LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
WEDNESDAY, MAY 31, 2017
PERSPECTIVE

Budget calls for cybersecurity funding

By Jennifer Martin

On May 11, President Donald Trump signed an executive order titled Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. On May 22, the White House released its proposed 2018 federal budget which, consistent with the order's goals, generally proposes increased funding to meet the growing challenges of cybersecurity. Specifically, the proposed budget increases resources for Department of Homeland Security (DHS), Department of Defense (DOD) and law enforcement agencies' programs to manage cybersecurity risks. It also establishes a Technology Modernization Fund to invest in updating the information technology (IT) infrastructure of federal agency networks. The funding levels, however, are less than those originally proposed by the previous administration and Congress; moreover, proposed funding for other important initiatives is reduced.

Background

The long-anticipated order on cybersecurity was issued several months after the White House originally planned to release a cybersecurity-focused order on Feb. 1.


JENNIFER MARTIN

The order encourages the use of shared IT services, including cloud services, across agencies; and places reporting and coordination responsibility on the newly formed American Technology Council ... which is currently comprised of government officials, including Trump himself, is part of the White House Office of Innovation led by Jared Kushner.

Trump was expected to sign an executive order on cybersecurity shortly after taking office, but the signing was postponed pending revisions to the draft order after it was widely criticized. The original draft order, titled Strengthening U.S. Cyber Security and Capabilities, articulated a general policy focused on enhancing the nation's cybersecurity defenses and capabilities under the primary direction of the DOD and DHS, in coordination with representatives of the intelligence community. Specifically, the original draft order directed those agencies to review cybersecurity vulnerabilities in national security systems, federal networks, and critical civilian infrastructure systems; identify cyber adversaries; and review key governmental agency's cybersecurity capabilities. It also directed the DOD to conduct a review of the U.S. education system as it relates to building a workforce to meet evolving cybersecurity challenges.

On Feb. 10 a revised draft order was released that differed significantly from the initial draft, particularly with respect to distributing responsibility for managing risks to federal systems to the heads of each of the federal agencies. In this regard, the Feb. 10 revised draft order is generally aligned with, and was a continuation of the initiatives described in, Executive Order 13636, Improving Critical Infrastructure Security, which was signed by President Barack Obama in 2013. The revised draft order focused on cybersecurity risk management of federal agency networks and of critical infrastructures, with particular emphasis on the "core" communications infrastructure, the energy sector and the military industrial base. Like Executive Order 13636, the revised draft order focused on an agency-led, risk-based approach to cybersecurity and, in particular, required federal agencies to adopt the National Institute of Standards and Technology (NIST) "Framework for Improving Critical Infrastructure Cybersecurity" to manage cybersecurity risk.

Executive Order on Cybersecurity

With few exceptions the final executive order mirrors the Feb. 10 revised draft order, and continues to be organized around managing the cybersecurity risks of: federal agency networks, critical infrastructure and the nation.

Cybersecurity of Federal Networks and the American Technology Council

The first section of the order primarily addresses cybersecurity risk management and IT modernization within the executive branch consistent with earlier proposals by the Trump and Obama administrations. Notably, although agency-driven, the order encourages the use of shared IT services, including cloud services, across agencies; and places reporting and coordination responsibility on the newly formed American Technology Council. The council was established on May 1 by executive order with the stated objective of coordinating the "vision, strategy, and direction" of federal government IT modernization efforts. The council, which is currently comprised of government officials, including Trump himself, is part of the White House Office of Innovation led by Jared Kushner.

The executive order further directs each agency to provide a risk management report to the secretary of Homeland Security and the director of the Office of Management and Budget (OMB) within 90 days of the execution of the order. In light of this requirement, on May 19, the director of OMB disseminated a memorandum to the heads of all executive agencies providing order implementation and reporting guidance. The memorandum provides instructions to each agency to satisfy executive order requirements including directions for designating an accountable official, establishing a risk-assessment methodology and reporting process and implementing the NIST Framework. The appendix to the May 19 memorandum contains specific criteria for assessing the adequacy of federal network and system security controls.

