Treasury Sanctions Russia with Sweeping New Sanctions Authority

home.treasury.gov/news/press-releases/jy0127

April 15, 2021

WASHINGTON — Today, the U.S. Department of the Treasury took multiple sanctions actions under a new Executive Order (E.O.) targeting aggressive and harmful activities by the Government of the Russian Federation. Treasury's actions include the implementation of new prohibitions on certain dealings in Russian sovereign debt, as well as targeted sanctions on technology companies that support the Russian Intelligence Services' efforts to carry out malicious cyber activities against the United States.

"The President signed this sweeping new authority to confront Russia's continued and growing malign behavior," said Treasury Secretary Janet L. Yellen. "Treasury is leveraging this new authority to impose costs on the Russian government for its unacceptable conduct, including by limiting Russia's ability to finance its activities and by targeting Russia's malicious and disruptive cyber capabilities."

NEW AUTHORITY IN RESPONSE TO RUSSIAN MALIGN ACTIVITIES

The E.O. of April 15, 2021, "Blocking Property with Respect to Specified Harmful Foreign Activities of the Government of the Russian Federation," elevates the U.S. government's capacity to deploy strategic and economically impactful sanctions to deter and respond to Russia's destabilizing behavior. In particular, this new E.O. authorizes sanctions to counter

Russia's harmful foreign activities that threaten the national security and foreign policy of the United States, including: undermining the conduct of free and fair elections and democratic institutions in the United States and its allies and partners; engaging in and facilitating malicious cyber activities against the United States and its allies and partners that threaten the free flow of information; fostering and using transnational corruption to influence foreign governments; pursuing extraterritorial activities targeting dissidents or journalists; undermining security in countries and regions important to the United States' national security; and violating well-established principles of international law, including respect for the territorial integrity of states. To address these threats, the E.O. of April 15, 2021 authorizes sanctions on a wide range of persons, including, among others, those operating in the technology and defense and related materiel sectors of the Russian Federation economy, and in any additional sectors of the Russian Federation economy as may be determined by the Secretary of the Treasury, in consultation with the Secretary of State.

SOVEREIGN DEBT PROHIBITIONS

Pursuant to the E.O. of April 15, 2021, Treasury's Office of Foreign Assets Control (OFAC) is issuing a directive that generally prohibits U.S. financial institutions from participating in the primary market for ruble or non-ruble denominated bonds issued after June 14, 2021 by the Central Bank of the Russian Federation, the National Wealth Fund of the Russian Federation, or the Ministry of Finance of the Russian Federation, and further prohibits U.S. financial institutions from lending ruble or non-ruble denominated funds to these three entities. This directive expands upon existing prohibitions on certain dealings in Russian sovereign debt that have been in place since August 2019.

TREASURY DESIGNATES RUSSIAN COMPANIES IN THE TECHNOLOGY SECTOR SUPPORTING RUSSIAN INTELLIGENCE SERVICES

Treasury's first use of the E.O. of April 15, 2021 targets companies operating in the technology sector of the Russian Federation economy that support Russian Intelligence Services. The following companies are designated for operating in the technology sector of the Russian Federation economy: **ERA Technopolis; Pasit, AO** (Pasit); **Federal State Autonomous Scientific Establishment Scientific Research Institute Specialized Security Computing Devices and Automation** (SVA); **Neobit, OOO** (Neobit); **Advanced System Technology, AO** (AST); and **Pozitiv Teknolodzhiz, AO** (Positive Technologies).

ERA Technopolis is a research center and technology park funded and operated by the Russian Ministry of Defense. ERA Technopolis houses and supports units of Russia's Main Intelligence Directorate (GRU) responsible for offensive cyber and information operations and leverages the personnel and expertise of the Russian technology sector to develop military and dual-use technologies.

Pasit is a Russia-based information technology (IT) company that conducted research and development in support of Russia's Foreign Intelligence Service's (SVR) malicious cyber operations.

SVA is a Russian state-owned research institute specializing in advanced systems for information security located in Russia. SVA conducted research and development in support of the SVR's malicious cyber operations.

