wiley

ALERT

POTUS Launches Significant Cybersecurity and Privacy Initiatives

February 9, 2016

On February 9, President Obama initiated a number of consequential actions on cybersecurity. The initiatives range from establishing by Executive Order a new Federal Privacy Council made up of senior privacy officials from two dozen agencies that will improve federal privacy protections for individuals, to creating a comprehensive Cybersecurity National Action Plan that will encompass a long-term, strategic assessment of cybersecurity in the 21st century.

Several federal agencies also have been looking at and acting on critical issues related to cybersecurity; some appear to be inching toward oversight or regulatory efforts aimed at assessing use or compliance with the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Notable components of the President's initiatives include:

- Creating a Commission on Enhancing National Cybersecurity that draws from the private sector to make recommendations by year end to improve cybersecurity awareness and practices and foster new technologies;
- Funding significant financial investments in government information technology and cybersecurity efforts beginning in the next fiscal year;
- Establishing the Federal Chief Information Security Officer to lead and coordinate the various new programs and efforts; and
- Harnessing private initiatives to help secure personal data online through multifactor authentication and other methods, to be spearheaded in a new National Cybersecurity Awareness

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Nova J. Daly
Senior Public Policy Advisor
202.719.3282
ndaly@wiley.law

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

Campaign focused on consumers.

These efforts are further evidence of the urgency with which the government is looking at the private sector's approach to cybersecurity and the operations put in place to safeguard digital information and protect against cybersecurity vulnerabilities. The President's actions today build on previous Executive Orders like Executive Order 13636, creation of the voluntary Cybersecurity Framework by NIST, and successful passage of the Cybersecurity Enhancement Act of 2014 and the Cybersecurity Information Sharing Act of 2015. In addition, the Office of Management and Budget (OMB) released proposed guidance designed to take "major steps" to improve cybersecurity in federal acquisitions in August 2015.

Important questions remain concerning the implementation of many of these recent federal efforts. NIST is evaluating the use and role of its Cybersecurity Framework in protecting critical infrastructure. The Department of Homeland Security (DHS) and other agencies are just beginning to implement the terms of The Cybersecurity Act of 2015, and the federal government is trying to improve communication through Information Sharing and Analysis Organizations. We expect one critical program, the Protected Critical Infrastructure Information (PCII) regime, administered by DHS, also to be revisited this Spring. Some states also have expressed interest in private sector cyber preparedness, further complicating the landscape.

In today's effort, President Obama is also requiring agencies to identify and prioritize their highest value and most at-risk IT assets and then take additional concrete steps to improve their security. Whether such steps result in procurement obligations or regulation more broadly remains to be seen.

The private sector should follow the progress of these initiatives and related developments to be aware of the government's expectations and their implications to U.S. business, security, and investment.