President Obama Announces New Cybersecurity Sanctions Regime

Skadden

04 / 7 / 15

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on Page 4, or your regular Skadden contact.

1440 New York Avenue, NW
Washington, D.C. 20005
202.371.7000

Four Times Square
New York, NY 10036
212.735.3000

skadden.com

On April 1, 2015, President Barack Obama issued an executive order (the Order) authorizing sanctions against foreign individuals or entities found to be responsible for certain malicious cyberattacks.[1] Under the Order, the U.S. government can block the assets of designated persons and entities located outside of the U.S., in whole or in substantial part, who are involved in cyber activities that could significantly threaten U.S. national and economic security interests. Designated individuals will also be denied entry into the United States.

The Order responds to a presidential finding that "malicious cyber-related activities originating from, or directed by persons located, in whole or in substantial part, outside the United States constitutes an unusual and extraordinary threat to the national security, foreign policy, and the economy of the United States."[2] The perpetrators of these activities may be foreign governments, their proxies, terrorist groups, criminal organizations — particularly those operating under some form of nation-state tolerance — or, in some cases, businesses.

While these sanctions may appear to be expansive, they are limited in very specific ways that are intended to ensure they target dangerous actors and not the legitimate business activities of U.S. companies. The sanctions are designed to enable swift action against only the most significant malicious foreign cyber actors who, for jurisdictional or other reasons, may be outside the reach of other U.S. governmental authorities. To date, no individual or entity has been designated under these sanctions. For this reason, we do not see an immediate impact on our clients; however, the use of this new authority against certain foreign individuals or companies could in turn impact U.S. businesses that leverage services or products those foreign entities provide.

The sanctions target the most significant foreign threats to U.S. cybersecurity.

The Order authorizes the secretary of the Treasury to impose sanctions on any person "responsible for or complicit in, or … [having] engaged in, directly or indirectly" certain "cyber-enabled" activities and, in certain cases, persons who benefit from them. Specifically, "cyber-enabled" activities may be subject to sanctions when they have the purpose or effect of:

- Harming or otherwise significantly compromising a "computer or network of computers" that supports a critical infrastructure sector as defined in Presidential Policy Directive 21;[3]

[1] Executive Order, Blocking the Property of Certain Persons Engaged 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.

[2] Although the Order authorizes sanctions against certain "malicious" cyber-enabled activities, the Order's specific requirements do not use the term "malicious." Several of the Office of Foreign Assets Control (OFAC) frequently asked questions (FAQs) related to the Order do make reference to the term.

[3] These sectors are: 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, Waste, Transportation Systems, and Water and Wastewater Systems. Presidential Policy Directive 21, Critical Infrastructure Security and Resilience, Feb 12, 2013, available at https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

- Significantly compromising services by a critical infrastructure entity;
- Causing significant disruption to the availability of a computer or computer network; or
- Causing a significant misappropriation of funds or economic resources, trade secrets,[4] personal identifiers or financial information for commercial advantage or financial gain.

The Order also authorizes sanctions against individuals or entities who:

- Benefit commercially or financially from the receipt or use of intellectual property known to have been misappropriated through cyber-enabled activities;
- Provide material support in furtherance of such activities;
- Are owned or controlled by, or agents of, any person subject to sanctions pursuant to the Order; or
- Attempt the activities described above.

The Order narrows the scope of the sanctions by conditioning their imposition on the following additional circumstances:

- *Foreign threat*. Cyber-enabled activities that trigger sanctions must have originated or have been directed substantially from outside the United States. The receipt or use of misappropriated trade secrets must also have been outside the United States.
- *Foreseeable or actual threat to U.S. security interests*. To trigger sanctions, the cyber-enabled activities must be "reasonably likely to result in, or have materially contributed to a significant threat" to U.S. national security, foreign policy, economic health, or financial stability. Note, however, that the Order does not define the full scope of these protected U.S. interests.
- *Significance*. Most of the activities that could trigger or lead to the imposition of sanctions, as well as the potential threat to U.S. national and economic security interests, must be "significant." However, the Order does not define "significant" in the context of either these activities or the threat to protected U.S. interests.

