wiley

ARTICLE

Executive Order: Cybersecurity Information Sharing

February 18, 2015

Friday, President Obama issued an Executive Order, *Promoting Private Sector Cybersecurity Information Sharing* (EO), designed to help companies rapidly share information related to cyber threats with the government and each other. This is another step in a line of actions the President has taken on cybersecurity, shaping the federal government's response in the wake of cyberattacks against the federal government, as well as major companies such as Sony, Home Depot Inc., and Anthem Inc. The EO was released on the heels of Friday's White House Summit on Cybersecurity and Consumer Protection, which gathered business leaders, experts, and advocates involved in the cybersecurity and consumer protection landscape to discuss and promote best practices and next steps.

The Executive Order Promotes Venues for Information Sharing

This EO focuses on improving information-sharing, which industry and others believe is critical to better enable attack prevention and response. To that end, the EO promotes the formation and use of information sharing and analysis organizations (ISAOs) as coordination points for sharing cyber threat information between companies and with the federal government. Many industry sectors already successfully employ Information Sharing and Analysis Centers (ISACs) for this purpose. The EO makes clear that ISACs could be considered ISAOs, and encourages additional sectors and types of organizations to employ this model. The EO directs the Department of Homeland Security (DHS) to create a non-profit entity to develop a common set of voluntary standards for the operation of ISAOs, which will be subject to a public review and comment process. These standards shall address, but not be limited to, contractual agreements, business processes, operating procedures, technical

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Privacy, Cyber & Data Governance
Telecom, Media & Technology
Uncrewed Aircraft Systems (UAS)

means, and privacy protections for ISAO operation and ISAO member participation.

The EO seeks to improve and speed information-sharing with the private sector through the use of ISAOs in two ways. First, the EO improves the means by which the National Cybersecurity and Communications Integration Center enters into information-sharing agreements with ISAO. Second, the EO will ease the approval process for ISAOs to be able to access classified cybersecurity information from the government.

The EO also sets forth important privacy protections. The EO will require ISAOs to abide by voluntary privacy standards, which will include privacy protocols, such as minimization, for ISAO operation and member participation. In addition, agencies collaborating with ISAOs will work with their senior officials for privacy and civil liberties to ensure that appropriate privacy protections are in place.

The EO is Part of Ongoing Cyber Activity at the Federal Level

This EO is the most recent in a series of Executive Branch activities on cybersecurity. In February of 2013, the President issued an Executive Order, *Improving Critical Infrastructure Cybersecurity*. That EO resulted in a voluntary, risk-based Cybersecurity Framework for critical infrastructure, developed by the National Institute of Standards and Technology (NIST).

Many federal agencies are taking action on cyber. DHS is implementing programs to encourage industry to work on cybersecurity, and other federal agencies, from the Food and Drug Administration to the Federal Communication Commission, are studying the NIST Cybersecurity Framework and considering how the private sector is using it. Myriad federal agencies are actively examining cyber security issues in a variety of contexts.

These and other Executive Branch activities occur as Congress continues to refine and consider legislative solutions, including those proposed by the President. The President highlighted cybersecurity issues in his 2015 State of the Union address, and in January he sent several cybersecurity-related bills to Congress. The White House recently announced the creation of a Cyber Threat Intelligence Integration Center, to help review and synthesize cyber threat information.

Given the passage of cybersecurity legislation in the House, and emerging consensus on some issues in the Senate, observers are optimistic that legislation could pass this year.