WILMERHALE

# *President Biden Signs New Executive Order Escalating US Sanctions Against Russia*

April 16, 2021

On April 15, 2021, President Biden signed a new executive order, Blocking Property with Respect to Specified Harmful Foreign Activities of the Government of the Russian Federation, escalating US sanctions against the Russian government and against Russian actors that threaten US interests. Concurrently, the Department of the Treasury's Office of Foreign Assets Control (OFAC) made several dozen new sanctions designations—some in coordination with US allies—targeting individuals and entities in connection with Russian interference in the 2020 US presidential election, Russia's occupation of Crimea, and the cyber-espionage campaign that exploited the SolarWinds platform. OFAC issued a new directive pursuant to the executive order, prohibiting US financial institutions from participating in certain transactions involving Russian sovereign debt and from lending to the Russian government. OFAC also issued several new frequently asked questions (FAQs) providing guidance on its implementation of the new executive order.

The executive order, new OFAC designations and new financial restrictions are part of a broader, coordinated effort by the Biden Administration to "impose costs for Russian Government actions that seek to harm us," which includes the expulsion of diplomatic personnel, the formal identification of the perpetrator of the SolarWinds hack and an increased commitment to cybersecurity in coordination with US allies.

Unlike some past US measures targeting Russia, the new executive order does not establish novel forms of sanctions. Instead, it largely fits within the existing paradigm of blocking sanctions, which require US companies to block, and report to OFAC, any property or property interests of the designated persons that are under their possession or control. As a practical matter, the OFAC sanctions designations underscore the importance of counterparty due diligence and risk-based, restrictive party screening, especially—though not exclusively—when doing business in Russia and elsewhere in the region. And while the new OFAC directive expands prohibitions on Russian sovereign debt, US sanctions targeting Russian sovereign debt that were put in place in 2019 already included a narrower set of restrictions under the Chemical and Biological Weapons Control

and Warfare Elimination (CBW) Act and Executive Order 13883. The new US sanctions against Russia do not include any so-called secondary sanctions, though such sanctions remain in effect under the Countering America's Adversaries Through Sanctions Act (CAATSA) and other statutes.

The Biden Administration stated that the United States seeks a "stable and predictable" relationship with Russia and specifically noted that the EO "sends a signal that the United States will impose costs in a strategic and economically impactful manner on Russia if it continues or escalates its destabilizing international actions." We recommend that companies with direct or indirect exposure to Russia or Russian counterparties carefully review the new measures and continue to closely follow developments in United States–Russia relations as continued "harmful foreign activities" by Russia are likely to result in additional US sanctions.

***April 15 Executive Order***

The April 15 executive order, Blocking Property with Respect to Specified Harmful Foreign Activities of the Government of the Russian Federation (April 15 EO), blocks the property and interests in property under US jurisdiction of persons determined by the Secretary of the Treasury or, in some cases, the Secretary of State to engage in certain activities that threaten US national security or foreign policy interests. In particular, the following individuals and entities may be subject to US blocking sanctions:

- Those operating in the technology or defense sectors of the Russian economy, or in other sectors determined by the Secretary of the Treasury in consultation with the Secretary of State [Sec. 1(a)(i)];
- Those responsible for or complicit in, or those who have directly or indirectly engaged or attempted to engage in, the following activities for or on behalf of, or for the benefit of, the Russian government [Sec. 1(a)(ii)]:
  - Malicious cyber-enabled activities;
  - Interference in a US or other foreign government election;
  - Actions or policies that undermine democratic processes or institutions in the United States or abroad;
  - Transnational corruption;
  - Assassination, murder or other unlawful killing of, or infliction of other bodily harm against, a US person or a citizen or national of a US ally or partner;
  - Activities that undermine the peace, security, political stability, or territorial integrity of the United States, its allies, or its partners; or
  - Deceptive or structured transactions or dealings to circumvent US sanctions, including through the use of digital currencies or assets, or physical assets.

- Those who are or have been a leader, official, senior executive officer, or member of the board of directors of the Russian government, an entity that has (or whose members have) engaged in the activities enumerated under Sec. 1(a)(ii), or an entity blocked under the April 15 EO [Sec. 1(a)(iii)];
- A political subdivision, agency or instrumentality of the Russian government [Sec. 1(a)(iv)];
- A spouse or adult child of a blocked person under Sec. 1(a)(ii) or 1(a)(iii) [Sec. 1(a)(v)];
- Those who have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services in support of, the activities described in Sec. 1(a)(ii) or for or in support of a person blocked under the April 15 EO [Sec. 1(a)(vi)];
- Those who are owned or controlled by, or have acted for or on behalf of, the Russian government or a person blocked under the April 15 EO [Sec. 1(a)(vii)];
- Russian citizens or nationals, entities organized under Russian law, or persons ordinarily resident in Russia, that provide financial, material, or technological support for, or goods or services to or in support of, a sanctioned government [Sec. 1(b)]; or
- Russian citizens or nationals or entities organized under Russian law that are responsible for or complicit in, or have directly or indirectly engaged in or attempted to engage in, cutting or disrupting gas or energy supplies to Europe, the Caucasus or Asia [Sec. 1(c)].