The Order was issued without an initial set of designations.[5] Following designation of any individual or entity under the Order, the obligations of U.S. persons (and persons otherwise subject to the jurisdiction of the Treasury Department's Office of Foreign Assets Control (OFAC)) will be the same as those with regard to Specially Designated Nationals (SDNs) designated under other OFAC-administered sanctions regimes. Specifically, U.S. persons must ensure they are not engaging in trade or other transactions with persons named under the Order.[6]

The sanctions represent a concrete action the government can take immediately to address cyber threats.

In the last few years, actors from outside the United States have engaged in malicious cyber activities targeting the United States. The Order is another step in the government's efforts to counter the increasing threat of loss of intellectual property, personal information and funds associated with these malicious cyber activities. In January and February 2015, the president proposed several legislative cybersecurity and data privacy initiatives.[7] Some of these initiatives relate to the duties of data collectors to protect personal data and report data breaches. Other initiatives are intended to expand the authority of law enforcement organizations to pursue and prosecute cyber criminals.

The Order complements these prior efforts by providing the administration with a tool to raise the cost of hacking to individuals, organizations and nation-state actors that engage in such activities. Sanctions against individuals and companies are widely perceived to be an effective tool in combatting threats to the U.S. economy and national security. Sanctions provide for a U.S. government response in instances where criminal prosecution is difficult for jurisdictional or other reasons. Sanctions can be imposed without prior notice and without the procedural and substantive hurdles faced in a prosecution, including the admissibility of evidence and more stringent burdens of proof.

[4] Protected "trade secrets" are not defined in the Order but likely would include those already covered by the Economic Espionage Act of 1996, as amended (18 U.S.C. § 1839). Under the act's definition, "trade secrets" include all information that its legal owner has taken reasonable measures to keep secret and that derives independent economic value from not being known to or readily ascertainable by the public.

[5] OFAC FAQ 445. What are my immediate compliance obligations with respect to this EO? Apr. 1, 2015.

[6] OFAC FAQ 446. What will my compliance obligations be once Treasury designates individuals or entities pursuant to this EO? Apr. 1, 2015.

[7] For more information, please see our January and February 2015 editions of *Privacy & Cybersecurity Update*, available here and here.

The application of sanctions to cyber threats is also in keeping with the "whole government" approach applied to other problems, such as counterterrorism and counternarcotics, where military, law enforcement, economic and diplomatic instruments have been used in concert.[8]

The sanctions are designed in a manner intended to reduce the impact on legitimate activities.

Like counterterrorism and counternarcotics sanctions regimes, these sanctions focus on an activity, not a country or sector. As such, they have potentially worldwide scope. However, the cyber sanctions are limited in important ways that are intended to reduce the compliance concerns associated with this regime:

- The sanctions are largely focused on "cyber-enabled" activities, described by OFAC as "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."[9] Under the Computer Fraud and Abuse Act, "unauthorized access" is distinguished from "exceeding authorized access."[10] If the Treasury regulations implementing the Order continue to reference only the former, it is possible that the sanctions will be aimed at remote unauthorized actors and not the insider threat posed by employees or third-party vendors.
- The sanctions are intended to only apply to the most significant cyber actors. The sanctions are not intended to interfere with or target legitimate educational, network defense or research purposes.[11] Nor are the sanctions to be imposed on individuals or entities whose computers are used, without their knowledge or consent, in malicious cyber activities.[12]
- These sanctions are intended to be used when other instruments of national power are unavailable or would be ineffective.[13] As such, these sanctions would be applicable to foreign actors outside the jurisdictional reach of the U.S. government and against whom other forms of legal, political or economic mechanisms would be ineffective.

Practical and legal challenges will shape the implementation of these sanctions.

