WILMERHALE

Executive Order Creates Cybersecurity Sanctions Framework

FRIDAY, APRIL 03, 2015

On April 1, 2015, President Obama issued an Executive Order authorizing the imposition of sanctions against designated individuals or entities found to be engaged in malicious cyber activity, including various forms of commercial espionage and trade secret theft.[1] No specific designations or implementing regulations accompanied the Order. Nevertheless, the President's action highlights the increasing importance of cybersecurity in U.S. national security policy and the government's increasing willingness to use creative policy tools, including list-based sanctions, to combat cyber threats to U.S. economic and national security interests.

As with other list-based sanctions programs, the Order highlights the importance of establishing strong internal procedures to conduct transaction screening. An effective screening program ensures that a company's dealings do not involve designated parties or their property interests, including entities that are owned 50 per cent or more (individually or in the aggregate) by such SDNs. Companies should take this opportunity to review their compliance programs generally and be ready to incorporate new requirements as OFAC issues more detailed supporting regulations. It will also be important for companies to monitor the overseas reaction to this Order. Certain EU Member States, for example, are already discussing the possibility of taking similar types of action, and other countries may implement similar policies of their own.

Targets of the Order

The Order authorizes the imposition of sanctions against two basic categories of designated individuals or entities:

First, those that take part in "cyber-enabled activities" from outside the United States that "are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States" and that have any of four purposes or effects: (i) "harming, or otherwise significantly compromising the provision of services by, a computer or network of computers that support one or more entities in a critical infrastructure sector"; (ii) "significantly compromising the provision of services by one or more entities in a critical infrastructure sector"; (iii) "causing a significant disruption to the availability of a computer or network of computers"; or (iv) "causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or

competitive advantage or private financial gain." There are sixteen critical infrastructure sectors, including chemical, communications, critical manufacturing, defense, energy, financial services, healthcare and agriculture.[2]

Second, those that are “responsible for or complicit in, or to have engaged in, the receipt or use for commercial or competitive advantage or private financial gain, or by a commercial entity, outside the United States of trade secrets misappropriated through cyber-enabled means, knowing they have been misappropriated, where the misappropriation of such trade secrets is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States.”

The provision of material assistance, sponsorship, or financial, material, or technological support, or goods or services in support of any of the targeted activities is likewise now grounds for sanctions under the Order.

Implementing the Order

As with other list-based sanctions, the Order generally prohibits U.S. persons from engaging in any dealings with designated persons, and any property or property interests within U.S. jurisdictions or held by U.S. persons must be blocked. The Order also prohibits transactions designed to evade or avoid the sanctions regime.

We expect that the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) will ultimately promulgate regulations implementing this Order, which will include procedures to designate individuals or entities under the Order. As with other sanctioned parties, these designees will be added to OFAC’s list of Specially Designated Nationals and Blocked Persons (SDNs).[3]

In the meantime, OFAC provided initial guidance in the form of FAQs[4] that sets forth a number of important definitions, including the term "malicious cyber-enabled activity":

> "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."

OFAC’s guidance clarifies that the Order is "not designed to prevent or interfere with legitimate cyber-enabled academic, business, or non-profit activities," and is intended to target only significant, malicious cyber actors that threaten U.S. interests. Normal network administration that incidentally disrupts network access (e.g., blocking online retail access from an office network) does not fall under the scope of the Order.

The Order also constitutes an additional tool for the U.S. government to combat the growing threat of cyber-enabled misappropriation or theft of trade secrets held by U.S. companies. Recently, the U.S. government has increased prosecution of trade secret theft under current authorities, Congress has considered legislation to create a uniform federal civil cause of action and strengthen criminal penalties against trade secret theft, and negotiators have pushed to include the protection of trade

secrets in international trade agreements under negotiation. This Order could prove to be a further important new means to deter and punish egregious cases of trade secret theft. The government also clearly hopes to encourage the private sector to increase information sharing on such attacks. "The more information about trade secret theft, the better off we are," John Smith, the acting director of the Treasury Department's Office of Foreign Assets Control, told reporters Wednesday on a conference call. "We would welcome the input from the private sector and others that may have relative information on trade secret theft that might be covered by the executive order."[5] However, real questions relating to the more detailed implementation of and procedures applicable to this and other aspects of the Order will remain until OFAC issues accompanying regulations.

The Order represents the third significant deployment of U.S. sanctions law in just the past several months to combat cyber-related malfeasance as a national security threat. Section 1637 of this year's National Defense Authorization Act authorized the President to block the assets of any foreign person who "knowingly requests, engaged in, supports, facilitates, or benefits from the significant appropriation" of U.S. technologies or proprietary information through economic or industrial espionage in cyberspace.[6] And, in January, President Obama issued a separate Executive Order imposing new sanctions on North Korea because of "the provocative, destabilizing, and repressive actions and policies of the Government of North Korea, including its destructive, coercive cyber-related actions during November and December 2014."[7]

---

[1] "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. Supporting materials are available at http://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20150401.aspx.

[2] The full list of critical infrastructure sectors is identified in Presidential Policy Directive 21(Feb. 12, 2013) (citing 42 U.S.C. 5195c(e)): 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, and water and wastewater systems.

[3] *See*, OFAC Specially Designated Nationals List, *available at* http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx.

[4] *See*, OFAC Frequently Asked Questions #444-52.

[5] Philip Ewing, "U.S. hopes cyber rule draws info from vendors," POLITICO (April 1, 2015).

[6] Pub. L. No. 113- 291, 128 Stat. 3292.

[7] "Imposing Additional Sanctions with Respect to North Korea" (January 2, 2015), *available at* https://www.whitehouse.gov/the-press-office/2015/01/02/executive-order-imposing-additional-

sanctions-respect-north-korea.

Authors

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

Co-Chair, Artificial Intelligence Practice

benjamin.powell@wilmerhale.com

+1 202 663 6770

Aaron M. Zebley

PARTNER

aaron.zebley@wilmerhale.com

+1 202 663 6808

Gregory H. Lantier

PARTNER

Chair, Western District of Texas Working Group

Co-Chair, Post-Grant Proceedings Group

gregory.lantier@wilmerhale.com

+1 202 663 6327

Ronald I. Meltzer

SENIOR COUNSEL

ronald.meltzer@wilmerhale.com

+1 202 663 6389

Jason C. Chipman

PARTNER

jason.chipman@wilmerhale.com

+1 202 663 6195