Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Obama's $19B Cybersecurity Budget Bridges Spending Gap

By **Allison Grande**

Law360, New York (February 9, 2016, 10:38 PM ET) -- The Obama administration on Tuesday revamped its approach to cybersecurity by proposing a lofty $19 billion budget to fund efforts the private sector has long embraced, such as updating antiquated computer systems and creating a security chief post, advancing spending goals that would put the government on more equal footing with private companies in the uphill fight to fortify cyberdefenses.

President Barack Obama elevated cybersecurity's profile in a big way with his most recent budget proposal — his administration's final one — for the fiscal year 2017, in which he requested a 35 percent increase from current funding levels in order to finance projects such as modernizing the government's outdated information technology infrastructure and creating the new position of federal chief information security officer.

"The significant budget increase and creation of the modernization fund are a recognition of what the private sector has already accepted: that cybersecurity will require significant sums of money, and diligence, and effective management," said Rick Martinez, the chair of the privacy and cybersecurity litigation practice at Robins Kaplan LLP.

While the government is hamstrung by funding and policy constraints that generally don't extend to the private sector, the budget request steers efforts to protect federal networks in a new direction that would begin the process of closing the gap between the sectors.

"The private sector is ahead of the government in this space, but this will likely help the government catch up in their ability to protect their systems and improve information security practices," Dechert LLP partner Timothy Blank said.

The White House is pressing its enhanced budget to help finance its cybersecurity national action plan, which it characterized as "the capstone of more than seven years of determined efforts" to enhance cybersecurity awareness and protections and build upon lessons learned from increasingly prevalent cyberthreats and intrusions.

Besides requesting the $19 billion in funds to finance the plan, the president on Tuesday also issued a pair of executive orders that attorneys predict will further strengthen the growing alliance between the public and private sectors.

That partnership was given a significant boost in December, when Congress enacted legislation intended

to facilitate the sharing of information about cyberthreats between the sectors.

The newest executive orders signed Tuesday build upon the foundation laid down in the cybersecurity legislation by creating a pair of groups to enhance the government's capabilities on that front, including a permanent federal privacy council that will bring together privacy officials from across the government to help ensure the implementation of more strategic and comprehensive federal privacy guidelines.

"As a result of the privacy council, we can hope to see a more uniform and coordinated approach to privacy at the federal level, and perhaps an approach that understands privacy and security are two sides of the same coin," said Al Saikali, co-chair of Shook Hardy & Bacon LLP's data security and privacy practice.

Aside from being an immense monetary increase compared with previous years, the 2017 budget proposal also significantly departs from prior White House requests in that it doesn't designate the bulk of its funds for the U.S. Department of Justice, the U.S. Department of Homeland Security and the U.S. Department of Defense to protect other federal agencies.

While the DOJ would see increased funding for cybersecurity-related activities by more than 23 percent and all three regulators would still play a prominent role in the government's cybersecurity regulation, the budget proposal takes the unique approach of setting aside $3.1 billion for the creation of an Information Technology Modernization fund, which would enable a wide range of government agencies to retire, replace and modernize legacy information technology systems that have been in place for decades and have proven to be difficult to secure and expensive to maintain.

"In the past, most of the money in the budget has gone to the protector agencies such as the Defense Department, DHS or DOJ," said Ari Schwartz, a former senior director for cybersecurity at the White House who is now the managing director for cybersecurity services at Venable LLP. "But the breaches at government entities such as the U.S. Postal Service and the State Department and the Office of Personnel Management have taught people that we can't just rely on a few agencies to protect everyone. The agencies also need to protect themselves."

The infusion of cash for information security system enhancements is also likely to send a strong message not only to companies but also to the broader international community about the U.S. government's commitment to combating cyberthreats, attorneys say.

"It's hard for the government to play an enforcer role or to have international credibility when negotiating things like the safe harbor data transfer mechanism and its progeny when its systems are not in a good place from a security standpoint," Blank said. "The federal government's reaction is sending the message that it is looking to become a much more credible leader in the field and take more of a leadership role in protecting corporate information and trade secrets."

The budget proposal also takes cues from the private sector in establishing a federal chief information security officer position within the Office of Management and Budget to oversee cybersecurity policy, planning and implementation across the federal government and pushing to accelerate the government's efforts to move beyond passwords and adopt strong multifactor authentication for access to digital services offered by the government.

"The rules that the government lives by are different than the private sector, but the fact that the government seems to be turning towards some of the best practices that the private sector has already

adopted is important," Crowell & Moring LLP partner Evan Wolff said.

But while the budget proposal and accompanying executive orders will undoubtedly provide a boost to the nation's cybersecurity framework, attorneys caution that gaps will remain, and vulnerabilities are likely to persist.

"No matter how much is spent by the U.S. government on cybersecurity, there will always be an adversary who will find a way to penetrate the defenses," Pillsbury Winthrop Shaw Pittman LLP partner Brian Finch said. "This is a good start and the right move by the Obama administration, but proposing a big budget number by no means guarantees increased security."

— Editing by Mark Lebetkin.