Practical and legal challenges unique to cybersecurity will shape, and even limit, the government's use of these sanctions:

- *Attribution*. Attribution in the cybersecurity realm presents significant difficulties, both in the acquisition of potentially relevant information from assorted parties and in its subsequent analysis. The government also will have to carefully balance its enforcement goals against protecting sensitive sources and methods that may be used in detecting these activities.
- *Protected Interests and Significance*. As noted above, the Order does not define the full scope of the interests protected by the regime. Likewise, the term "significant" is undefined in the Order. How the government defines these terms will impact how the sanctions are implemented.
- *Due Process*. The Order allows for designation without prior notification. Like other sanctions regimes, such a designation may implicate the due process rights of the individuals or entities subject to sanctions under the regime. Persons sanctioned under the Order can challenge their designation with OFAC via administrative petition or file a suit in federal district court.

The new cyber sanctions regime is unlikely to have an immediate impact but could present challenges in the longer term for those reliant on foreign information technology.

We do not anticipate any immediate impact of the new cyber sanctions regime. No individual or entity has been designated by OFAC under this new regime, and the obligation of U.S. persons to avoid trade or transactions with OFAC-designated individuals and entities remains unchanged. In addition, the sanctions are not intended to target normal business, research and network defense activities. Rather, they are designed to target only the

[8] OFAC FAQ 451. How do financial sanctions relate to existing legal authorities in this context? Apr. 1, 2015.

[9] OFAC FAQ 447. What will significant malicious "cyber-enabled" activities mean for the purposes of this Executive Order? Apr. 1, 2015.

[10] 18 U.S.C. § 1030.

[11] OFAC FAQ 448. I conduct cyber-related activities for legitimate educational, network defense, or research purposes only. Am I vulnerable to the application of sanctions under this authority for these activities? Apr. 1, 2015. *See also* OFAC FAQ 449. I administer a network for my employer and I regularly deny access to certain services and systems (*e.g.*, retail websites, social media platforms) in order to ensure the performance of the network for authorized business activities. Could I or my employer be sanctioned for this? Apr. 1, 2015.

[12] OFAC FAQ 450. Will Treasury impose sanctions on persons whose personal computers (or other networked electronic devices) are, without their knowledge or consent, used in malicious cyber-enabled activities (*e.g.*, in denial-of-service attacks against U.S. financial institutions)? Apr. 1, 2015.

[13] OFAC FAQ 444. How will Treasury decide whom to sanction under this authority? Apr. 1, 2015.

most significant and malicious cyber activities currently beyond the effective reach of the U.S. government. As a result, clients can expect that their own good-faith network management and development will continue to be permissible under the new regime.

Going forward, however, certain foreign entities could face sanctions under the Order. In today's globalized technology market, nearly everyone uses IT products and services sourced directly or indirectly from overseas. As such, businesses should take steps to become familiar with the various OFAC sanctions regimes, including those created under the Order. If such steps are taken early, these businesses will be prepared to implement restrictions with respect to parties designated under the Order, reducing the risk of potential penalties and business interruption associated with dealing with an SDN.

Contacts

Partners

Cyrus Amir-Mokri
New York
212.735.3279
cyrus.amir-mokri@skadden.com

Jamie L. Boucher
Washington, D.C.
202.371.7369
jamie.boucher@skadden.com

Stuart D. Levi
New York
212.735.2750
stuart.levi@skadden.com

Ivan A. Schlager
Washington, D.C.
202.371.7810
ivan.schlager@skadden.com

William J. Sweet, Jr.
Washington, D.C.
202.371.7030
william.sweet@skadden.com

Counsel

John M. Beahn
Washington, D.C.
202.371.7392
john.beahn@skadden.com

Jonathan M. Gafni
Washington, D.C.
202.371.7273
jonathan.gafni@skadden.com

Kelvina M. Smith Moore
Washington, D.C.
202.371.7284
kelvina.smith@skadden.com

Malcolm Tuesley
Washington, D.C.
202.371.7085
malcolm.tuesley@skadden.com

Associates

Joshua F. Gruenspecht
Washington, D.C.
202.371.7316
joshua.gruenspecht@skadden.com

John P. Kabealo
Washington, D.C.
202.371.7156
john.kabealo@skadden.com

James E. Perry
Washington, D.C.
202.371.7652
james.e.perry@skadden.com