COVINGTON

U.S. Expands Sanctions, Takes Other Steps in Response to Russia's Election-Related Cyber Operations

January 4, 2017

International Trade Controls, Data Privacy and Cybersecurity

President Obama announced several actions on December 29 to respond to Russian cyber operations that the U.S. intelligence community previously had concluded were intended to influence the U.S. presidential election. Specifically, the President revised and expanded an earlier executive order that blocks the property and interests in property of persons that engage in significant malicious cyber-enabled activities, and designated 5 Russian entities and 6 Russian individuals for sanctions pursuant to the revised and expanded order. The President also released a report by the U.S. Department of Homeland Security ("DHS") and Federal Bureau of Investigation ("FBI") containing declassified information attributing cyber attacks to Russia, expelled 35 Russian diplomats, and barred Russian access to two compounds in the United States. Additionally, today, the U.S. Commerce Department added the five designated Russian entities involved in Russia's election-related cyber operations to the Entity List, which prohibits the export, reexport, or transfer of any item subject to the U.S. Export Administration Regulations ("EAR") to the listed entities, absent Commerce Department licensing. Although these actions are politically significant, they do not expand the U.S. sectoral sanctions against Russia and should have a limited near-term economic effect.

This alert provides an overview of the revised executive order (the scope of which is not limited to Russia), the Russia-specific sanctions designations, and the cybersecurity and diplomatic steps the Obama Administration announced in response to Russia's election-related cyber operations. It also considers the prospects for further developments in U.S. sanctions against Russia in the coming months.

Sanctions Measures

Revised Executive Order

In April 2015, President Obama issued Executive Order 13694, which blocks the property and interests in property that are or come into the United States or the possession or control of a U.S. person of any person who is determined to be responsible for or complicit in, or to have engaged in, directly or indirectly, cyber-enabled activities that: (1) originate from or are directed by persons located entirely or substantially outside the United States; (2) 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 (3) have the purpose or effect of:

- Significantly compromising the provision of services by entities in a critical infrastructure sector (or harming or significantly compromising the provision of services by a computer or network of computers that support such entities);
- Causing a significant disruption to the availability of a computer or network of computers (e.g., through a distributed denial-of-service attack); or
- 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 (e.g., by stealing large quantities of credit card information, trade secrets, or sensitive information).

On December 31, 2015, the Treasury Department's Office of Foreign Assets Control ("OFAC") issued regulations to implement Executive Order 13694. *See* 31 C.F.R. Part 578, Cyber-Related Sanctions Regulations.

After concluding that Executive Order 13694 was not sufficiently broad to allow the U.S. government to impose sanctions against Russian parties engaged in election-related cyber activities, President Obama revised and expanded the order last week to reach persons involved in "tampering with, altering, or causing a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions." Significantly, the order is not limited to interference with U.S. election processes. Simultaneous with the issuance of the expanded executive order, OFAC published several new Frequently Asked Questions ("FAQs") regarding the order.

SDN Designations

Pursuant to the revised and expanded executive order, President Obama added 11 Russian individuals and entities to the List of Specially Designated Nationals and Blocked Persons ("SDN List") maintained by OFAC. The first nine were added for cyber-related activities targeting the U.S. election, while the final two were added for cyber-enabled misappropriation of financial information and personal identifiers for private financial gain:

1. The Main Intelligence Directorate (a.k.a. Glavnoe Razvedyvatel'noe Upravlenie or GRU), which is involved in external intelligence collection using both human intelligence officers and technical tools, and which was designated for tampering, altering, or causing a misappropriation of information with the purpose or effect of interfering with U.S. election processes;
2. The Federal Security Service (a.k.a. Federalnaya Sluzhba Bezopasnosti or FSB), which assisted the GRU in carrying out election-related cyber activities;
3. The Special Technology Center (a.k.a. STLC, Ltd. Special Technology Center St. Petersburg), which assisted the GRU in conducting signals intelligence operations;
4. Zorsecurity (a.k.a. Esage Lab), which provided the GRU with technical research and development support;
5. The Autonomous Noncommercial Organization "Professional Association of Designers of Data Processing Systems" (a.k.a. ANO PO KSI), which provided specialized training to the GRU;
6. Igor Valentinovich Korobov (Chief of the GRU);
7. Sergey Aleksandrovich Gizunov (Deputy Chief of the GRU);

8. Igor Olegovich Kostyukov (First Deputy Chief of the GRU);
9. Vladimir Stepanovich Alexseyev (First Deputy Chief of the GRU);
10. Evgeniy Mikhailovich Bogachev, who was designated for engaging in cyber-enabled misappropriation of financial information for private financial gain, including the theft of over $100 million from U.S. financial institutions, *Fortune* 500 firms, universities, and government agencies; and
11. Aleksey Alekseyevich Belan, who was designated for engaging in cyber-enabled misappropriation of personal identifiers for private financial gain, including compromising the computer networks of at least three major U.S.-based e-commerce companies.

