Akin Gump
STRAUSS HAUER & FELD LLP

Client Alert

January 4, 2017

Key Points

- This action marks the first time sanctions have been imposed under the Cybersecurity Sanctions Program established on April 1, 2015, with the designation of nine entities and individuals.
- President Obama expanded the scope of the executive order creating the Cybersecurity Sanctions Program to allow for designations against persons determined to have engaged in malicious cyber--enabled activities directed at, interfering with or undermining election processes or institutions in the United States or abroad.
- Five entities that are subject to the new sanctions are now also subject to export licensing requirements by the U.S. Department of Commerce.
- Clients subject to U.S. jurisdiction should ensure that their screening software is updated to safeguard their compliance obligations against transactions involving the newly designated persons and entities.
- Clients should review the technical information released to evaluate and assess potential cyber intrusion risks.

United States Imposes Cybersecurity Sanctions on Russia

Overview of Actions Taken by the United States

On December 29, 2016, President Obama announced that he was sanctioning nine individuals and entities: the Main Intelligence Directorate (aka Glavnoe Razvedyvatel'noe Upravlenie) (GRU) and the Federal Security Service (aka Federalnaya Sluzhba Bezopasnosti) (FSB), two Russian intelligence services; four individual officers of the GRU; and three companies that were stated to have provided material support to the GRU's cyber operations. In addition, two Russian individuals were sanctioned for using cyber-enabled means to cause misappropriation of funds and personal identifying information. These actions mark the first expansion of the Specially Designated Nationals (SDN) List to include entities and individuals under the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) cybersecurity program since it was established on April 1, 2015. The 2015 client alert can be found here.

On January 4, 2017, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) added the five entities newly designated as SDNs to the Entity List. As a result of such designations, additional licensing requirements and restrictions apply to exports, re-exports, and transfers (in-country) to these entities under the Export Administration Regulations (EAR).

The State Department also announced that it is denying Russian access to two Russian government-owned recreational compounds in Maryland and New York and is declaring "persona non grata" 35 officials from the Russian Embassy in Washington and the Russian Consulate in San Francisco. The State Department announced that these measures were part of a comprehensive response to Russia's interference in the U.S. election; a pattern of harassment of U.S. diplomats overseas (including arbitrary police stops, physical assault and the broadcast on Russian State TV of personal details about our personnel that put them at risk); and Russian government actions that the State Department maintained impeded U.S. diplomatic operations.

Finally, on December 29, the Department of Homeland Security and the Federal Bureau of Investigation (FBI) released declassified technical information on Russian civilian and military intelligence service cyber activity to allow for the public to be able to better identify, detect and disrupt "Russia's global campaign of malicious cyber activities." This Joint Analysis Report follows the October 7, 2016, joint statement by Secretary Johnson and Director Clapper that the intelligence community was confident that the Russian government directed recent compromises of emails from U.S. persons and institutions and that the disclosures of alleged hacked emails was consistent with the Russian--directed efforts, both in the United States and to influence public opinion in Europe and Eurasia. The full Joint Analysis Report can be found here.

President Obama suggested that additional actions are already under way and forthcoming: "These actions are not the sum total of our response to Russia's aggressive activities. We will continue to take a variety of actions at a time and place of our choosing, some of which will not be publicized."

Congressional leaders have generally supported the December 29 actions by President Obama, with certain senior Republican members of Congress remarking that measures should have been taken earlier.

Russian President Vladimir Putin has indicated that he will not take retaliatory measures at this time and will await the inauguration of President--elect Donald Trump. In response, President--elect Trump praised President Putin's restrained response to these measures.

These and other sanctions involving Russia are subject to potential change by executive order. Although the U.S. Congress is considering legislation to codify existing sanctions and/or impose additional sanctions against Russia, President--elect Trump may seek to roll back these executive actions after he takes office on January 20, 2017. An initial indication of what is to come will likely occur during the upcoming confirmation hearings for Rex Tillerson as the nominee for Secretary of State, who has extensive business experience in Russia.

Cybersecurity Executive Order Expanded to Cover Election Interference

As originally issued in April 2015, Executive Order 13694 created an authority for the U.S. government to respond more effectively to the most significant cyber threats and targeted persons who engage in malicious cyber-enabled activities. The President amended Executive Order 13694 to authorize sanctions

on those who engage in malicious cyber--enabled activities that 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."

