KING & SPALDING

Client Alert

Data, Privacy & Security and International Trade & Litigation Practice Groups

April 9, 2015

New Executive Order Authorizes Economic Sanctions to Combat Malicious Cyber Activity

Calling cyber threats "one of the most serious economic and national security challenges to the United States" and declaring a national emergency relating to those threats, on April 1, 2015, President Obama issued an Executive Order "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activity." [1] The Executive Order is part of the U.S. Government's effort to combat widespread cyber theft from the networks of public and private organizations. Former National Security Agency Director Keith Alexander previously stated that these widespread cyber thefts "represent the greatest transfer of wealth in human history." [2]

The Executive Order Provides a Broad, Flexible Tool

The Executive Order authorizes sanctions on individuals or entities that are responsible for, complicit in, or engage in malicious cyber-enabled activities originating or directed from abroad.[3] The cyber-enabled activities must significantly threaten the national security, foreign policy, or economic health or financial stability of the United States.[4] In addition, the cyber-enabled activities must have the purpose or effect of

- harming or significantly compromising the provision of services by an entity in a critical infrastructure sector;

- causing significant disruption to the availability of a computer or network of computers (for example, through a denial of service attack);

- causing significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain;

- knowingly receiving or using trade secrets misappropriated through cyber-enabled means for commercial or competitive advantage or private financial gain (for example, a corporation that knowingly profits from stolen trade secrets); or

- materially assisting, sponsoring, or providing financial, material, or technological support for any of the above activities.[5]

For more information, contact:

Phyllis B. Sumner
+1 404 572 4799
psumner@kslaw.com

Christine E. Savage
+1 202 626 5541
csavage@kslaw.com

Jeffrey M. Telep
+1 202 626 2390
jtelep@kslaw.com

Nicholas A. Oldham
+1 202 626 3740
noldham@kslaw.com

Kerianne Tobitsch
+1 212 556 2310
ktobitsch@kslaw.com

Elizabeth E. Owerbach
+1 202 626 9223
eowerbach@kslaw.com

King & Spalding
Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500
Fax: +1 202 626 3737

www.kslaw.com

The Executive Order sanctions both the "supply side" of cyber thefts—hackers and their sponsors—as well as the "demand side"—the recipients or beneficiaries of stolen information.[6]

The President issued the Executive Order based primarily on his authority under the International Emergency Economic Powers Act (50 U.S.C. § 1701 et seq.) and the National Emergencies Act (50 U.S.C. § 1601 et seq.), pursuant to which the President may authorize a variety of regulatory actions to address foreign threats. The Executive Order delegates to the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, the authority to promulgate rules and regulations and to take any other action required to implement the Executive Order.[7] Finally, the Executive Order authorizes a visa ban for those targeted by the sanctions.[8]

What Those Combating Cyber Threats Should Know

The Executive Order is the first to directly address malicious cyber threats without targeting a particular country or group. Significant issues might arise when implementing the Executive Order, and the resolution of those issues will drive the long-term effectiveness of the new sanctions regime. Below is our list of the most significant issues.

What will these sanctions entail, and when will they be implemented?

The sanctions authorized by this Executive Order would freeze the assets of individuals and entities specifically named by Treasury, in consultation with the Attorney General and Secretary of State.[9] It is unclear when the Administration will actually use this new authority. Unlike several other sanctions programs, no designations were issued with the Executive Order to sanction any individuals or entities, and as of publication the Administration has not named such parties. According to Special Assistant to the President and Cybersecurity Coordinator Michael Daniel, the Administration does not have "any particular timeline" for when parties will be named under this program.[10]

Going forward, the Office of Foreign Assets Control (OFAC), U.S. Department of Treasury, has the authority to coordinate with other agencies and determine which parties should be targeted under the Executive Order. OFAC will then add any designated entities to its list of Specially Designated Nationals ("SDN List").[11] Under the Executive Order, OFAC also has authority to issue any rules and regulations necessary to implement the program, although it is unclear when OFAC plans to issue such regulations.[12] John Smith, Acting Director of OFAC, stated that anyone sanctioned under the Executive Order will be able to challenge their designation through an administrative petition or by filing suit in federal court. [13]