Although the April 15 EO does not create a new sanctions framework, it contains several notable features, including broad authorities to target for designation individuals involved in corruption or other activities that are inconsistent with US national security and foreign policy interests.

First, the April 15 EO consolidates and simplifies, to some extent, several pre-existing sanctions authorities. For example, Executive Order 13848 already established the authority to impose blocking sanctions against persons determined to have engaged in foreign interference in a US election.

Other new criteria for sanctions designations are more general, however. Executive Order 13694, as amended by Executive Order 13757, authorized the imposition of blocking sanctions based on an enumerated list of activities that were characterized in those measures as "malicious cyber-enabled activities," whereas the April 15 EO simply authorizes the imposition of sanctions against those determined to be involved in "malicious cyber-enabled activities." Nothing prevents OFAC from designating persons under multiple sanctions authorities, and indeed, OFAC has already done so on April 15.

Second, several of the designation criteria target activities that threaten not only the United States but also its allies. For example, the April 15 EO authorizes the imposition of blocking sanctions against persons determined to have engaged in interference not only in US elections, but also in those of a foreign government; to have engaged in actions that undermine US democratic

processes or institutions, as well as those abroad; and to have engaged in unlawful killings not only of US persons, but also of citizens and nationals of US allies and partners.

Third, the April 15 EO delegates the authority to determine whether persons meet the criteria for designation to both the Secretary of the Treasury and the Secretary of State. Accordingly, sanctions designations under Sec. 1(a) of the April 15 EO may be made by either agency, provided that each consults with the other prior to any designation.[1] In addition, the April 15 EO requires that any determination under Sec. 1(a)(ii) also be made in consultation with the U.S. Attorney General. The prominent role that the Department of Justice will play in the implementation of these sanctions authorities reflects a whole-of-government approach to combating "harmful foreign activities" by Russia and, in particular, reflects the role that federal law enforcement is playing and will continue to play.

Fourth, the April 15 EO authorizes sanctions not only on those involved in the activities enumerated above but also on their spouses and adult children. This type of authority had not been a common feature of past executive orders addressing sanctions, though it was included in Executive Order 14014 of Feb. 10, 2021, Blocking Property With Respect to the Situation in Burma. The Biden Administration therefore appears increasingly willing to at least establish the authority to sanction the familial relations of the direct targets of US sanctions.[2]

Fifth, while past executive orders did authorize sanctions against Russian government officials and entities operating in certain sectors of the Russian economy (including state-owned firms), the April 15 EO authorizes sanctions against any agency or instrumentality of the Russian government. OFAC has relied on this authority to establish the new restrictions on Russian sovereign debt, discussed below. In addition, because the April 15 EO authorizes the imposition of sanctions against not only Russian government officials but also leaders, senior executive officers and members of the board of directors of "the Government of the Russian Federation"—which is a defined term that includes "any person owned, controlled, or directed by, or acting for or on behalf of, the Government of the Russian Federation"—individuals linked to Russian state-owned firms as officers and directors may now be subject to US sanctions. Likewise at risk of US sanctions are those individuals who have acted or purported to act on behalf of Russian state-owned firms.

Sixth, the executive order specifically calls attention to the use of digital currencies or assets to circumvent US sanctions. In addition, several of the new designations include, in their description, the designated person's digital currency address(es). The Treasury Department, including OFAC, has been increasingly focused on the use of digital currencies for illicit purposes, and the inclusion

[1] The April 15 EO delegates authority to make designations under Sec. 1(b), which concerns support to sanctioned governments, to the Secretary of the Treasury; it delegates authority to make designations under Sec. 1(c), which concerns disruptions to regional energy supply, to the Secretary of State.
[2] Notably, Sec. 228 of CAATSA already established secondary sanctions authority for the United States to sanction foreign persons who facilitate significant transactions for or on behalf of the children, spouse, parent or sibling of an individual subject to US sanctions with respect to Russia.

of this language in the executive order further signals that such use will be the subject of close enforcement scrutiny.