Specific Additions to the SDN List

Under this new authority, President Obama added five entities and four individuals to the SDN List. The Fact Sheet issued by the White House explained the basis for each of these additions, indicating that each of these entities and individuals had tampered, altered or caused a misappropriation of information with the purpose or effect of interfering with the 2016 U.S. election processes, as explained below:

- Two Russian intelligence services: the Main Intelligence Directorate (aka Glavnoe Razvedyvatel'noe Upravlenie) (GRU), which was involved in external collection using human intelligence officers and a variety of technical tools; and the Federal Security Service (aka Federalnaya Sluzhba Bezopasnosti) (FSB), which assisted the GRU in conducting the activities described above
- Three companies that provided material support to the GRU's cyber operations: the Special Technology Center (aka STLC, Ltd. Special Technology Center St. Petersburg), which assisted the GRU in conducting signals intelligence operations; Zorsecurity (aka Esage Lab), which provided the GRU with technical research and development; and Autonomous Noncommercial Organization "Professional Association of Designers of Data Processing Systems" (ANO PO KSI), which provided specialized training to the GRU
- Four individual officers of the GRU: Igor Valentinovich Korobov, the current Chief of the GRU; Sergey Aleksandrovich Gizunov, Deputy Chief of the GRU; Igor Olegovich Kostyukov, a First Deputy Chief of the GRU; and Vladimir Stepanovich Alexseyev, also a First Deputy Chief of the GRU.

In addition, OFAC designated two Russian individuals under a pre-existing portion of Executive Order 13694 for using cyber--enabled means to cause misappropriation of funds and personal identifying information, explaining the bases for such designations as indicated below:

- Evgeniy Mikhailovich Bogachev, who engaged in significant malicious cyber--enabled misappropriation of financial information for private financial gain; Bogachev and his associates were responsible for the theft of more than $100 million from U.S. financial institutions, Fortune 500 firms, universities and government agencies
- Aleksey Alekseyevich Belan, who engaged in significant malicious cyber-enabled misappropriation of personal identifiers for private financial gain; Belan compromised the computer networks of at least three major United States--based e-commerce companies, and he used his unauthorized access to steal user data belonging to approximately 200 million accounts worldwide and then actively engaged in successful efforts to sell the stolen information for private financial gain.

Both men have multiple arrest warrants pending in the United States for various computer--related crimes and remain on the FBI's Most Wanted List.

U.S. persons are prohibited from dealing with SDNs, and all assets of SDNs that are currently in, or come within, the United States or the possession or control of a U.S. person are blocked, and U.S. persons are generally prohibited from engaging in transactions with them. Any entities that these SDNs own (defined as a direct or indirect ownership interest of 50 percent or more) are also blocked, regardless of whether those entities are separately named on the SDN List, and U.S. persons are generally prohibited from engaging in transactions with such entities as well. The individuals designated as SDNs will also be denied entry into the United States.

Corresponding Additions to the Entity List

Following OFAC's designations, BIS added the two Russian intelligence agencies (GRU and FSB) and the three companies (Special Technology Center, Zorsecurity and ANO PO KSI) to the Entity List.

As a result of such designations, additional licensing requirements and restrictions apply to exports, re-exports and transfers (in-country) under the Export Administration Regulations (EAR) to such entities. Specifically, a license is required where items subject to the EAR are to be exported, re-exported, or transferred (in-country) to any of the entities added to the Entity List or in which such entities act as purchaser, intermediate consignee, ultimate consignee, or end-user. No license exceptions are available and BIS has imposed a presumption of denial policy to any license applications for the export, re-export or transfer of items subject to the EAR to these entities.

Practical Implications

Entities and individuals subject to U.S. jurisdiction should ensure that they do not engage in impermissible transactions with persons named on OFAC's SDN List or any entity owned by such persons. Exporters should also ensure that their export compliance programs have adequate measures in place to address the export, re-export and transfer restrictions imposed by BIS. Additionally, U.S. officials are encouraging the public to review the declassified technical information relating to the cyber activities by Russia to help identify, detect and disrupt cyber activities that may have occurred or remain ongoing.

Additional Information

The White House: Amended Executive Order, President Obama's Statement on the Executive Order and Fact Sheet

The White House Blog: The Administration's Response to Russia: What You Need to Know

Bureau of Industry and Security: Addition of Certain Entities to the Entity List

Contact Information

If you have any questions regarding this alert, please contact:

Daniel F. Feldman
feldman@akingump.com
+1 202.887.4035
Washington, D.C.

Jonathan C. Poling
jpoling@akingump.com
+1 202.887.4029
Washington, D.C.

Wynn H. Segall
wsegall@akingump.com
+1 202.887.4573
Washington, D.C.

Melissa J. Schwartz
mjschwartz@akingump.com
+1 202.887.4539
Washington, D.C.

Alexis G. Guinan
aguinan@akingump.com
+1 202.887.4318
Washington, D.C.