Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks

March 15, 2018

Washington – Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) designated five entities and 19 individuals under the Countering America's Adversaries Through Sanctions Act (CAATSA) as well as Executive Order (E.O.) 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," as amended, and codified pursuant to CAATSA.

"The Administration is confronting and countering malign Russian cyber activity, including their attempted interference in U.S. elections, destructive cyber-attacks, and intrusions targeting critical infrastructure," said Treasury Secretary Steven T. Mnuchin. "These targeted sanctions are a part of a broader effort to address the ongoing nefarious attacks emanating from Russia. Treasury intends to impose additional CAATSA sanctions, informed by our intelligence community, to hold Russian government officials and oligarchs accountable for their destabilizing activities by severing their access to the U.S. financial system."

Today's action counters Russia's continuing destabilizing activities, ranging from interference in the 2016 U.S. election to conducting destructive cyber-attacks, including the NotPetya attack, a cyber-attack attributed to the Russian military on February 15, 2018 in statements released by the White House and the British Government. This cyber-attack was the most destructive and costly cyber-attack in history. The attack resulted in billions of dollars in damage across Europe, Asia, and the United States, and significantly disrupted global shipping, trade, and the production of medicines. Additionally, several hospitals in the United States were unable to create electronic records for more than a week.

Since at least March 2016, Russian government cyber actors have also targeted U.S. government entities and multiple U.S. critical infrastructure sectors, including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors. Indicators of compromise, and technical details on the tactics, techniques, and procedures, are provided in the recent technical alert issued by the Department of Homeland Security and Federal Bureau of Investigation.

In addition to countering Russia’s malign cyber activity, Treasury continues to pressure Russia for its ongoing efforts to destabilize Ukraine, occupy Crimea, meddle in elections, as well as for its endemic corruption and human rights abuses. The recent use of a military-grade nerve agent in an attempt to murder two UK citizens further demonstrates the reckless and irresponsible conduct of its government. To date, this Administration has sanctioned more than 100 individuals and entities under our Ukraine and Russia-related sanctions authorities, including 21 individuals, nine entities, and 12 subsidiaries that are owned 50 percent or more by previously sanctioned Russian companies on January 26, 2018. These sanctions are in addition to other ongoing efforts by Treasury to address destabilizing activity emanating from within Russia, including our sanctioning of Russians targeted for activities related to the North Korea sanctions program, the Global Magnitsky program, and the Sergei Magnitsky Act.

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

E.O. 13694 SANCTIONS

Today’s action includes the designation of three entities and 13 individuals pursuant to E.O. 13694, as amended, which targets malicious cyber actors, including those involved in interfering with election processes or institutions.

The **Internet Research Agency LLC** (IRA) tampered with, altered, or caused a misappropriation of information with the purpose or effect of interfering with or undermining election processes and institutions. Specifically, the IRA tampered with or altered information in order to interfere with the 2016 U.S. election. The IRA created and managed a vast number of fake online personas that posed as legitimate U.S. persons to include grassroots organizations, interest groups, and a state political party on social media. Through this activity, the IRA posted thousands of ads that reached millions of people online. The IRA also organized and coordinated political rallies during the run-up to the 2016 election, all while hiding its Russian identity. Further, the IRA unlawfully utilized personally identifiable information from U.S. persons to open financial accounts to help fund IRA operations.

Yevgeniy Viktorovich Prigozhin (Prigozhin) provided material assistance to the IRA. Specifically, Prigozhin funded the operations of the IRA. OFAC previously designated Prigozhin under E.O. 13661, “Blocking Property of Additional Persons Contributing to the Situation in Ukraine,” on December 20, 2016.

Concord Management and Consulting LLC provided material assistance to the IRA. Concord Management and Consulting LLC, which is controlled by Prigozhin, provided funding to the IRA. Concord Management and Consulting LLC was previously designated under E.O. 13661 on June 20, 2017.

Concord Catering provided material assistance to the IRA. Concord Catering, which is controlled by Prigozhin, provided funding to the IRA. OFAC previously designated Concord Catering under E.O. 13661 on June 20, 2017.

Dzheykhun Nasimi Ogly Aslanov (Aslanov) acted for or on behalf of and provided material and technological support to the IRA. Aslanov acted as the head of the translator project, a department which focused on the United States and conducted operations on multiple social media platforms. He also oversaw many of the operations that targeted the 2016 U.S. election.

Anna Vladislavovna Bogacheva (Bogacheva) acted for or on behalf of and provided material and technological support to the IRA. Bogacheva worked for the IRA from at least April 2014 to July 2014. She worked on the translator project.

Maria Anatolyevna Bovda (Bovda) acted for or on behalf of and provided material and technological support to the IRA. Bovda worked for the IRA from at least November 2013 to October 2014. She served as the head of the translator project and held other positions within the firm.

