Cybersecurity: Washington Week in Review, Week of April 10

APRIL 15, 2016

Hoyer to Sponsor White House IT Plan

This week, House Minority Whip Steny Hoyer (D-MD) announced that he will introduce a White House proposal for an Information Technology Modernization Fund (ITMF), a central component of the president's February Cybersecurity National Action Plan. The bill would create a $3.1 billion revolving fund, overseen by an independent review board, to be used to upgrade aging, vulnerable systems. Agencies would be required to repay the ITMF, with the goal of using the fund to address $12 billion in projects over 10 years.

House and Senate Examine IRS Cybersecurity

Three congressional committees heard testimony this week from IRS officials about the agency's cybersecurity.

On Tuesday, April 12, IRS officials testified at a Senate Finance Committee hearing. In his opening statement, Chair Orrin Hatch (R-UT) pointed to "unprecedented growth in the scope and scale of cyberattacks aimed at stealing personal information and billions of dollars from taxpayers." Ranking member Ron Wyden (D-OR) struck a more dire tone, saying that, in his view, "taxpayers have been failed by the agencies, the companies, and the policymakers here in Congress they rely on to protect them." "And it's my judgement," he continued, "that you can't have an honest discussion about protecting taxpayer information without including the vulnerabilities from e-file providers, as well as crooked return preparers who operate in the shadows and steal from customers."

During the hearing, Senator Hatch said that the committee will soon consider a bill aimed at combatting tax-refund fraud. The bill was abandoned in September following objections from the American Institute of CPAs regarding a provision that would give the IRS more authority to regulate paid tax preparers, a recommendation the IRS inspector general and the Comptroller General made again on Tuesday. Another, less controversial, provision would renew the agency's streamlined critical pay authority, a tool to recruit IT professionals that expired in 2013. IRS Commissioner John Koskinen reiterated calls for the program's renewal, noting the IRS would lose 10 top technology officials by this time next year without it.

Commissioner Koskinen also rebuffed criticism against the agency, noting the unprecedented

volume of cyber criminals attempting to attack the IRS, and that the agency has implemented 80 of the GAO's cybersecurity recommendations over the last few years. Senator Tom Carper (D-DE) also came to the agency's defense while blaming Congress for failing to properly fund the IRS's efforts. "When it comes to protecting American taxpayers' sensitive information online, Congress continues to ask the IRS to do more with less by enacting deep and damaging cuts to the agency's budget," Senator Carper said. "Over the last five fiscal years, with roughly a 10 percent reduction in funding from 2010 to 2015, Congress has cornered the IRS into cherry picking what services it can afford to provide American taxpayers."

On Wednesday, April 13, Commissioner Koskinen testified before the House Small Business Committee, where he faced questions about how small businesses can be assured that their information is being kept safe by the IRS.

And on Thursday, April 14, Commissioner Koskinen came back to the Capitol to testify before a House Science subcommittee. "The IRS has not taken the necessary steps to ensure that individuals are who they claim to be before handing over Americans' confidential tax information," Subcommittee Chair Lamar Smith (R-TX) said in his opening statement. "Slow responses and partial measures at the IRS do not protect innocent Americans from cyberattacks." Members of the subcommittee particularly criticized the IRS for not following the National Institute of Standards and Technology (NIST) authentication standard, which might have prevented last year's breach. Commissioner Koskinen responded that the agency has to balance convenience and security, noting that, even with the measures the IRS is taking, many taxpayers have difficulty filing online.

House Holds Hearing on Security of Electric Grid

On Thursday, a House Transportation subcommittee questioned officials from the Departments of Energy and Homeland Security about the electricity grid's ability to recover from a cyber attack. "Whether it is a Category 5 hurricane hitting Miami or an 8.0 earthquake in Los Angeles, the federal government has realistic estimates or scenarios for states to plan," Subcommittee Chair Lou Barletta (R-PA) said in his opening statement. "The federal government does not have this basic planning scenario for a cyber threat to the power system and there is a huge disparity in what different groups think is a potential scenario for which states and local governments should prepare."

