OFAC Issues New Cyber-Related Sanctions Regulations

To ring in the new year, the US Treasury Department's Office of Foreign Assets Control (OFAC) issued the Cyber-Related Sanctions Regulations, 31 CFR Part 578, on December 31, 2015 (the Cyber Sanctions Regulations). In its release of these implementing regulations, OFAC noted that they have been "published in abbreviated form for the purpose of providing immediate guidance to the public." OFAC explained that it "intends to supplement this part with a more comprehensive set of regulations, which may include additional interpretive and definitional guidance, including regarding 'cyber-enabled' activities, and additional general licenses and statements of licensing policy."[1] Companies are well advised to consider appropriate steps to mitigate their risks arising under these new regulations.

Cyber Sanctions Background

On April 1, 2015, OFAC issued Executive Order 13694 "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities" (EO 13694). EO 13694 targets persons who engage in malicious "cyber-enabled" activities, persons or entities outside the United States that receive or use misappropriated trade secrets, and anyone that provides "financial, material, or technological support" for prohibited activities. Unlike past Executive Orders that target specific sanctionable activities, OFAC did not designate (and has not designated as of the date of this publication) any individuals or entities as "Specially Designated Nationals" (SDNs) under EO 13694. Nor did it issue supporting regulations, until now.

Under EO 13694, OFAC is authorized to designate any person who engages in "cyber-enabled"[2] activities that compromise the "critical infrastructure sector"[3] or misappropriates trade secrets "for commercial or competitive advantage or private financial gain."[4] OFAC did not define malicious "cyber-enabled" activities in EO 13694 or the Cyber Sanctions Regulations, but in its "Frequently Asked Questions" OFAC has indicated that "malicious cyber-enabled activities" will include "deliberate activities

---

1 Note to 31 CFR § 578.101.
2 EO 13694, Section 1(a)(i).
3 According to Section 6(d) of EO 13694, "critical infrastructure sector" means any of the designated critical infrastructures in Presidential Policy Directive 21. This directive identifies 16 critical infrastructure 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; Water and Wastewater Systems. The Presidential Policy Directive 21 is available here.
4 EO 13694, Section 1(a)(ii).

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."[5] In addition, any entities that knowingly rely on or use stolen information or trade secrets "where the misappropriation of such trade secrets is reasonably likely to result in, or … materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States" could be targeted as SDNs under EO 13694.

In terms of targeting persons who have provided support for prohibited activities, the Cyber Sanctions Regulations define "financial, material, or technological support" as

> *any property, tangible or intangible, including but not limited to currency, financial instruments, securities, or any other transmission of value; weapons or related materiel; chemical or biological agents; explosives; false documentation or identification; communications equipment; computers; electronic or other devices or equipment; technologies; lodging; safe houses; facilities; vehicles or other means of transportation; or goods.*[6]

The definition goes on to clarify "technologies" as "specific information necessary for the development, production, or use of a product, including related technical data such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals, or other recorded instructions."

Under the Cyber Sanctions Regulations, property and interests in property of designated individuals or entities that are in the United States, enter the United States, or come into possession or control of a US person, are blocked, including any transactions in US dollars. The designation will also apply to any entities owned, directly or indirectly, 50% or more by an SDN. As of the effective date of designation, US persons are prohibited from participating in all transactions and/or dealing with a designated entity, including any "wind-down" activities, absent a general or specific authorization or license from OFAC.

Looking Ahead

Although it is difficult to tell how these sanctions will be implemented in the future, the recent publishing of the Cyber Sanctions Regulations indicates an increased focus within OFAC regarding these issues and we expect to see individuals and/or entities added to the SDN List in 2016. OFAC may make such a designation, which can become immediately effective, without providing notice. OFAC also is likely to provide additional substantive updates to these sanctions, specifically a definition of "cyber-enabled" activity.

Companies should take steps to mitigate their risks under EO 13694, including, for example, the risk that they are providing "financial, material, or technological support" for the prohibited activities, and the risk that their transactional targets, business partners, vendors, agents, or other contractual third parties are involved in any prohibited "cyber-enabled" activities or the misappropriation of trade secrets through cyber-enabled means.

---

5 *See* OFAC Frequently Asked Question 447, available here.
6 31 CFR § 578.304.

Authors

David DiBari
Partner
T: +1 202 912 5098
E: david.dibari
@cliffordchance.com

Wendy Wysong
Partner
T: +1 202 912 5030
(Washington)
T: +852 2826 3460 (Hong Kong)
E:wendy.wysong
@cliffordchance.com

Timothy Cornell
Partner
T: +1 202 912 5220
E: timothy.cornell
@cliffordchance.com

Megan Gordon
Partner
T: +1 202 912 5021
E: megan.gordon
@cliffordchance.com

Adam Klauder
Counsel
T: +1 202 912 5029
E:adam.klauder
@cliffordchance.com

Hena Schommer
Associate
T: +1 202 912 5447
E:hena.schommer
@cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

www.cliffordchance.com