Client Alert

pillsbury

Cybersecurity

International Trade Public Policy April 22, 2015

New Executive Order Allows for Sanctions Related to Cybersecurity

By Brian E. Finch, Nancy A. Fischer, Aaron R. Hutman, Aimee P. Ghosh and Stephanie J. Rohrer

On April 1, 2015, President Obama issued a groundbreaking Executive Order (E.O.) enabling the United States to sanction persons that have (1) participated in malicious cyber-enabled activities constituting a "significant threat to the national security, foreign policy, or economic health or financial stability of the United States," or (2) misappropriated trade secrets for commercial or financial gain outside the United States. No sanctions have yet been imposed and it is unclear how the U.S. government will deploy this new regime. Nonetheless, applying economic sanctions to the U.S. cybersecurity response is a potentially powerful tool that can fill gaps in law enforcement and deterrence. It also is a tool that could be leveraged by companies that have fallen victim to damaging cyber-attacks or competitors using stolen trade secrets. Further, companies outside the United States will need to consider compliance measures to manage exposure to sanctions under these new rules.

Overview of the Executive Order

Executive Order 13694 targets significant, malicious "cyber-enabled" activities that have the purpose or effect of causing specific harms to security, infrastructure and business interests. It intends to enable the U.S. government to address malicious cyber actors outside of the United States who have traditionally hidden beyond the reach of other enforcement tools.

Specifically, the E.O. allows the Secretary of Treasury, in consultation with the Attorney General and the Secretary of State, to designate persons for certain activities wholly or substantially outside the United States which result in or contribute to "a significant threat to the national security, foreign policy, or economic health or financial stability of the United States." This includes two categories of activities:

(1) **Cyber-attacks** that have the purpose or effect of:

- Harming or compromising computers/computer networks supporting critical infrastructure entities;
- Compromising the provision of services by critical infrastructure entities; or
- Disrupting the availability of a computer/computer network (e.g., denial of service attacks).

(2) **Cyber-crime and commercial benefit from such crime**, specifically:

- Misappropriating funds, trade secrets, personal or financial information for commercial advantage or private financial gain; and
- Responsibility for, complicity in or engaging in the receipt or use of trade secrets for commercial or competitive advantage, private financial gain, or receipt/use by a commercial entity outside the United States which were misappropriated through cyber-enabled means, where knowing they were misappropriated.

Sanctions also may be applied to persons who materially assist, sponsor, or provide material financial, technological, or goods-and-services support for any of the activities described above or for any party blocked under the E.O. Thus, this order threatens not only primary actors but anyone operating within the global cyber ecosystem that may support or supply cyber-attackers, terrorists or thieves.

A sanctions designation by the Office of Foreign Assets Control (OFAC) under this E.O. blocks the parties' assets, likely via listing as a Specially Designated National or "SDN," which freezes the property and interests in property of the listed person that are or come within the United States, or the possession of a U.S. person, and bans the person from traveling to the United States. No designations have been made at this time.

OFAC issued frequently asked questions numbers 444 to 452 together with the E.O. which provide important definitions and clarify some limitations of the intended application of the sanctions:

- The anticipated definition of "cyber-enabled" includes "any act that is primarily accomplished through or facilitated by computers or other electronic devices." The "malicious cyber-enabled activities" targeted by the E.O. include "deliberate activities accomplished through unauthorized access to a computer system, including by remote access; circumventing one or more protection measures, including by bypassing a firewall; or compromising the security of hardware or software in the supply chain." (FAQ 447)

- "Critical infrastructure sector" means any of the following sectors: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; and Water and Wastewater Systems. (E.O. Section 6(d), Presidential Policy Directive 21 and FAQ 447)

- This E.O. does not target cyber-related activities for legitimate educational, network defense, or research purposes. Similarly, legitimate network defense or maintenance activities performed by computer security experts and companies as part of their normal business operations are also not targeted by the E.O. (FAQs 448-450)

Practical Effects for Companies

Initial reports indicate that the Obama administration intends to use this E.O. in a careful and limited fashion, but given the nature of the challenge, it may evolve in a variety of ways. It also is unclear how future Presidents may use the regime. Companies should carefully consider both (a) how the new cyber-sanctions can be a path to address attacks and unfair competition, and (b) how to pursue cyber-compliance to ensure the sanctions do not target them.

Recourse for Cyber-victims. Companies (especially those in the financial, health care, energy, or defense industries) that are victims of cyber-attacks may consider seeking relief under this sanctions regime. Where traditional law enforcement, civil, intellectual property, trade and other remedies fail to stop or recover from cyber criminals, sanctions under the new E.O. may offer U.S. companies an additional form of response for malicious cyber-attacks and wrongful use of trade secrets. This response would involve policy outreach and deployment of sanctions strategy in Washington, DC. Such outreach would be tactical, confidential and low profile in most cases. There is some potential that countries of persons designated under this executive order may look at retaliatory options, and so a potential defense strategy would also be needed.

Protect against being a sanctions target. Companies outside of the United States which are at risk of being accused of cyber-misconduct, cyber-espionage or coordinating with persons or governments alleged to have stolen trade secrets should consider proactive steps in order to minimize sanctions risk. There are a number of compliance steps used in other contexts to address sanctions risk which may apply here and can be tailored to cyber concerns. For example, companies might issue formal statements by senior management proscribing cyber-misconduct or knowing use of stolen trade secrets; and publish compliance programs to emphasize that cyber-misconduct reflects rogue activity of employees and not company policy or intent. Companies that deal in intellectual property may consider enhanced due diligence on new information and its sources. Companies that supply goods or software which could be misused in cyber activities also should consider their risk, given the application to persons providing material support.

If you have any questions about the content of this alert, please contact the Pillsbury attorney with whom you regularly work, or the authors below.

Brian E. Finch (bio)
Washington, DC
+1.202.663.8062
brian.finch@pillsburylaw.com

Nancy A. Fischer (bio)
Washington, DC
+1.202.663.8965
nancy.fischer@pillsburylaw.com

Aaron R. Hutman (bio)
Washington, DC
+1.202.663.8341
aaron.hutman@pillsburylaw.com

Aimee P. Ghosh (bio)
Washington, DC
+1.202.663.8091
aimee.ghosh@pillsburylaw.com

Stephanie J. Rohrer (bio)
Washington, DC
+1.202.663.8009
stephanie.rohrer@pillsburylaw.com

About Pillsbury Winthrop Shaw Pittman LLP

Pillsbury is a full-service law firm with an industry focus on energy & natural resources, financial services including financial institutions, real estate & construction, and technology. Based in the world's major financial, technology and energy centers, Pillsbury counsels clients on global business, regulatory and litigation matters. We work in multidisciplinary teams that allow us to understand our clients' objectives, anticipate trends, and bring a 360-degree perspective to complex business and legal issues—helping clients to take greater advantage of new opportunities, meet and exceed their objectives, and better mitigate risk. This collaborative work style helps produce the results our clients seek.