Members of the committee appeared particularly concerned following the December 2015 attack on the Ukrainian electrical grid. North American Electronic Reliability Corp. (NERC) Chief Gerry Cauley tried to ease concerns, saying "I can't imagine a cyberattack that's going to damage equipment and have an outage of more than hours or days," he said, noting that the security controls in North America are very different than in Ukraine.

Cyber Commission Completes Roster, Holds First Meeting

President Obama's newly created Commission on Enhancing National Cybersecurity met for the first time on Thursday. Prior to the meeting, the White House announced the remaining appointees to the Commission, including former NSA head and IronNet CEO Keith Alexander; MasterCard President and CEO Ajay Banga; CrowdStrike General Counsel and Chief Risk Officer Steven

Chabinsky; former NIST director Patrick Gallagher; Microsoft Vice President Peter Lee; Stanford University scholar Herbert Lin; and Uber Chief Security Officer Joe Sullivan.

At the inaugural meeting, the Commission began the task of trying to break new ground to develop recommendations for the President by December 1. "There are a lot of reports, there are a lot of smart people working on this and we keep seeing the same failures over and over again," Gallagher said. Lisa Monaco, White House counterterrorism director, urged the commission to develop “actionable, concrete recommendations that address the root causes of the challenges that we are facing.” Lin noted complaints from the private sector that the federal government asks them to share cyber threat information and then never follows up or offer anything in return. General Alexander said a high priority for the commission is to improve public-private relations.

Congress Presses Administration on Ransomware

On Friday, April 8, Senator Barbara Boxer (D-CA) sent a letter to FBI Director James Comey, expressing “grave concerns” about the recent ransomware attacks against hospitals. “I am concerned that by hospitals paying these ransoms,” the letter said, “we are creating a perverse incentive for hackers to continue these dangerous attacks.” The letter requested information regarding the FBI’s efforts to investigate these attacks, as well as steps hospitals and other businesses can take to protect themselves before and after such attacks. And on Tuesday, Representative Derek Kilmer (D-WA) sent a letter to Assistant Secretary of Homeland Security for the Office of Cybersecurity and Communications, Andy Ozment, regarding the threat posed by ransomware. Similar to Senator Boxer’s letter, Representative Kilmer requested that DHS provide guidance on steps that can be taken to reduce the chances of ransomware attacks and to whom companies and agencies can “turn for assistance either to prevent attacks, report attacks, or mitigate the damage from an attack.”

Sector-Specific Updates

- ***Automotive.*** Following a visit to Detroit earlier this week to talk to auto industry officials, Assistant Attorney General John Carlin spoke about the cyber threat to internet-enabled and self-driven vehicles. He said that, while in Detroit, he emphasized that “all the same bad guys, crooks, nation states who want to steal and cause destruction and terrorists, they go where our technology goes.” Referencing a Jeep recall last year following the hacking of the vehicle’s onboard system, Carlin said the auto industry can be a model for staying ahead of the problem. "We want the future to be safe cars at the moment they are deployed," he said.
- ***Energy.*** On Tuesday, the Nuclear Regulatory Commission (NRC) published a final regulatory basis document to support the future adoption of new cybersecurity requirements for certain nuclear fuel cycle facility licensees. While NRC took comments on a draft version published in September, it won’t take further comments until the proposed rule is published.
- ***Financial Services.*** On Tuesday, SEC Chair Mary Jo White told the Senate Appropriations Financial Services Subcommittee that the agency needs to hire additional staff in order to strengthen its cybersecurity. “Funding at the requested level will permit the agency to hire

an additional 250 staff in critical, core areas and continue to improve our information technology so that we can better oversee today's markets with the sophisticated tools necessary to safeguard investors," she said. She noted that the request would help improve cybersecurity controls to secure agency data and "what companies provide to us."

Upcoming Hearings of Note

- On Tuesday, April 19, the Senate Armed Services Subcommittee on Emerging Threats and Capabilities will hold a closed hearing to examine cybersecurity and US Cyber Command in reviewing the Defense authorization request for FY 2017.
- On Wednesday, April 20, the House Small Business Committee will hold a hearing entitled "Small Business and the Federal Government: How Cyber-Attacks Threaten Both."
- On Wednesday, the House Oversight Subcommittee on Information Technology will hold a hearing entitled "Federal Cybersecurity Detection, Response, and Mitigation."