***Restrictions on Russian Sovereign Debt***

On April 15, OFAC issued Directive 1 under the April 15 EO. Directive 1 begins with OFAC's determination under Sec. 1(a)(iv) of the April 15 EO that the Central Bank of the Russian Federation, the National Wealth Fund of the Russian Federation, and the Ministry of Finance of the Russian Federation are political subdivisions, agencies, or instrumentalities of the Russian government. Rather than impose blocking sanctions against these entities, however, OFAC's Directive 1 subjects them to a relatively narrower set of restrictions. Specifically, beginning June 14, 2021, US financial institutions (a term defined in Directive 1) will be prohibited from (1) participating in the primary market for ruble or non-ruble denominated bonds issued after that date by any of those three entities; and (2) lending ruble or non-ruble denominated funds to those three entities.[3]

OFAC FAQ # 889 states unequivocally that Directive 1 does not prohibit US financial institutions from participating in the secondary market for Russian sovereign debt.

As noted above, Russian sovereign debt had already been the target of US sanctions under the CBW Act. Under the CBW Act Directive, US banks are prohibited from participating in the primary market of *non-ruble* denominated funds issued by the Russian sovereign, and from lending such funds to the Russian sovereign.[4] As OFAC reminds the public in newly issued FAQ # 890, these prohibitions apply to US banks (as that term is defined in the CBW Act Directive) even before June 14, 2021. But beginning on that date, Directive 1 will expand these prohibitions to include participation by US financial institutions (as that term is defined in Directive 1) not only in the primary market for non-ruble denominated funds, but also in the primary market for ruble denominated funds.

Notably, the scope of Directive 1 is narrower than that of the CBW Act Directive in its targeting of Russian agencies or instrumentalities. Whereas the CBW Act Directive defined the term "Russian sovereign" to mean any ministry, agency or sovereign fund of the Russian Federation *including* the Central Bank, National Wealth Fund and Ministry of Finance, Directive 1 applies *only* to bonds issued by or funds lent to those three entities. OFAC's new FAQ # 891 also affirms that the prohibitions in Directive 1 apply only to the named entities, not to entities owned 50 percent or more by those entities, whether individually or in the aggregate.

---

[3] Directive 1 specifically states that, other than the two categories of activities described above, "all other activities with" the three entities "involving their property or interests in property are permitted, provided such activities are not otherwise prohibited pursuant to the Order" or under other OFAC sanctions programs.

[4] In a background press call on the new sanctions, White House officials noted that prior restrictions on purchases of non-Ruble denominated Russian sovereign debt impacted a far smaller portion of sovereign debt issued—only less than 20 percent of sovereign debt issued by Russia is non-ruble denominated, whereas over 80 percent is ruble denominated. https://www.whitehouse.gov/briefing-room/press-briefings/2021/04/15/background-press-call-by-senior-administration-officials-on-russia/

While Directive 1 remains relatively narrow, e.g., because it is limited only to primary market trading in Russian sovereign debt, nothing prevents the Biden Administration from revising Directive 1 or issuing a new directive under the April 15 EO that would target secondary market trading in such debt. If the Biden Administration's efforts to establish a "stable and predictable" relationship with Russia falter, then it could impose additional, more expansive sanctions.

***Blocking Sanctions Under the Executive Order***

OFAC immediately exercised the designation authority under the April 15 EO, though most of the day's designations were pursuant to pre-existing authorities.

OFAC designated six Russian technology companies that each support Russian government information and/or cyber operations, including private firms with clients such as the Federal Security Service (FSB), the Foreign Intelligence Service (SVR) and the Main Intelligence Directorate. Among these are Pasit, AO, a Russia-based information technology (IT) company; SVA, a Russian state-owned research institute specializing in advanced systems for information security; and Positive Technologies, a Russian IT security firm that supports Russian government clients, including the FSB. OFAC also designed Positive Technologies under several other sanctions authorities.[5] The Treasury Department has provided information about these companies and their relationship to the Russian Intelligence Services, which can be found here.

***Additional Blocking Sanctions***

OFAC also designated 16 individuals and 16 entities pursuant to pre-existing authorities (including CAATSA and past executive orders) for attempting, at the direction of Russian government leadership, to influence the 2020 US presidential election. These include four disinformation and/or propaganda outlets run by or closely affiliated with the Russian Intelligence Services. They also include additional individuals and entities in the African network of Yevgeniy Prigozhin, whom OFAC has previously designated for his role in the Russian troll farm the Internet Research Agency (IRA), as well as Mr. Prigozhin's "complex network of shell and front companies" used to evade US sanctions and obscure his ownership in property. The sanctions include the designation of the Pakistan-based Second Eye Solution (SES), which, according to the Treasury Department, helps the IRA conceal its identity to evade sanctions by creating and selling fraudulent identities, as well as several Pakistani nationals and front companies associated with SES. The Treasury Department noted that fraudulent documents created by SES "are likely used at many online services to evade sanctions and anti-money laundering (AML) screening protocols beyond what OFAC has been able to identify," including social media, freelance job postings and commerce platforms. Finally, OFAC designated Konstantin Kilimnik, who is currently under indictment and wanted by the Federal Bureau of Investigation (FBI), for having engaged in foreign interference in the 2020 US

[5] The company was also designated pursuant to Executive Order 13694, Executive Order 13382 and CAATSA for providing support to the FSB.

presidential election. Additional information about these persons their relationship to the Russian Intelligence Services can be found here.