Some have already inquired as to how this new authority will relate to other sanctions regimes. In January 2015, after the attack on Sony Pictures, the President issued an Executive Order imposing targeted sanctions on North Korean entities, based in part on the "coercive cyber-related actions during November and December 2014[.]"[14] Mr. Smith clarified that the April 1 Executive Order serves a different purpose. While the North Korea sanctions are jurisdictional and primarily target North Korean government officials, the authority under the new Executive Order is global. Like current counter-narcotics and counterterrorism sanctions, the new Executive Order will enable the United States to target illicit foreign activity "wherever it arises."[15]

Mr. Smith indicated that while the new sanctions tool is "powerful," it is intended to be used "judiciously and in extraordinary circumstances."[16] It remains to be seen just what circumstances will motivate the Administration to take that step. While the Administration has not yet sanctioned any parties under the new Executive Order, OFAC has encouraged "firms that facilitate or engage in online commerce" to develop "tailored, risk-based compliance program[s]" as a general practice.[17]

What activities will trigger the sanctions?

Determining which cyber activities are targeted by the sanctions will be difficult. It is well accepted that malicious cyber activity occurs daily. The Executive Order suggests that the cyber activities to be targeted could be measured in terms of harm to consumer privacy, commercial competitive advantage, or certain sectors, particularly the critical infrastructure sector, but it is unclear what degree will be considered significant. For example, the Executive Order does not describe the size of economic damages or the type of misappropriated trade secrets that would be sufficient to trigger sanctions. As of yet few guidelines or precedents guide the use of this new authority. Given that the Executive Order intends to create a high bar for the type of malicious cyber activities that are sanctionable, and the sanctions only address malicious activities after they cause harm, practitioners should continue to review their data security policies and ensure they have in place reasonable security measures to protect sensitive information.

Who are the likely targets?

Determining which individuals or entities will be targeted with sanctions will also be difficult. The Executive Order authorizes sanctions on individuals or entities that are "responsible for, complicit in, or have engaged in, directly or indirectly, malicious cyber-enabled activities" that significantly threaten "the national security, foreign policy, or economic health or financial stability of the United States." This scope appears exceedingly expansive, authorizing sanctions in areas not traditionally thought of as national security, such as the economic competitiveness of private organizations. The Executive Order, however, does not define the key terms although the Administration has indicated that those terms will be broadly defined. For example, OFAC has hinted at forthcoming definitions, stating that "malicious cyber-enabled activities 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."[18] Moreover, malicious cyber activities are exceptionally difficult to attribute. Hackers, for example, have rapidly evolving technology arsenals, purposefully obscure their identities, and can leave digital fingerprints anywhere the Internet reaches.

Recognizing these concerns, the Administration stated that it will target only the "worst of the worst," that sanctions will not "target free speech or interfere[] with the free and open Internet," are "not designed to police the Internet or stifle technological innovations," and are "not meant to protect any one individual U.S. company." [19] In addition, Mr. Smith stated that the standard of evidence will be a "reasonable basis to believe or reasonable cause to believe," which is the "basic standard of evidence that administrative agencies across the government use under the Administrative Procedure Act[.]"[20] It is unclear how this standard will be applied to evidence attributing malicious cyber-enabled activities to particular actors.

King & Spalding will continue to monitor developments with regard to the new Executive Order and will provide updates to you if new regulations or guidelines are implemented. We invite you to consult with us further regarding the implications of this new authority.

