

Treasury Targets Russian Operatives over Election Interference, World Anti-Doping Agency Hacking, and Other Malign Activities

December 19, 2018

Washington – Today, the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) took action in response to Russia’s continued disregard for international norms. Specifically, OFAC designated a former officer of Russia’s Main Intelligence Directorate (GRU) for having acted on behalf of sanctioned oligarch Oleg Deripaska (Deripaska). OFAC also issued new designations related to the Internet Research Agency (IRA), an entity previously sanctioned for its efforts to interfere in U.S. elections. Today’s action also includes the designation of 15 members of the GRU, a previously designated Russian military intelligence organization, for their involvement in a wide range of malign activity, including attempting to interfere in the 2016 U.S. election, efforts to undermine international organizations through cyber-enabled means, and an assassination attempt in the United Kingdom. These 15 operatives are being sanctioned pursuant to the Countering America’s Adversaries Through Sanctions Act (CAATSA). To date, this Administration has sanctioned 272 Russia-related individuals and entities for a broad range of malign activities.

“Treasury is sanctioning Russian intelligence operatives involved in cyber operations to interfere with the 2016 election and a wide range of other malign activities. We are taking action against operatives working on behalf of a sanctioned oligarch, hacking the World Anti-Doping Agency and other international organizations, and engaging in other subversive actions,” said Steven T. Mnuchin, Secretary of the Treasury. “The United States will continue to work with international allies and partners to take collective action to deter and defend against sustained malign activity by Russia, its proxies, and intelligence agencies.”

As a result of today’s designations, all property and interests in property of these persons subject to or transiting U.S. jurisdiction are blocked, and U.S. persons are generally prohibited from engaging in transactions with them.

OLEG DERIPASKA RELATED DESIGNATION

Victor Alekseyevich Boyarkin (Boyarkin) is a former GRU officer who reports directly to Deripaska and has led business negotiations on Deripaska's behalf. Deripaska and Boyarkin were involved in providing Russian financial support to a Montenegrin political party ahead of Montenegro's 2016 elections. Boyarkin was designated pursuant to Executive Orders (E.O.) 13661 and 13662 for having acted or purported to act for or on behalf of, directly or indirectly, Oleg Deripaska, who was previously designated pursuant to E.O. 13661 for having acted or purported to act for or on behalf of a senior Russian government official, as well as pursuant to E.O. 13662 for operating in the energy sector of the Russian Federation economy, as well as with entities 50 percent or more owned by designated persons.

ATTEMPTED ELECTION INTERFERENCE

Project Lakhta

Today, OFAC also designated several entities and individuals related to Project Lakhta, a broad Russian effort that includes the IRA, designated previously under E.O. 13694, as amended, which has sought to interfere in political and electoral systems worldwide. Since at least 2014, Project Lakhta has used among other things, fictitious online personas that posed as U.S. persons in an effort to interfere in U.S. elections, as the IRA did during the 2016 U.S. election. Concord Management and Consulting LLC and Concord Catering — two entities owned by Yevgeniy Prigozhin (Prigozhin) — controlled Project Lakhta's funding, recommended personnel, and oversaw Project Lakhta's activities. Concord Management and Consulting LLC, Concord Catering, and Prigozhin were all previously designated pursuant to E.O. 13694, as amended, on March 15, 2018 for providing funding to the IRA's operations. Prigozhin was also previously designated for materially assisting senior officials of the Russian Federation under E.O. 13661, while Concord Management and Consulting LLC and Concord Catering were designated under E.O. 13661 on June 20, 2017.

Since 2014, Project Lakhta concealed its activities by operating through several entities to include the IRA, **Nevskiy News LLC**, **Economy Today LLC**, and the **Federal News Agency LLC**. As a result, Nevskiy News LLC, Economy Today LLC, and the Federal News Agency LLC were designated pursuant to E.O. 13694, as amended, for being owned or controlled by or having acted or purported to act for or on behalf of, directly or indirectly, Concord Management and Consulting LLC and Concord Catering.

Within weeks after the designation of the IRA, the Federal News Agency LLC — an entity utilized by Project Lakhta to obscure its activities that was also designated today — announced that it was creating a new Russian-funded, English-language website called **USA Really**. USA Really, which is operated by **Alexander Aleksandrovich Malkevich (Malkevich)**, engaged in efforts to post content focused on divisive political issues but is generally riddled with inaccuracies. In June 2018, USA Really attempted to hold a political rally in the United States, though its efforts were unsuccessful. As of June 2018, Malkevich was a member of Russia's Civic Chamber commission on mass media, which serves in a consultative role to the Russian government. Based on this activity, USA Really was designated pursuant to E.O. 13694, as amended, for being owned or controlled by the Federal News Agency LLC, while Malkevich was designated pursuant to E.O. 13694, as amended, for having acted or purported to act for or on behalf of, directly or indirectly, USA Really.