Neobit is a Saint Petersburg, Russia-based IT security firm whose clients include the Russian Ministry of Defense, SVR, and Russia's Federal Security Service (FSB). Neobit conducted research and development in support of the cyber operations conducted by the FSB, GRU, and SVR. Neobit was also designated today pursuant to cyber-related E.O. 13694, as amended by E.O. 13757, WMD-related E.O. 13382, and the Countering America's Adversaries Through Sanctions Act (CAATSA) for providing material support to the GRU.

AST is a Russian IT security firm whose clients include the Russian Ministry of Defense, SVR, and FSB. AST provided technical support to cyber operations conducted by the FSB, GRU, and SVR. AST was also designated today pursuant to E.O. 13694, E.O. 13382, and CAATSA for providing support to the FSB.

Positive Technologies is a Russian IT security firm that supports Russian Government clients, including the FSB. Positive Technologies provides computer network security solutions to Russian businesses, foreign governments, and international companies and hosts large-scale conventions that are used as recruiting events for the FSB and GRU. Positive Technologies was also designated today pursuant to E.O. 13694, E.O. 13382, and CAATSA for providing support to the FSB.

SANCTIONS TARGET RUSSIAN MALICIOUS CYBER ACTORS

The Russian Intelligence Services — specifically the Federal Security Service (FSB), Russia's Main Intelligence Directorate (GRU), and the Foreign Intelligence Service (SVR) — have executed some of the most dangerous and disruptive cyber attacks in recent history, including the SolarWinds cyber attack. The FSB and GRU were previously sanctioned in 2016, and again in 2018, for malicious cyber activity, and most recently on March 2, 2021 for activities related to the proliferation of weapons of mass destruction (WMD).

The FSB was involved in the August 2020 poisoning of Aleksey Navalny with a chemical weapon, specifically a nerve agent known as Novichok. The GRU also engaged in activities that materially contributed to the possession, transportation, and use of Novichok related to a March 2018 poisoning in the United Kingdom.

The FSB has also used its cyber capabilities to target Russian journalists and others who openly criticize the regime, as well as U.S. government personnel and millions of private citizens around the world. To bolster its malicious cyber operations, the FSB cultivates and

co-opts criminal hackers, including the previously designated Evil Corp, enabling them to engage in disruptive ransomware attacks and phishing campaigns.

The GRU's malign cyber activities include deployment of the NotPetya and Olympic Destroyer malware; intrusions targeting the Organization for the Prohibition of Chemical Weapons and the World Anti-Doping Agency; cyber attacks on government systems and critical infrastructure in Ukraine and the state of Georgia; and hack-and-leak operations targeting elections in the United States and France.

In addition, the Russian Intelligence Services' third arm, the SVR, is responsible for the 2020 exploit of the SolarWinds Orion platform and other information technology infrastructures. This intrusion compromised thousands of U.S. government and private sector networks. The scope and scale of this compromise combined with Russia's history of carrying out reckless and disruptive cyber operations makes it a national security concern. The SVR has put at risk the global technology supply chain by allowing malware to be installed on the machines of tens of thousands of SolarWinds' customers. Victims of the compromise include the financial sector, critical infrastructure, government networks, and many others. Further, this incident will cost businesses and consumers in the United States and worldwide millions of dollars to fully address.

Additionally, the SVR stole "red team tools," which mimic cyber attacks to help customers better protect themselves, from a U.S. cyber security company. These tools, if made public or used offensively by the SVR or other actors, would create additional opportunities for malign actors to target computer systems worldwide.

The private and state-owned companies designated today enable the Russian Intelligence Services' cyber activities. These companies provide a range of services to the FSB, GRU, and SVR, ranging from providing expertise, to developing tools and infrastructure, to facilitating malicious cyber activities.

SANCTIONS IMPLICATIONS

As a result of today's action, all property and interests in property of the designated persons described above that are in the United States or in the possession or control of U.S. persons are blocked and must be reported to OFAC. In addition, any entities that are owned, directly or indirectly, 50 percent or more by one or more blocked persons are also blocked. Unless authorized by a general or specific license issued by OFAC, or exempt, OFAC's regulations generally prohibit all transactions by U.S. persons or within (or transiting) the United States that involve any property or interests in property of designated or otherwise blocked persons. The prohibitions include the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any blocked person or the receipt of any contribution or provision of funds, goods, or services from any such person.

###

Use featured image

Off