Robert Sergeyevich Bovda (Bovda) acted for or on behalf of and provided material and technological support to the IRA. Bovda worked for the IRA from at least November 2013 to October 2014. He served as the deputy head of the translator project and held other positions within the firm.

Mikhail Leonidovich Burchik (Burchik) acted for or on behalf of and provided material and technological support to the IRA. Burchik acted as the executive director of the IRA and held the firm’s second-highest ranking position. He was involved in operational planning, infrastructure, and personnel throughout the firm’s operations to interfere in the U.S. political system.

Mikhail Ivanovich Bystrov (Bystrov) acted for or on behalf of and provided material and technological support to the IRA. Bystrov acted as the general director of the IRA and served as the head of other entities used by the firm to mask its operations.

Irina Viktorovna Kaverzina (Kaverzina) acted for or on behalf of and provided material and technological support to the IRA. Kaverzina worked for the translator project and operated multiple U.S. personas that she used to post, monitor, and update social media content for the IRA.

Aleksandra Yuryevna Krylova (Krylova) acted for or on behalf of and provided material and technological support to the IRA. Krylova worked for the IRA from at least September 2013 to November 2014, where she served as a director and was the firm's third-highest ranking position.

Vadim Vladimirovich Podkopaev (Podkopaev) acted for or on behalf of and provided material and technological support to the IRA. Podkopaev was responsible for conducting U.S.-focused research and drafting social media content for the IRA.

Sergey Pavlovich Polozov (Polozov) acted for or on behalf of and provided material and technological support to the IRA. Polozov acted as the manager of the IRA's information technology department and oversaw the procurement of U.S. servers and other computer infrastructure that masked the firm's location when conducting operations within the United States.

Gleb Igorevich Vasilchenko (Vasilchenko) acted for or on behalf of and provided material and technological support to the IRA. Vasilchenko worked for the IRA from at least August 2014 to September 2016, and was responsible for controlling social media content and posing as U.S. persons or U.S. grassroots organizations.

Vladimir Venkov (Venkov) acted for or on behalf of and provided material and technological support to the IRA. Venkov worked for the translator project and operated multiple U.S. personas that were used to post, monitor, and update social media content for the IRA.

These entities and individuals are subjects of an indictment announced on February 16, 2018.

CAATSA SANCTIONS

Today's action also includes the designation of two entities and six individuals pursuant to section 224 of CAATSA, which targets cyber actors operating on behalf of the Russian government.

Federal Security Service (FSB), a Russian intelligence organization, knowingly engages in significant activities that undermine cybersecurity on behalf of the Russian government. Specifically, the FSB has utilized its cyber tools to target Russian journalists and politicians critical of the Russian government; Russian citizens and government officials; former officials from countries bordering Russia; and U.S. government officials, including cyber security, diplomatic, military, and White House personnel. Additionally, in 2017, the U.S. Department of Justice indicted two FSB officers for their involvement in the 2014 hacking of Yahoo that compromised millions of Yahoo accounts. OFAC previously sanctioned the FSB under E.O. 13694, as amended, on December 28, 2016.

Main Intelligence Directorate (GRU), a Russian military intelligence organization, knowingly engages in significant activities that undermine cybersecurity on behalf of the Russian government. The GRU was directly involved in interfering in the 2016 U.S. election through cyber-enabled activities. The Russian military, of which the GRU is a part, was also directly responsible for the NotPetya cyber-attack in 2017. OFAC previously sanctioned the GRU under E.O. 13694, as amended, on December 28, 2016.

Sergei Afanasyev (Afanasyev) acts for or on behalf of the GRU. As of February 2017, Afanasyev was a senior GRU official.

Vladimir Alexseyev (Alexseyev) acts for or on behalf of the GRU. As of December 2016, Alexseyev was a First Deputy Chief of the GRU. OFAC previously sanctioned Alexseyev under E.O. 13694, as amended, on December 28, 2016.

Sergey Gizunov (Gizunov) acts for or on behalf of the GRU. As of July 2017, Gizunov was the Deputy Chief of the GRU. OFAC previously sanctioned Gizunov under E.O. 13694, as amended, on December 28, 2016.

Igor Korobov (Korobov) acts for or on behalf of the GRU. As of January 2018, Korobov was the Chief of the GRU. OFAC previously sanctioned Korobov under E.O. 13694, as amended, on December 28, 2016.

Igor Kostyukov (Kostyukov) acts for or on behalf of the GRU. As of December 2016, Kostukov was a First Deputy Chief of the GRU. OFAC previously sanctioned Kostyukov under E.O. 13694, as amended, on December 28, 2016.

Grigoriy Molchanov (Molchanov) acts for or on behalf of the GRU. As of April 2016, Molchanov was a senior GRU official.

Identifying information on the individuals and entities designated today.

####