Published on *The National Law Review* https://natlawreview.com

OFAC Publishes Cyber-Related Sanctions Regulations

Article By:

James A. Treanor

Keith M. Gerver

Joseph V. Moreno

On December 31, 2015, the ***Department of the Treasury***'s ***Office of Foreign Assets Control ("OFAC")*** issued regulations[1] implementing ***Executive Order 13694*** of April 1, 2015, which authorized the imposition of economic sanctions on individuals and entities determined to be responsible for, complicit in, or benefitting from significant cyber attacks or cyber theft.[2] The new regulations—which were issued in abbreviated form and are expected to be supplemented in the future—do not identify any specific individuals or entities to be sanctioned or trigger any immediate compliance obligations for U.S. companies. However, their publication is an indicator that the cyber sanctions program remains active and that more comprehensive regulations are forthcoming.

Executive Order 13694 created a new cyber sanctions program authorizing the Secretary of the Treasury to designate for inclusion in the Specially Designated Nationals List ("SDN List") two categories of individuals or entities.[3] The first category includes individuals and entities engaged in certain kinds of "cyber-enabled activities"[4] outside the United States that pose a "significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that have the purpose or effect of:"

(A) "harming, or otherwise significantly compromising the provision of services by, a computer or network of computers that support" a critical infrastructure sector entity;

(B) "significantly compromising" services provided by a critical infrastructure sector entity;

(C) significantly disrupting the availability of a computer or computer network; or

(D) significantly misappropriating "funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain."

The second category includes individuals and entities who have knowingly received or used—or attempted to receive or use—"trade secrets misappropriated through cyber-enabled means" for "commercial or competitive advantage or private financial gain," provided that the misappropriation rises to the level of being, resulting in, or materially contributing to a significant threat to U.S. national

security, foreign policy, or economic health or financial stability.

As with other sanctions regimes, inclusion on the SDN List results in the blocking of all the designated entity or individual's property, and interests in property, that are in the United States, come within the United States, or are in or come within the possession or control of a U.S. person. Since the issuance of Executive Order 13694, there has been speculation that the Obama Administration was prepared to impose sanctions on certain Chinese companies and individuals that benefitted from the theft of U.S. companies' intellectual property, but ultimately declined to do so after high-level meetings between senior U.S. and Chinese officials.[5] In fact, the threat of sanctions may have been a factor that led to the September 2015 agreement between the United States and China not to engage in economic espionage in cyberspace.[6]

The addition of two new categories of individuals and entities for inclusion on the SDN List, and the expected issuance of additional regulations to implement Executive Order 13694, provide an important opportunity for U.S. businesses to evaluate their compliance with existing U.S. sanctions regimes. This is especially true for those outside the financial industry who may not have previously focused on identifying and complying with economic sanctions programs. Individuals and companies who do business with potential targets of the new cyber sanctions regime, particularly in the technology and defense sectors, should remain especially vigilant in anticipation of future OFAC scrutiny.

---

[1] 80 Fed. Reg. 81,752 (December 31, 2015) (codified at 31 C.F.R. part 578), *available* here

[2] Executive Order 13694 of April 1, 2015, Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities.

[3] The names of individuals and entities whose property and interests in property are blocked pursuant to Executive Order 13694 are identified in the SDN List with the tag "[CYBER]." The SDN List is accessible at www.treasury.gov/sdn.

[4] Neither Executive Order 13694 nor the new regulations define "cyber-enabled activities." FAQs on OFAC's website indicate that future regulations are anticipated to define "cyber-enabled" activities to include "any act that is primarily accomplished through or facilitated by computers or other electronic devices." *See* here (last updated Apr. 1, 2015).

[5] Ellen Nakashima, *here*, Wash. Post, Sept. 14, 2015

[6] Ellen Nakashima & Steven Mufson, *here* Wash. Post, Sept. 25, 2015

National Law Review, Volume VI, Number 8