As of 2018, **Elena Alekseevna Khusyaynova (Khusyaynova)** served as the Chief Accountant in Project Lakhta's finance department, where she managed Project Lakhta's budgeting and payment of expenses associated with its social media operations, advertising campaigns, infrastructure, and registration of legal entities used to further its activities. Khusyaynova maintained Project Lakhta's monthly budgets and submitted requests to Concord Management and Consulting LLC and Concord Catering. As a result of these activities, Treasury designated Khusyaynova pursuant to E.O. 13694, as amended, for having acted or purported to act for or on behalf of, directly or indirectly, Concord Management and Consulting LLC and Concord Catering. Khusyaynova is also the subject of a criminal complaint announced on October 19, 2018.

GRU ATTEMPTED ELECTION INTERFERENCE

Nine Russian GRU officers were designated today for their direct involvement in efforts to interfere in the 2016 U.S. election by targeting election systems and political parties, as well as releasing stolen election-related documents. These nine individuals worked within Unit 26165 and Unit 74455 of the GRU. Unit 26165 engaged in cyber operations that involved the staged release of documents stolen through computer intrusions. Unit 74455 assisted in the release of stolen documents through various online personas, promoted those releases, and then aided in the publication of stolen content on social media accounts operated by the GRU. These nine GRU officers are subjects of an indictment announced on July 13, 2018.

Viktor Borisovich Netyksho (Netyksho) was designated pursuant to CAATSA Section 224 for knowingly engaging in significant activities undermining cybersecurity against any person, including a democratic institution or government, on behalf of the Government of the Russian Federation, and for acting or purporting to act for or on behalf of, directly or indirectly, the GRU. As of March 2016, Netyksho was in command of Unit 26165 of the GRU.

Boris Alekseyevich Antonov (Antonov) was designated pursuant to CAATSA Section 224 for knowingly engaging in significant activities undermining cybersecurity against any person, including a democratic institution or government, on behalf of the Government of the Russian Federation, and for acting or purporting to act for or on behalf of, directly or indirectly, the GRU. As of March 2016, Antonov was a Major assigned to Unit 26165 of the GRU and was responsible for supervising those who targeted the 2016 U.S. Presidential election.

Ivan Sergeyeovich Yermakov (Yermakov) was designated pursuant to CAATSA Section 224 for knowingly engaging in significant activities undermining cybersecurity against any person, including a democratic institution or government, on behalf of the Government of the Russian Federation, and for acting or purporting to act for or on behalf of, directly or indirectly, the GRU. As of March 2016, Yermakov was an officer assigned to Unit 26165 of the GRU. Between March and May 2016, Yermakov participated in the hacking of email accounts and servers associated with the 2016 U.S. election. Yermakov also played an integral role in compromising WADA's database in 2016.

Aleksey Viktorovich Lukashev (Lukashev) was designated pursuant to CAATSA Section 224 for knowingly engaging in significant activities undermining cybersecurity against any person, including a democratic institution or government, on behalf of the Government of the Russian Federation, and for acting or purporting to act for or on behalf of, directly or indirectly, the GRU. As of March 2016, Yermakov was a Senior Lieutenant within Unit 26165 of the GRU who sent spearphishing emails to campaign members associated with the 2016 U.S. election.

Nikolay Yuryevich Kozachek (Kozachek) was designated pursuant to CAATSA Section 224 for knowingly engaging in significant activities undermining cybersecurity against any person, including a democratic institution or government, on behalf of the Government of the Russian Federation, and for acting or purporting to act for or on behalf of, directly or indirectly, the GRU. As of March 2016, Kozachek was a Lieutenant Captain assigned to Unit 26165 of the GRU. Kozachek also developed and monitored malware utilized by the GRU used to hack into networks associated with the 2016 U.S. election.

Artem Andreyevich Malyshev (Malyshev) was designated pursuant to CAATSA Section 224 for knowingly engaging in significant activities undermining cybersecurity against any person, including a democratic institution or government, on behalf of the Government of the Russian Federation, and for acting or purporting to act for or on behalf of, directly or indirectly, the GRU. As of March 2016, Malyshev was a Second Lieutenant within Unit 26165 of the GRU who monitored malware implanted by the GRU on networks associated with the 2016 U.S. election. Malyshev also played an integral role in compromising WADA's database in 2016.

Aleksandr Vladimirovich Osadchuk (Osadchuk) was designated pursuant to CAATSA Section 224 for knowingly engaging in significant activities undermining cybersecurity against any person, including a democratic institution or government, on behalf of the Government of the Russian Federation, and for acting or purporting to act for or on behalf of, directly or indirectly, the GRU. As of March 2016, Osadchuk was the commanding officer of Unit 74455 of the GRU.

