WILMERHALE

Cybersecurity: Washington Week in Review, Weeks of February 14 and 27

FEBRUARY 26, 2016

Cybersecurity Information Sharing Act: Implementation Guidance and Future Revisions?

Last Tuesday, February 16, pursuant to mandates under the Cybersecurity Information Sharing Act (CISA), the Departments of Homeland Security, Justice, and Defense (DHS, DOJ, and DoD, respectively) and the Office of the Director of National Intelligence (ODNI) released several key guidance documents concerning cybersecurity information-sharing: (i) DHS/DOJ information-sharing guidance for non-federal entities; (ii) DHS/DOJ interim operational procedures for federal government receipt of information; (iii) ODNI/DHS/DoD/DOJ information-sharing guidance for federal entities; and (iv) DHS/DOJ interim privacy and civil liberties guidance.

On Wednesday, February 24, Secretary of Homeland Security Jeh Johnson said "it's too early to tell" whether CISA's liability protections were effective, while testifying before the House Appropriations Committee. Secretary Johnson also told the committee that Einstein 3-Advanced, the next generation of the DHS-run intrusion prevention system, will cover all federal agencies before he leaves office.

Also on Wednesday, Brett DeWitt, a Republican aide on the House Homeland Security Committee staff, while speaking on a panel discussion hosted by the Financial Services Roundtable, acknowledged that CISA is "not a perfect bill," and expects "kinks to be worked out" as soon as this year. The committee will likely hold hearings around May on CISA's implementation, and then produce a technical corrections bill. At the same event, Edward Roback, who works on critical infrastructure protection at the Treasury Department, acknowledged that the initial guidance issued this week was on a short timeline that didn't allow for "what [the government] would normally do in terms of an extensive consultative process," and pledged to consult more with industry executives for later versions.

SEC: Breached Companies Could See Enforcement Actions

Last Friday, February 19, Stephanie Avakian, deputy director for the SEC's Enforcement Division (and former WilmerHale partner), warned that companies withholding information about data breaches could get hit with civil and criminal enforcement actions from the agency. Speaking at the

Practice Law Institute's annual SEC Speaks event, Avakian said that the SEC is looking to bring more enforcement actions against companies that don't come forward when they become aware of a breach.

"We see a spectrum of cyber awareness and attention and some firms essentially have nothing, so this is something we have to look at," Avakian said. "We understand it may be difficult to assess the nature of a situation, these situations are fluid and core facts can change," Avakian added, but noted that the enforcement division would act where it felt companies violated their duties. She also said that the division wants firms to involve law enforcement when it's appropriate, rather than hide breaches for fear of an investigation. "All of us, both the public and the private sectors, want the same thing to protect our financial infrastructure from hacking, to protect customer data and present accurate information to the market," she said.

While the SEC has not yet brought a case against a company for failing to disclose a breach, Avakian said it was possible in the future, though acknowledged it would require a "significant disclosure failure" for enforcement to be warranted.

More Problems at OPM

The Office of Management Personnel (OPM) has faced a slew of problems over the last couple weeks. First, shortly after Acting OPM Director Beth Cobert's nomination was voted out of committee, it was revealed that the OPM Inspector General (IG) recently determined that she was legally barred from serving as Acting Director while her nomination was pending. According to the IG, the Federal Vacancies Reform Act generally restricts officials from serving as acting heads of agencies while their presidential nominations to hold the job permanently are pending if they haven't served as "first assistant" to that office within a year of the position becoming vacant. But Senate Homeland Security Committee Chair Ron Johnson (R-WI) said that the administration's "failure to follow the law" in appointing Cobert doesn't change his position as to her qualification, but that the Senate should still not move forward on a vote until the House Oversight Committee receives the documents it subpoenaed.

Then, on Monday, February 22, the House Oversight Committee announced that Donna Seymour, OPM's Chief Information Officer (CIO), would be testifying on Wednesday at a hearing on the OPM breach. However, the hearing was promptly cancelled hours later when Committee Chair Jason Chaffetz (R-UT) announced that Seymour had resigned. According to Seymour, she decided to resign because she felt "it is in the agency's best interest that [her] presence does not distract" from the agency's work. Rep. Chaffetz called Seymour's exit "good news and an important turning point" for OPM, noting that her retirement—which he had called for on a number of occasions—was "necessary and long overdue." Oversight Committee Ranking Member Elijah Cummings (D-MD) blasted Republicans for scapegoating Seymour in the wake of the data breach.

