce Cyber Partnership

On Tuesday, January 18, President Obama and Australian Prime Minister Malcolm Turnbull announced that the US and Australia plan to launch a new dialogue to improve cooperation in responding to cyberattacks and cybercrimes. The leaders also agreed to promote peacetime rules of the road in cyberspace, according to the White House fact sheet, which did not provide further details. However, during a speech the day before at the Center for Strategic and International Studies, Prime Minister Turnbull endorsed a key US-backed cyber norm, saying "states should not knowingly conduct or support cyber-enabled intellectual property theft for commercial advantage."

Carson Releases Cyber Plan

On Monday, January 25, Ben Carson became the latest GOP candidate to release a cyber plan.

Comparing the race to win the cyberspace race to the more traditional space race, Carson's plan calls for unifying the government's "disjointed and ineffective" approach to cybersecurity, similar to "[w]hen President Kennedy said he'd land an American on the moon." Carson's plan would consolidate federal cyber efforts under a new agency, the National Cyber Security Administration (similar to the creation of NASA). Rather than adding federal bureaucracy, the new agency would consolidate and unify "countless and often redundant programs, initiatives and offices which [currently] operate disjointedly throughout the government."

Sector-Specific Updates:

- ***Automotive.*** On Friday, January 15, the Transportation Secretary Antony Foxx announced that the agency has reached a "historic" data sharing agreement with 17 automakers in an effort to catch safety defects sooner, and minimize cybersecurity risks for increasingly computer-reliant vehicles. The protocol encourages the government and automakers to focus on ways they can proactively identify safety trends and spot problems, while also increasing participation in safety recalls. It also calls on the groups to come up with best practices to mitigate threats posed by hackers and other cybersecurity concerns.

  But the following Wednesday, FTC Commissioner Maureen Olhausen, speaking at the Washington Auto Show's Public Policy preview panel, said automakers will have to take reasonable steps to secure consumer information or face enforcement actions over privacy. "[Automakers] really need to take into account the security of information for connected cars and connected trucks and the security of those systems," Olhausen said.
- ***Energy.*** On Tuesday, January 26, the Federal Energy Regulatory Commission (FERC) announced final approval of new critical infrastructure standards addressing the cybersecurity of the electric grid. The revised version of the Critical Infrastructure Protection Reliability Standards include standards addressing security management controls, physical security of cyber systems, recovery plans for bulk electric system cyber systems, vulnerability assessments, and information protections. "The proposed CIP Reliability Standards are designed to mitigate the cybersecurity risks to bulk electric system facilities, systems, and equipment, which, if destroyed, degraded, or otherwise rendered unavailable as a result of a cybersecurity incident, would affect the reliable operation of the Bulk-Power System," the notice states. The new rules will go into effect on March 31.
- ***Healthcare.*** On Friday, January 15, the Food and Drug Administration published draft cybersecurity guidance for medical device manufacturers. The guide outlines recommendations for medical device manufacturers to plan and assess cybersecurity vulnerabilities in their products, encouraging implementation of cyber risk management frameworks and quick response to identified vulnerabilities. Such a program should apply the National Institute of Standards and Technology's cybersecurity framework; monitor cyber information sources for identification and detection of cyber risks; adopt a coordinated vulnerability disclosure policy; and include the deployment of mitigation measures to address cyber risks ahead of exploitation. Public comments on the guidelines will be accepted until April 15.