Aleksey Aleksandrovich Potemkin (Potemkin) was designated pursuant to CAATSA Section 224 for knowingly engaging in significant activities undermining cybersecurity against any person, including a democratic institution or government, on behalf of the Government of the Russian Federation, and for acting or purporting to act for or on behalf of, directly or indirectly, the GRU. As of March 2016, Potemkin was an officer assigned to Unit 74455 of the GRU and supervised a department that was responsible for the administration of computer infrastructure used in the release of stolen documents online.

Anatoliy Sergeyevich Kovalev (Kovalev) was designated pursuant to CAATSA Section 224 for knowingly engaging in significant activities undermining cybersecurity against any person, including a democratic institution or government, on behalf of the Government of the Russian Federation, and for acting or purporting to act for or on behalf of, directly or indirectly, the GRU. As of March 2016, Kovalev was an officer assigned to Unit 74455 of the GRU. By July 2016, Kovalev hacked the website of a state board of elections and stole voter information. By August 2016, Kovalev also hacked into computers of a U.S. company that supplied software used to verify voter registration information for the 2016 U.S. elections.

WORLD ANTI-DOPING AGENCY-RELATED DESIGNATIONS

Between 2016 and 2018, Russia targeted the World Anti-Doping Agency (WADA), the Organization for the Prohibition of Chemical Weapons (OPCW), and other international nonpolitical organizations using cyber hacking techniques. In 2016, WADA announced that malicious actors, who were in fact the GRU, had accessed data on its networks through

spearphishing attacks and then illegally released confidential medical data pertaining to professional athletes, with modifications from the original version in some instances. These cyber-enabled operations followed WADA's exposure of Russia's extensive state-sponsored doping program in an independent WADA commission report. On October 4, 2018, the U.S. Department of Justice indicted and Dutch authorities announced the expulsion of the four GRU officers identified below involved in malicious cyber activity targeting the OPCW, the international organization responsible for eradicating chemical weapons worldwide under a United Nations mandate, who Treasury is also designating today.

Specifically, OFAC designated **Aleksei Morenets (Morenets)** and **Evgenii Serebriakov (Serebriakov)**, officers in the GRU who played an integral role in compromising WADA's database in 2016, as well as assisting the GRU's attempted cyber intrusions into the OPCW. Morenets and Serebriakov were designated pursuant to CAATSA Section 224 for knowingly engaging in significant activities undermining cybersecurity against any person, including a democratic institution or government, on behalf of the Government of the Russian Federation, and for acting or purporting to act for or on behalf of, directly or indirectly, the GRU.

Oleg Sotnikov (Sotnikov) served as a Russian military intelligence officer who provided support to the GRU during its targeting of the OPCW, and was designated pursuant to CAATSA Section 224 for knowingly engaging in significant activities undermining cybersecurity against any person, including a democratic institution or government, on behalf of the Government of the Russian Federation, and for acting or purporting to act for or on behalf of, directly or indirectly, the GRU.

Alexey Minin (Minin) also served as a Russian military intelligence officer who supported the targeting of the OPCW, and also worked with Sotnikov to assemble hacking equipment during the operation. Minin was designated pursuant to CAATSA Section 224 for knowingly engaging in significant activities undermining cybersecurity against any person, including a democratic institution or government, on behalf of the Government of the Russian Federation, and for acting or purporting to act for or on behalf of, directly or indirectly, the GRU.

NOVICHOK NERVE AGENT ATTACK

In a brazen attack that defied international norms and Russia's obligations under the Chemical Weapons Convention, GRU officers attempted to assassinate Sergei Skripal and his daughter by using a military grade nerve agent called Novichok in Salisbury, England in March 2018. Skripal, his daughter, and a police officer survived the attack; however, months later, two additional

British nationals were exposed to the agent, one of whom died as a result. Many governments, including the United States, United Kingdom, Germany, France, and Canada, have made it clear that the Russian government was responsible for this attack.

Today OFAC is designating **Alexander Petrov (Petrov)** and **Ruslan Boshirov (Boshirov)**, the GRU officers responsible for carrying out this attempted assassination of Sergei Skripal and his daughter. Petrov and Boshirov were designated pursuant to CAATSA Section 224 for acting or purporting to act for or on behalf of, directly or indirectly, the GRU.

STATE DEPARTMENT CONCURRENT ACTION

In a concurrent action, the Department of State also added 12 individuals and entities designated today to the List of Specified Persons under Section 231 of CAATSA for being part of, or operating for or on behalf of, the defense or intelligence sector of the Russian Federation. As a result of this action, any person determined to knowingly engage in a significant transaction with these 12 individuals will be subject to CAATSA Section 231 sanctions.

[Identifying information on the individuals and entities designated today.](#)

####