Now's the Time to Review Your OFAC Compliance Program

Written by Gwendolyn Wilber Jaramillo, Colin J. Zick, Michael N. Glanz, Shrutih V. Tewarie

April 7, 2015

Obama Executive Order Targets International Cyberattacks Against U.S. with New Sanctions

New Sanctions Are Part of U.S. Escalation of Efforts to Bolster Cyber-Security

As part of a series of measures aimed at increasing preparedness and defenses against international cyberattacks on U.S. industries and government agencies, on April 1, President Obama issued Executive Order No. 13694, authorizing the Treasury Department's Office of Foreign Assets Control (OFAC) to sanction foreign individuals or entities committing such attacks. The new sanctions will allow the Treasury Department to block or freeze the assets of those outside the U.S. engaging in malicious cyber activities that threaten the national security, foreign policy and financial stability of the U.S. Once OFAC designates specific entities and individuals for sanctions under the Executive Order, all U.S. Persons will have to ensure that they are not engaging in trade or any other transactions with the designated entities and individuals. U.S. Persons required to comply with these provisions include all U.S. citizens and permanent resident aliens, all persons and entities within the U.S., and all U.S.–incorporated entities and their foreign branches.

Unlike most sanctions programs administered by OFAC, this program does not target individuals that are controlled by, or acting on behalf of a specific foreign government. Instead, the new Executive Order adds cyberattacks to a select group of activities, including drug trafficking and terrorism, that are targets of OFAC sanctions.

Persons residing outside the U.S. may be subject to sanctions if they undertake certain actions via cyberspace, namely:

- Harming or significantly compromising the provision of services by entities in "critical infrastructure sectors";
- Disrupting the availability of a computer or network of computers;
- Misappropriating funds or sensitive information, such as trade secrets or personal financial information, for commercial or private economic gain;
- Knowingly receiving or using trade secrets that were stolen through cyberattacks for commercial or private economic gain; or
- Assisting or providing material support to any individuals or entities engaged in any of the harms listed above.

"Critical infrastructure sectors" are defined broadly to include numerous industries ranging from chemical and nuclear, communications, healthcare, and emergency services, to manufacturing, and financial services. Also included are information technology, defense and government facilities.

Legitimate Cyber Activities Will Not be Targeted

In FAQs released on the same day as the Executive Order, OFAC and the White House have emphasized that the sanctions will not target individuals or entities that conduct legitimate cyber-related activities. The sanctions are not meant to interfere with general network defense testing conducted by IT departments in the ordinary course of business, and will not affect cyber activities conducted for educational or research purposes. The program is also not aimed at victims of cyberattacks, including entities and individuals who have had their computers stolen or networks compromised and unknowingly utilized in cyberattacks.

Compliance Steps to Take in the Near Future

To date, no specific entities or individuals have been designated for sanctions under the Executive Order. However, OFAC has stated that it will work with other government agencies to identify and designate entities and individuals who meet the criteria for sanctions under the Executive Order. Once the designated persons are included on OFAC's Specially Designated Nationals and Blocked Persons (SDN) list, companies should take care to implement or strengthen risk-based OFAC compliance programs enabling them to avoid dealings with SDNs. While any such program should be tailored to the company's size, industry and need, companies should consider implementing compliance programs that incorporate automated sanctions screening processes.

Resources

The full text of the Executive Order can be found here: Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities.

Additional information on the OFAC sanctions program under the Executive Order can also be found on the OFAC FAQ page, and on the White House Blog.

To obtain further information about OFAC's SDN list, please click here: OFAC SDN List Resource Center.

RELATED INDUSTRIES

- Education
- Life Sciences
- Technology

RELATED PRACTICES

- International Business
- White Collar Crime & Government Investigations
- Business Counseling
- Trade Sanctions & Export Controls