As a result of these designations, the property and interests in property of these entities and individuals that are or come within the United States or the possession or control of a U.S. person—as well as the property and property interests of any entities 50 percent or more owned by the listed entities or individuals (on their own or in combination with other SDNs)—are blocked, and U.S. persons are prohibited from dealing with such entities and individuals.

Additionally, today, the U.S. Commerce Department's Bureau of Industry and Security ("BIS") added the GRU, FSB, STLC, Zorsecurity, and ANO PO KSI to its Entity List. As a result, a BIS license is required to export, reexport, or transfer (in-country) to the listed entities any item subject to the EAR, including all U.S.-origin items, all items being exported from the United States (regardless of origin), and non-U.S. items that contain more than a de minimis amount of controlled U.S.-origin content (by value). Applications for such licenses are subject to a presumption of denial.

Potential for Additional Sanctions Against Russia

It is quite possible that the new Congress will introduce sanctions legislation targeting Russia, though neither the contours of such legislation nor the prospects for enactment into law are clear at this stage.

Notably, following last week's actions, Republican Senators John McCain and Lindsey Graham released a joint statement saying that they intended to "lead the effort in the new Congress to impose stronger sanctions on Russia." And earlier last week, before the Administration's actions described above were announced, Senator Graham reportedly stated that "we're going to put sanctions together that hit Putin as an individual and his inner circle for interfering in our election."

Last year, the U.S. House of Representatives passed sanctions legislation targeting Russia. Although that legislation, which died in the Senate, was in response to Russia's annexation of Crimea and conduct relating to eastern Ukraine, rather than Russia's election-related cyber operations, it suggests that Congress may be prepared to take up Russia sanctions legislation if it views the executive branch's actions in this area as insufficient or ineffective.

In that regard, it is also worth noting that the underlying legal authority for the expansion of the executive order and SDN designations announced last week is set to expire on April 1, 2017, while the underlying legal authority for the separate U.S. sectoral sanctions against Russia is set to expire on March 6, 2017, unless President Obama (before his term ends) or President Trump (once sworn in) renews the relevant legal authorities before those dates. The early March expiration of the legal authority for the U.S. sectoral sanctions, in particular, could provide an initial indication as to how the Trump Administration intends to handle sanctions against Russia.

Other Actions

In addition to the sanctions measures described above, the Obama Administration declassified certain cybersecurity information relating to Russia's election-related cyber operations, and also took several diplomatic measures.

DHS-FBI Joint Analysis Report

The DHS and FBI Joint Analysis Report ("JAR") released on December 29 contains detailed declassified information about Russian cyber activities, with the goal of assisting network defenders in the United States and abroad to identify, detect, and disrupt Russian malicious cyber intrusions.

The JAR includes recently declassified indicators of compromise related to computers that the U.S. government believes Russian intelligence services have co-opted without the knowledge of their owners in order to obfuscate Russia's malicious cyber activities. The JAR specifically focuses on the targeting and compromise of a U.S. political party (widely reported to be the Democratic Party) by two Russian threat actors. The JAR also includes information designed to enable cybersecurity firms and other network defenders to identify and block certain malware that the U.S. government believes Russian intelligence services use. Further, the JAR includes information on how Russian intelligence services typically conduct cyber operations, which the U.S. government believes can help network defenders identify new Russian tactics to better detect and disrupt an ongoing intrusion.

The JAR also encourages security companies and private-sector owners and operators of information systems to review their network traffic for signs of malicious activity based on the shared indicators. DHS has added these indicators to its Automated Indicator Sharing ("AIS") service. Thus, any entity that receives an AIS feed should already have this data; if not, DHS and FBI also separately released the indicators in two different file formats—CSV and STIX.

Diplomatic Actions

The Obama Administration also declared 35 Russian diplomats based at the Russian embassy in Washington, D.C. and the Russian consulate in San Francisco as "persona non grata" for having acted "in a manner inconsistent with their diplomatic status." These officials and their families were required to leave the United States within 72 hours. The Obama Administration also has denied Russia access to two Russian government-owned facilities in Maryland and New York.

* * *

Covington has deep experience advising clients concerning international sanctions against Russia and with respect to cybersecurity. We will continue to monitor developments in these areas, and are well-positioned to assist clients in understanding how these recent announcements may affect their business operations.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our International Trade Controls and Cybersecurity practices:

Peter Flanagan	+1 202 662 5163	pflanagan@cov.com
Corinne Goldstein	+1 202 662 5534	cgoldstein@cov.com
Peter Lichtenbaum	+1 202 662 5557	plichtenbaum@cov.com
Kimberly Strosnider	+1 202 662 5816	kstrosnider@cov.com
David Addis	+1 202 662 5182	daddis@cov.com
David Fagan	+1 202 662 5291	dfagan@cov.com
James Garland	+1 202 662 5337	jgarland@cov.com
Ashden Fein	+1 202 662 5116	afein@cov.com
Josh Williams	+1 202 662 5618	jnwilliams@cov.com