King & Spalding's Data, Privacy and Security Practice

King & Spalding is particularly well equipped to assist clients in the area of privacy and information security law. Our Data, Privacy & Security Practice regularly advises clients regarding the myriad statutory and regulatory requirements that businesses face when handling personal customer information and other sensitive information in the U.S. and globally. This often involves assisting clients in developing comprehensive privacy and data security programs, responding to data security breaches, complying with breach notification laws, avoiding potential litigation arising out of internal and external data security breaches, defending litigation, whether class actions brought by those affected by

data breaches, third party suits, or government actions, and handling both state and federal government investigations and enforcement actions.

With more than 50 Data, Privacy & Security lawyers in offices across the United States, Europe and the Middle East, King & Spalding is able to provide substantive expertise and collaborative support to clients across a wide spectrum of industries and jurisdictions facing privacy and data security-based legal concerns. We apply a multidisciplinary approach to such issues, bringing together attorneys with backgrounds in corporate governance and transactions, healthcare, intellectual property rights, complex civil litigation, e-discovery, government investigations, government advocacy, insurance recovery, and public policy.

King & Spalding's International Trade/WTO Practice

King & Spalding's International Trade Group, headquartered in the Washington, D.C., and Geneva offices, handles a wide range of international trade matters for U.S. and non-U.S. clients. The group's export controls and sanctions practice provides assistance to clients on compliance with U.S., U.K., and EU law and regulations. Our main goal is to help clients achieve their business objectives in compliance with this constantly changing area of the law. Lawyers in the group assist clients in navigating all stages of government regulation, including assisting with sanctions compliance, export classification and licensing, developing and implementing internal compliance systems, investigating violations, and responding to enforcement actions brought by government trade control agencies.

---

[1] Executive Order "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities" (Apr. 1, 2015), *available at* https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m [hereinafter "Executive Order"].
[2] Director Keith B Alexander, "An Introduction By General Alexander," The Next Wave Vol. 19, No. 4 (last modified May 19, 2012), *available at* https://www.nsa.gov/research/tnw/tnw194/article2.shtml.
[3] Executive Order.
[4] Executive Order, Sec. 1.
[5] Executive Order, Sec. 1.
[6] Statement by the President on Executive Order "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," (Apr. 1, 2015), *available at* https://www.whitehouse.gov/the-press-office/2015/04/01/statement-president-executive-order-blocking-property-certain-persons-en; President Barack Obama, "A New Tool Against Cyber Threats" (Apr. 1, 2015), *available at* https://medium.com/@PresidentObama/a-new-tool-against-cyber-threats-1a30c188bc4 [Statement on Medium].
[7] Executive Order, Sec. 8.
[8] Executive Order, Sec. 4.
[9] On-the-Record Press Call on the President's Executive Order, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities" (Apr. 1, 2015), *available at* https://www.whitehouse.gov/the-press-office/2015/04/01/record-press-call-president-s-executive-order-blocking-property-certain- [hereinafter "Press Call"] (Statement of Mr. John Smith, Acting Director for the Office of Foreign Assets Control).
[10] Press Call (Statement of Mr. Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator).
[11] Questions Related to Executive Order 13694 "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," U.S. Department of the Treasury, *available at* http://www.treasury.gov/resource-center/faqs/Sanctions/Pages/answers2.aspx#444 [hereinafter "Questions Related to EO 13694"] (Question 444 and 446).

[12] Executive Order, Sec. 8.
[13] Press Call (Statement by John Smith).
[14] Executive Order "Imposing Additional Sanctions With Respect To North Korea" (Jan. 2, 2015), *available at* http://www.treasury.gov/resource-center/sanctions/Programs/Documents/13687.pdf.
[15] Press Call (Statement by John Smith).
[16] Press Call (Statement by John Smith).
[17] Questions Related to EO 13694 (Question 446).
[18] Questions Related to EO 13694 (Question 447).
[19] Statement by the President on Executive Order "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," April 1, 2015; Statement on Medium; Press Call (Statements by Michael Daniel and John Smith).
[20] Press Call (Statement by John Smith).