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

Highlights Of Obama's Ambitious New Cybersecurity Plan

Law360, New York (February 10, 2016, 5:47 PM ET) --

Evan D. Wolff

This week, President Obama directed his administration to implement a cybersecurity national action plan (CNAP) with near- and long-term steps to improve both public and private sector cybersecurity. The president's fiscal year 2017 budget proposes spending $19 billion on CNAP initiatives, a 35 percent increase in cybersecurity spending over his FY 2016 budget. The CNAP places significant focus on the private sector's role in securing the nation's cyber borders and, in many ways, draws heavily on the private sector's experience with cyber resilience and an enterprise-wide, multiyear approach to cybersecurity.

As with earlier public/private initiatives, the CNAP contemplates voluntary activities and does not impose cybersecurity obligations on the private sector. Relevant highlights from the CNAP include:

Expanding Support for Critical Infrastructure

The CNAP extends prior federal efforts to strengthen voluntary partnerships with private companies that own and operate key resources and assets and that provide products and services critical to the nation's day-to-day life. These efforts include: (1) creating the National Center for Cybersecurity Resilience, where private companies can test their system security in a controlled environment before deploying to the real-world; (2) doubling the number of advisors available to assist critical infrastructure with cybersecurity assessments and best practices; (3) creating the Cybersecurity Assurance Program to test and certify connected devices within the Internet of Things that meet threshold security standards; and (4) urging health care stakeholders to develop and refine their data security practices.

Improving Cyberhygiene

The CNAP calls for Americans to move beyond basic passwords and instead take advantage of the increased protection provided by multifactor authentication (MFA). The administration will kick off a public awareness campaign and work in coordination with technology and financial services companies to make MFA technology accessible and to help individual Americans understand their role in protecting the nation's cybersecurity. Separate efforts will be made to further the president's "BuySecure" initiative that focuses on chip-and-PIN payment systems and to promote the Federal Trade Commission's IdentityTheft.Gov resource for victims of identity theft. The CNAP additionally calls on federal agencies to use MFA, adopt identity proofing practices, and further reduce their reliance on social security numbers.

Enhancing Cyberincident Response

Acknowledging the volume of U.S. cyberincidents experienced over the last year, the CNAP calls for maintaining resilience when incidents occur, in addition to focusing on prevention and deterrence. By this spring, the administration will release a policy for national cyberincident coordination. The policy will be accompanied by a methodology for evaluating the severity of cyberincidents to enable government agencies and the private sector to communicate effectively and provide an appropriate and consistent level of response when incidents occur.

Establishing the Commission on Enhancing National Cybersecurity

The commission will consist of 12 cybersecurity experts — all from outside of the federal government — who will be charged with crafting recommendations for government activities over the next decade to improve public and private cybersecurity while protecting privacy.

Modernizing Government IT and Governance

The CNAP directs federal agencies to begin retiring, replacing, and modernizing outdated information technology infrastructure, with the assistance of a $3.1 billion "IT Modernization Fund," which departs from the traditional federal model of year-end, lump-sum IT funding in favor of strategic and long-term agency investments in modernization. At the same time, agencies would transition to a shared-services, governmentwide approach to IT that would permit agencies to benefit from each other's experiences and move toward standardized cybersecurity practices. The CNAP creates the position of federal chief information security officer, who will report to the federal chief information officer and will be exclusively focused on developing, managing, and coordinating federal cyber strategy.

Developing Cybersecurity Technology and Workplace Skills

The CNAP also incorporates the National Science and Technology Council's 2016 Federal Cybersecurity Research and Development Strategic Plan for evidence-based improvements in cybersecurity technology, and identifies a number of cybersecurity education and training initiatives to develop the cybersecurity expertise that federal agencies will need to follow through on improving their cybersecurity.

The CNAP builds on recent federal efforts to enhance the country's cybersecurity posture, including proposed guidance for implementing cyber protections in federal acquisitions, President Obama's public-private sector cybersecurity information sharing executive orders, the National Institute of Standards and Technology's cybersecurity framework, and a cybersecurity strategy and implementation plan for agencies to identify and address their cybersecurity gaps. Significantly, much of the CNAP as applied to federal agencies reflects lessons learned and best practices already in place in the private sector, and thus is an important step toward bringing federal cybersecurity practices more in line with their private sector counterparts.

As the end of the president's term approaches, the CNAP is an ambitious and consistent next step in this administration's series of cybersecurity initiatives, but it is by no means a quick or light undertaking. To succeed, the CNAP requires a long-term commitment from the next administration, federal agencies, and the Hill, not to mention a $19 billion infusion from the House of Representatives.

—By Evan D. Wolff, Maida Oringher Lerner, Peter B. Miller, Kate M. Growley and Matthew B. Welling, Crowell & Moring LLP

Evan Wolff is a partner in Crowell & Moring's Washington, D.C. office, co-chairman of the firm's privacy and cybersecurity group and a former adviser to senior leadership at the U.S. Department of Homeland Security. Maida Lerner is senior counsel in the firm's Washington office. Peter Miller is senior counsel in the firm's Washington office and former chief privacy counsel at the Federal Trade Commission. Kate Growley and Matthew Welling are associates in the firm's Washington office.