On Thursday, February 25, Senator David Vitter (R-LA) officially blocked Cobert's nomination, not because of the breach or the Federal Vacancies Reform Act issue or the outstanding subpoenaed documents, but because he is waiting for a response to a letter he sent Cobert earlier this month regarding an OPM rule that allows members of Congress and Hill staffers to receive small

business subsidies to help pay for health insurance procured on the exchange.

Also on Thursday, the House Oversight Committee held a hearing on security clearance reform. Cobert testified that the National Background Investigations Bureau, the new office being established to manage background investigations, should be operating by October, though further implementation activity will remain ongoing. During the hearing, Rep. Cummings called Vitter's blocking of Cobert's nomination "outrageous." And, despite Rep. Chaffetz's repeated criticism over the outstanding subpoenaed documents, he pledged on Thursday to join Rep. Cummings to write a letter to Senate leaders to urge confirmation, calling Cobert "a breath of fresh air who actually has competency to run this agency."

House Homeland Security Subcommittee Holds Hearing on Emerging Cyber Threats

This Thursday, the House Homeland Security's cybersecurity subcommittee held a hearing on emerging cyber threats. Subcommittee Chair John Ratcliffe (R-TX) criticized the "Administrator's lack of proportional responses to these cyber attacks," which he said "has demonstrated to the world that there are no real consequences for such actions." He continued: "Without a comprehensive national cybersecurity strategy that addresses deterrence effectively, I worry that 2016 could bring an increasing number of those willing to push the boundaries." Full committee Chair Michael McCaul (R-TX) also urged the administration to release the National Cybersecurity Incident Response Plan, which the administration pledged to publish this spring.

Foreign Affairs Update: Iran, Cuba, and China

Last week, a new documentary "Zero Days" revealed that the US developed a plan, code-named "Nitro Zeus," to damage Iranian infrastructure with a cyber attack if nuclear negotiations failed to halt its weapons effort.

This week, US and Cuban government officials held a bilateral meeting on preventing cybercrime and online fraud, the State Department and Cuba's Ministry of Foreign Affairs announced on Wednesday. The US delegation was led by Alexis Torres, assistant deputy associate director of the US Immigration & Customs Enforcement's Homeland Security Investigations unit.

On Thursday, Director of National Intelligence James Clapper testified before the House Intelligence Committee that there had been "some reduction" in Chinese cyber theft since the agreement struck between Presidents Obama and Xi Jinping last fall. However, he said the "jury's out" and "we're [not] in a position today to say whether they're in strict compliance."

Cyber Commission Leadership Announced

Last Wednesday, February 17, White House press secretary Josh Earnest announced that former National Security Adviser Tom Donilon will lead the newly-created National Cybersecurity Commission. Sam Palmisano, former CEO of IBM, will serve as vice chairman.

Department of Education CIO to Resign

Education Department CIO Danny Harris, will retire at the end of the month. Harris faced heavy

scrutiny during a hearing earlier this month that focused on possible ethics violations, and the department's gaps on cybersecurity. Department press secretary Dorie Nolt said Harris has previously considered retiring, but decided to stay on to improve cybersecurity at the department. "Having made significant progress in recent months towards the department's cybersecurity goals, and because he did not want to risk becoming a distraction to the department's critical ongoing cybersecurity work, Danny has decided that now is the right time for him to retire and explore opportunities outside the department," Nolt said. "We are grateful to Danny for his decades of service and wish him and his family well in their future endeavors."

Sector-Specific Updates:

- ***Government Agencies and Contractors.*** The National Institute of Standards and Technology plans to update Special Publication (SP) 800-53 this year, according to a newly-published pre-draft call for comments. NIST SP 800-53, which has not been revised since April 2013, provides security control requirements for federal agency systems. Comments on the revision are due April 1.