Cybersecurity of Critical Infrastructure

The second section of the order focuses on providing federal support to critical infrastructure owners in managing cybersecurity risks. Primary responsibility for this initiative lies with DHS, working in coordination with law enforcement and intelligence agencies. The order focuses on four initiatives, in addition to the objective of providing support:

• promoting appropriate levels of transparency in the marketplace relating to cybersecurity risk management

• improving resilience against botnets and other automated, distributed threats, particularly through the communications and internet service provider ecosystem

• assessing incident response capabilities to respond to disruptions to the electricity sector and

• confronting risks to warfighting capabilities and defense industrial base systems.

Section two of the order now includes a paragraph titled "Resilience Against Botnets and Other Automated, Distributed Threats" that focuses specifically on the threats posed by botnets. Pursuant to the final executive order, the DHS and Department of Commerce (DOC) are directed to "identify and promote action by appropriate stakeholders ... in the internet and communications ecosystem ... with the goal of dramatically reducing threats perpetrated by automated and distributed attacks (e.g. botnets)." Moreover, the final order directs DHS and DOC to work with a much broader group of stakeholders in fulfilling this mandate. While the earlier draft order required DHS and DOC to collaborate only with stakeholders from "core communications infrastructure," the final order requires DHS and DOC to work with stakeholders, including owners and operators, throughout the "internet and communications ecosystem."

Cybersecurity for the Nation

The final section of the order directs various agencies to coordinate on long-term, sustainable efforts to protect the internet and U.S. citizens from cyber threats. In this regard, the order focuses on assessing relevant education and training programs from primary school through higher education. In addition, unlike the earlier drafts, the final order now recognizes the importance of international cooperation and that the United States is "especially dependent on a globally secure and resilient internet and must work with allies and other partners."

Cybersecurity Funding in the 2018 Budget Proposals

As noted previously, the proposed budget released on May 22 generally supports the order's objectives to manage cybersecurity risk and modernize federal IT systems. Of particular note, the White House budget proposes a $196 million increase in funding for DHS's National Protection and Programs Directorate which "leads efforts to protect the nation's critical infrastructure against cyber and physical threats, including terrorist attacks, cyber incidents, natural disasters, and other catastrophic incidents." This increase would provide for a total budget of $3.28 billion for the directorate. The White House proposal also calls for increased funding to support DOD IT infrastructure initiatives and law enforcement efforts, including increases to support additional cybersecurity personnel in DHS, DOD and the FBI to combat cybercrime and respond to attacks.

The budget proposal also establishes and funds a newly created Technology Modernization Fund, designed to be a "full cost recovery revolving fund that finances the transition of Federal agencies from antiquated IT legacy systems." The underlying assumption is that the fund will be self-funded as old systems are replaced with more cost-effective and shared solutions, including cloud-based platforms, resulting in a return on an investment that offsets the costs of modernization. The proposed budget provides for a $228 million initial allotment for the fund.

The proposed budget increases for IT investment, however, are in general less than those previously proposed to support modernization efforts. In particular, the proposed $228 million fund, which is specifically established to align with funding under the Modernizing Government Technology Act legislation, is less than the $250 million fund proposed by the House bill, which passed on May 1. Moreover, in his 2017 budget proposal, President Obama requested $3.1 billion for a new IT modernization fund to be run by the General Services administration.

Finally, although the executive order calls for increased efforts to educate and train a cyber-ready workforce, and the continued development of sustainable information sharing, deterrence and preventative measures, programs supporting education and research and development, including the critical work by NIST to develop cybersecurity standards, face significant acrossthe-board cuts.

Jennifer Martin *is of counsel in Covington's Silicon Valley office and leads the firm's West Coast Cybersecurity practice. She can be reached at jrmartin@cov.com.*

COVINGTON