Cybersecurity: Washington Week in Review, Week of April 17

APRIL 22, 2016

In this week's roundup of the latest cybersecurity-related happenings, DHS and NIST discuss cyber information-sharing and tax day arrives with calls for legislation to address identity theft and tax refund fraud.

Senate Finance Committee Advances Legislation Tackling Identity Theft and Tax Refund Fraud

Officials from the Internal Revenue Service (IRS) are celebrating tax season by continuing to testify before Congress. On Tuesday, IRS Commissioner John Koskinen testified before the House Ways and Means Oversight Subcommittee on the IRS's efforts to protect taxpayer information. "Our primary focus is to prevent criminals from accessing taxpayer information stored in our databases," he testified. He also noted that growing demand for online tax services "underscores the need for adequate information technology and cybersecurity funding," which may get a boost thanks to legislation coming out of the Senate Finance Committee. Senator Orrin Hatch (R-UT) followed up on promises he made during last week's hearing on tax fraud to consider a bill aimed at combatting tax refund fraud. On Wednesday, April 22, the Finance Committee approved two bipartisan taxpayer protection bills.

One bill is aimed specifically at addressing identity theft and cybersecurity at the IRS. It includes provisions to provide the IRS with "streamlined critical pay authority" to help the agency recruit and retain qualified information technology staff. An amendment added to the bill would require the IRS to notify victims of employment-related identity theft, which includes situations where Social Security numbers on a W-2 does not match the tax return filer's name.

Cyber Information-Sharing Continues to Expand

On Thursday, the Department of Homeland Security (DHS) released an advanced notice of proposed rulemaking to update its procedures for accepting Protected Critical Infrastructure Information (PCII). The agency seeks comment on transitioning its PCII program from paper records to an electronic environment, including how to establish an automated submission process with robust auditing and statistical reporting requirements.

DHS also provided an update on its cybersecurity information-sharing network launched as part of the Cybersecurity Act. Since March 17, fourteen private sector entities have connected to the

framework. Assistant Homeland Security Secretary Andy Ozment revealed at a hearing of the House Oversight Subcommittee on Information Technology on Wednesday that an additional 82 organizations have signed agreements to participate, as well.

As more organizations join the federal effort, the National Institute of Standards and Technology issued a second draft of Special Publication 800-150 on Thursday, which aims to provide guidance to "improve cybersecurity operations and risk management activities through safe and effective information sharing practices" and "help organizations plan, implement, and maintain information sharing." Public comments are due by May 24.

House Subcommittee Takes Steps to Give DOD More Control Over Federal Background Checks

On Thursday, the House Armed Services Subcommittee on Emerging Threats and Capabilities approved language to its section of the fiscal 2017 defense policy bill that would grant the Department of Defense (DOD) control over portions of the federal government's background check system. This action would reorganize the Office of Personnel Management (OPM) in the wake of last year's massive data breach, and it would require DOD to coordinate with OPM and the Office of the Director of National Intelligence to establish "a governance charter to delineate responsibilities between organizations, as well as to review and revise as necessary the executive orders, statutes, and other authorities related to personnel security." Additional reporting to Congress would also be required.

Sector-Specific Updates

- **Energy.** On Wednesday, the sweeping Energy Policy Modernization Act (S.2012) was approved 85-12 in the Senate, making the Department of Energy (DOE) the primary cybersecurity agency for the power grid. Specifically, the bill permits the President to determine when "immediate action" is necessary to protect the power grid from cyber threats and directs DOE to intervene. The legislation's cyber provisions also authorize funds for DOE to establish cyber-testing programs and to conduct cyber research. DOE would be authorized to spend $100 million annually through 2025 for research and development of digital defense testing systems and to identify vulnerabilities to known cyber threats. The bill now goes to conference to reconcile differences with H.R.8, which the House approved in December.
- **Aviation.** The Federal Aviation Administration (FAA) reauthorization bill (S.2658) passed 95-3 in the Senate. Among other provisions, the bill requires the FAA to address cybersecurity issues when approving new aircraft designs or modernizing air-traffic control. In the House, FAA reauthorization has advanced out of committee but remains stalled.