msk

president obama issues executive order promoting private sector cybersecurity information sharing

MSK Client Alert

February 17, 2015

On Friday, February 13, 2015, President Obama signed an executive order, *Promoting Private Sector Cybersecurity Information Sharing* (the "EO"), designed to encourage private companies to share information regarding threats to cybersecurity across private sector industries and with the federal government. The EO was signed almost exactly two years after Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, and one year after publication of the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity ("NIST Framework"). Similar to the NIST Framework, the EO does not impose mandatory requirements on the private sector, but rather is designed to encourage information sharing through providing a set of robust protections from public disclosure. Also similar to the NIST Framework, it is expected the best practices this new EO is intended to create will become the norm and so standards that all companies regardless of size or industry will need to implement.

Enacted as part of the Homeland Security Act of 2002, the Critical Infrastructure Information Act of 2002 created a framework that enables the private sector to voluntarily submit "critical infrastructure information" to the Department of Homeland Security (DHS) with the assurance such information, among other protections, cannot be used by agencies for regulatory enforcement purposes, will be subject to a special exemption from disclosure under the Freedom of Information Act (FOIA), and cannot be used by any federal or state agency in civil court proceedings. The term "critical infrastructure information" is broadly defined as information not customarily in the public domain and related to the security of critical infrastructure or protected systems, and is expected to include general technical data, such as information regarding zero day vulnerabilities, malware, harmful IP addresses, domains, or filenames. Much of the critical infrastructure in the U.S. (cargo terminals, banking systems, bridges, railroads, etc.) is owned by the private sector. Congress is yet to pass a

attorneys

Susan Kohn Ross

practice areas

corporate & business transactions

cybersecurity and privacy

international trade

comprehensive federal law on point, so it was not unexpected the President would call for yet another set of voluntary standards as an inducement to improve the cybersecurity safeguard mechanisms currently in place, fostering cooperation across various private sector industries. The fact that almost every week another successful intrusion is widely reported in the general press only added pressure to seek solutions which shore up the current protections to business operators and their customers.

Although the EO does not define particular cybersecurity threat information as "critical infrastructure information", it directs the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) to enter into "voluntary agreements" with Information Sharing and Analysis Organizations (ISAOs) "in order to promote critical infrastructure security with respect to cybersecurity." ISAOs include nonprofit and for-profit entities organized for purposes of gathering, analyzing, communicating, disclosing and voluntarily disseminating their members, whether private sector or government entities, in order to better understand security problems and interdependencies related to critical infrastructure and protected systems. The EO further directs the DHS Secretary to enter, through an open and competitive process, into an agreement with a nongovernmental organization to serve as the ISAO Standards Organization, which is tasked to identify a common set of voluntary standards or guidelines for the creation and functioning of ISAOs under the EO.

Notably, the framework and the purpose of the EO track a bill introduced two days earlier by U.S. Sen. Tom Carper, D-Del., the Cyber Threat Sharing Act of 2015. See Cyber Threat Sharing Act of 2015. As with the EO, this bill seeks to improve cybersecurity for private businesses and the federal government by authorizing the sharing of threat data between the NCCIC and certified analysis and information sharing organizations.

Again, the key word of the EO remains "voluntarily," and — at least for now — the government continues to use a carrot, rather than a stick, to gain private companies' cooperation. That said, the EO's framework is likely to represent yet another new "best practices" standard that will cause companies a dilemma – will companies have any choice but to incorporate these new "voluntary standards" as standard operating procedures? Given frequent headlines about the massive theft of personally identifiable information and the publication of otherwise business proprietary and sensitive data, cybersecurity policies will no doubt remain at the forefront of compliance measures for all companies, regardless of size or industry.