President Obama Sanctions Russia Over Malicious Cyber-Enabled Activities

DECEMBER 30, 2016

President Obama amended a previously-issued executive order designed to address cyber-enabled activities yesterday in response to "Russia's cyber activities [that] were intended to influence the election, erode faith in U.S. democratic institutions, sow doubt about the integrity of our electoral process, and undermine confidence in the institutions of the U.S. government."[1] At the same time, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) added five entities and four individuals to its list of Specially Designated Nationals and Blocked Persons (SDN List) in connection with what the White House has described as malicious Russian cyber activity.

These and related measures announced yesterday underscore the importance of sanctions compliance, while firms should ensure that their data security processes reflect the best available information concerning potential threats.

U.S. sanctions regulations prohibit most commercial and financial dealings with SDNs and require that U.S. persons block their property and interests in property. In this case, the sanctions target Russian intelligence services and their top officers, as well as three companies that the Obama Administration identified as supporting Russia's cyber-enabled activities through intelligence activities, special training, and other capabilities.

The five targeted entities are:

- Main Intelligence Directorate (a.k.a. Glavnoe Razvedyvatel'noe Upravlenie; a.k.a. GRU);
- Federal Security Service (a.k.a. Federalnaya Sluzhba Bezopasnosti; a.k.a. FSB);
- Autonomous Noncommercial Organization Professional Association of Designers of Data Processing Systems (a.k.a. Ano Po Ksi);
- Special Technology Center (a.k.a. STC, Ltd.); and
- Zorsecurity (f.k.a. Esage Lab; a.k.a. Tsor Security).

The four individuals are:

- Igor Valentinovich Korobov (Chief, GRU);
- Sergey Aleksandrovich Gizunov (Deputy Chief, GRU);
- Igor Olegovich Kostyukov (First Deputy Chief, GRU); and
- Vladimir Stepanovich Alekseyev (First Deputy Chief, GRU).

OFAC also designated two additional individuals—Evgeniy Mikhailovich Bogachev and Aleksey Alekseyevich Belan—for their cyber-enabled misappropriation of financial information and personal identifiers for private financial gain. OFAC stated that Mr. Bogachev developed the Zeus malware, which is associated with the theft of financial information and other criminal activity. According to OFAC, Mr. Bogachev directly benefited from the use of the malware by other cybercriminals and he also used a form of "ransomware" to hold at least 120,000 U.S. victims' data hostage for financial gain in excess of $100 million. OFAC stated that Mr. Belan's attacks on at least three U.S.-based e-commerce companies' computer networks led to the theft of email addresses, customer names, and encrypted passwords, which he sold for private financial gain.

Yesterday's action represents the first use of Executive Order 13694, which President Obama promulgated in April 2015 in response to a number of apparent cyber-enabled threats to U.S. interests.[2] Congress has previously authorized sanctions to combat cyber-related economic or industrial espionage,[3] and these measures parallel a separate executive order imposing sanctions against North Korea for "its destructive, coercive cyber-related actions during November and December 2014."[4]

The White House announced several additional actions beyond this initial use of Executive Order 13694. First, the State Department is expelling 35 Russian intelligence operatives and shutting down properties in Maryland and New York from which they were said to operate. Second, the Department of Homeland Security and the Federal Bureau of Investigation have released a Joint Analysis Report of declassified technical information on Russian civilian and military intelligence cyber activity. The release is intended to support U.S. and foreign cybersecurity efforts to "identify, detect, and disrupt Russia's global campaign of malicious cyber activities."

It is not clear how the new Trump Administration will respond to these new actions once in office. In the wake of these measures, President-Elect Donald Trump stated it was "time for our country to move on to bigger and better things" but that he would meet with the Intelligence Community "in order to be updated on the facts of this situation." However, members of Congress may be poised to push for even stronger measures. For example, Senator Lindsey Graham stated that he—along with Senator John McCain—intends to lead the effort for additional sanctions against Russia in the forthcoming legislative session.

With these new designations, firms should review the adequacy of their internal procedures to conduct effective counterparty due diligence and transaction screening. In particular, companies should ensure that their procedures are designed to detect possible dealings with SDNs (including entities they may 50 percent or more own individually or in the aggregate) and to meet applicable blocking and reporting requirements. Firms should also consider whether they have relationships with foreign security services or cybersecurity providers that are implicated by U.S. cyber sanctions and how to manage those going forward. Additionally, all organizations that may be a target for

state-sponsored cyber intrusions—such as defense contractors, organizations holding large amounts of personal information, and businesses operating in critical infrastructure sectors—should ensure that their IT security measures account for the information provided in the Joint Analysis Report.

---

[1] The White House, "The Administration's Response to Russia: What You Need to Know," (Dec. 29, 2016).

[2] President Obama amended Executive Order 13694 yesterday so that it applied to what the Obama Administration has described as an effort to "undermine democratic processes or institutions." The executive order had previously authorized the imposition of sanctions against those who engaged in cyber-enabled activities (i) threatening the national security, foreign policy, or economic health or financial stability of the United States and (ii) having the purpose or effect of negatively impacting the computer networks or entities in a critical infrastructure sector, causing a disruption to the availability of computer networks, or causing a significant misappropriation of funds, trade secrets, or other financial information for commercial or competitive advantage or private financial gain. Yesterday's amendment further authorized sanctions against cyber-enabled activities that threaten U.S. national security, foreign policy, or economic health or financial stability and have the purpose or effect of "tampering with, altering, or causing a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions."

[3] National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, 128 Stat. 3292.

[4] Executive Order 13687, "Imposing Additional Sanctions with Respect to North Korea," (Jan. 2, 2015).

Authors

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