WILMERHALE

Cybersecurity: Washington Week in Review, Week of February 7

FEBRUARY 12, 2016

In this week's review:

Obama Budget Request Supports Cybersecurity National Action Plan

On Tuesday, February 9, President Obama released a "Cybersecurity National Action Plan" backed by a $19 billion cybersecurity spending request in the newly-released administration FY17 budget proposal. The budget request, which represents a 35% increase in cyber spending over FY16, includes:

- $3.1 billion to help federal agencies update outdated systems, through a revolving fund managed by the General Services Administration, which will loan money to agencies to install new systems;
- $471 million to support the deployment of DHS's "Einstein" intrusion prevention system at all federal civilian agencies in FY17;
- $275 million to support DHS's Continuous Diagnostics and Monitoring program, which helps agencies identify and respond to risks;
- $62 million to strengthen federal cybersecurity personnel (including through federal loan forgiveness);
- $110 million for the Treasury Department to better protect sensitive financial information (including $62 million for the IRS) while improving cybersecurity cooperation with banks and investment firms; and
- the creation of a federal Chief Information Security Officer ("CISO"), an official with a coordination and policy role rather than an operational role.

The President said he spoke directly with House Speaker Paul Ryan (R-WI) about the cybersecurity funding proposal, saying it was “not an ideological issue” and deserved cross-aisle support. President Obama also stumped for the Cybersecurity National Action Plan in an op-ed in the Wall Street Journal on Tuesday. "The fact is we still don't have in place all the tools we need, including ones many businesses rely on every day," he wrote, adding, "We won't resolve all these challenges over the coming year, but we're laying a strong foundation for the future.” While key congressional leaders from both parties have expressed tentative support for the proposal’s broader goals, whether the provisions will actually pass in an election year with a lame duck President is far from a foregone conclusion.

Industry and cyber experts generally praised the proposal, though some noted more work needed to be done. Justin Harvey, chief security officer at Fidelis Cybersecurity, said "I think that this is the most forward-thinking, down-to-earth plan we've ever seen from a Presidency on cybersecurity." But he questioned whether a new federal CISO would have sufficient authority, and the wisdom of expanding the oft-criticized Einstein program.

"The new budget is a welcome step in the right direction," said Larry Clinton, president of the Internet Security Alliance. "We can't just throw money at the problem. Programs ought to be subjected to systematic cost benefit analysis so that we can document where they are, and are not succeeding."

EO Establishes National Cybersecurity Commission

On Tuesday, President Obama issued an executive order establishing the Commission on Enhancing National Cybersecurity within the Department of Commerce. The Commission will consist of 12 members appointed by the President, including “top strategic, business, and technical thinkers from outside of Government—including members to be designated by the bipartisan Congressional leadership,” according to a White House fact sheet. The Commission will make detailed recommendations, to be implemented over the next decade, for strengthening public and private sector cybersecurity, while protecting privacy, ensuring public safety and economic and national security, fostering development of new technology, and bolstering partnerships between government and the private sector in developing, promoting, and using cybersecurity technologies, policies, and best practices. The Commission is required to report to the White House by December 1, and its recommendations will be made public on January 15, 2017.

IRS Announces it Stopped Data Breach

On Tuesday, the IRS announced that it stopped an effort by criminals to enter its systems and steal refunds. According to the agency, in January, the attempted-hackers used 464,000 previously-stolen Social Security Numbers to successfully generate 101,000 PIN numbers used for electronic filing of returns.

IRS officials said no taxpayer data was compromised in the attempted breach, that it is reaching out to affected taxpayers and taking extra steps to protect their accounts, and that its cybersecurity

experts were investigating the incident. According to the agency, new technology installed following last year's breach interrupted the hack before taxpayer information was compromised. "The ability to...see this attack was ongoing was a direct result of us improving that environment," IRS Chief Technology Officer Terry Milholland told the House Oversight Committee during a previously-scheduled hearing on Wednesday, February 10.

Milholland also said that last week's temporary hardware failure was "with absolute certainty, not a cyberattack." However, House Oversight Committee Chair Jason Chaffetz (R-UT) said that the IRS only disclosed this incident because committee staffers were inquiring about that outage. "This level of incompetence is intolerable for an agency where millions of individuals file their most personal financial information," he said.

"We are in unchartered territory," Senate Finance Committee Chair Orrin Hatch (R-UT) said. "While it appears that the IRS was able to successfully block this attempted breach this time around, it's past time we fundamentally rethink our approach in authenticating taxpayers and processing tax returns." Senator Steve Daines (R-MT) on Wednesday criticized President Obama for not alerting Congress earlier. "The President has a duty to inform Congress of cyber attacks on federal infrastructure, yet once again has tried to sweep this under the rug."

Senate Passes North Korea Sanctions Bill with Cyber Provisions

On Wednesday, the Senate passed the North Korea Sanctions Enforcement Act of 2016 (H.R. 757) by a vote of 96-0. The legislation would require the Obama administration to sanction individuals involved in a number of programs in North Korea, including anyone involved in activities that negatively impact cybersecurity. Penalties would include freezing assets under US jurisdiction, banning individuals from traveling to the United States, and blocking government contracts. The House-passed North Korea sanctions bill, approved by the lower chamber last month, did not include these cyber-related provisions, so the bills will now move to conference.

House Committees Ask State to Renegotiate Cyber Export Control

Last Friday, February 5, leaders from the House Oversight and Homeland Security Committees sent a letter to Secretary of State John Kerry calling for the U.S. to renegotiate limits on the export of cybersecurity products under the Wassenaar Arrangement. "We unambiguously expect that the U.S. Department of State will work to renegotiate the controls at the Wassenaar plenary," the letter said. The letter was signed by the chairs and ranking members of both committees, as well as the Oversight Committee's Subcommittee on Information Technology and Homeland Security Committee's Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies.

Contact Info for DHS and FBI Personnel Hacked

On Sunday and Monday, February 7-8, an anonymous hacker posted the names, titles, and office phone number/email addresses of 10,000 DHS personnel and 20,000 FBI employees. The hacker claims to have obtained the information, which appears to have been stolen from internal

department directories, by compromising a DOJ email account, then tricking a DOJ IT support representative into giving him a token code allowing him to circumvent the agency's multi-factor authentication. Government officials say no sensitive data was compromised in the attack. Later in the week, the website where the information had been posted, indybay[.]org, pulled down the stolen information, and replaced it with a copy of an email from the FBI requesting that it removed.

Nominations

On Wednesday, the Senate Homeland Security committee approved the nomination Beth Cobert for OPM Director by a voice vote.