Finally, OFAC relied on two 2014 executive orders, issued in response to Russia's annexation of Crimea, to make eight designations against those associated with Russia's ongoing occupation and repression in Crimea. The designations fall into three categories: persons who have supported the construction of the Kerch Straight Bridge connecting Russia to the Crimean Peninsula; a notorious pre-trial detention center in Simferopol; and Russian government officials, including a local official, whom the Treasury Department described as "critical to the Russian government's malign efforts to exercise authority within Ukrainian territory following Russia's illegal seizure of Crimea." Additional information about these people can be found here. As the Treasury Department noted in its press release announcing the designations, several of these individuals have recently been sanctioned by the EU, the UK, Canada and Australia.

***Assessment of Attribution for Exploitation of SolarWinds Orion***

The White House Fact Sheet announcing the April 15 sanctions states that the United States is formally naming SVR, also known as APT 29, Cozy Bear and The Dukes, "as the perpetrator of the broad-scope cyber espionage campaign that exploited the SolarWinds Orion platform and other information technology infrastructures." The fact sheet affirmed that the US intelligence community "has high confidence in its assessment of attribution to the SVR." Concurrently, the National Security Agency, the Cybersecurity & Infrastructure Security Agency, and the FBI issued a joint cybersecurity advisory, "Russian SVR Targets US and Allied Networks." The advisory provides details on software vulnerabilities exploited by the SVR and provides steps that networks can take to identify and defend against the SVR's cyber-enabled activities.

The White House Fact Sheet also observes that the exploitation of SolarWinds "highlights the risks posed by Russia's efforts to target companies worldwide through supply chain exploitation," and that the US government "is evaluating whether to take action under Executive Order 13873 to better protect" the US information and communications technology and services (ICTS) supply chain. In a prior client alert, WilmerHale discussed the new Commerce Department regulations establishing a process whereby it will review commercial transactions between US and foreign parties involving ICTS supplied by firms subject to the jurisdiction of "foreign adversaries" including Russia.

***Additional Actions***

The White House did not announce any new sanctions against Russia in response to reports that the Russian government offered to pay bounties for attacks on US servicemembers and other coalition personnel in Afghanistan. However, the White House Fact Sheet stated that the issue "is being handled through diplomatic, military and intelligence channels" given its sensitivity. The White House also announced on April 15 that the United States is developing a course for global

policymakers "on the policy and technical aspects of publicly attributing cyber incidents" and that it is "bolstering" US support for the George C. Marshall Center in Garmisch, Germany, "to provide training to foreign ministry lawyers and policymakers on the applicability of international law to state behaviors in cyberspace and the non-binding peacetime norms that were negotiated in the United Nations and endorsed by the UN General Assembly." The White House also announced that the Defense Department is working to incorporate allies, including the UK, France, Denmark and Estonia, into the CYBER FLAG 21-1 exercise "to improve our defensive capabilities and resiliency in cyberspace." Finally, the United States is expelling 10 individuals from the Russian diplomatic mission in Washington, including representatives of the Russian Intelligence Services.

* * *

WilmerHale is prepared to advise clients on US sanctions regulatory compliance and enforcement and has particular expertise on US sanctions against Russia.

## *Contributors*


**Michael Dawson**
PARTNER

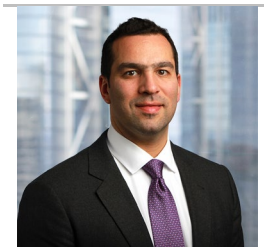
michael.dawson@wilmerhale.com
+1 202 663 6638

**Ronald I. Meltzer**
SENIOR COUNSEL

ronald.meltzer@wilmerhale.com
+1 202 663 6389

**David M. Horn**
SPECIAL COUNSEL

david.horn@wilmerhale.com
+1 202 663 6749



**Zachary Goldman**
COUNSEL

zachary.goldman@wilmerhale.com
+1 212 295 6309

**Semira Nikou**

SENIOR ASSOCIATE

semira.nikou@wilmerhale.com

+1 202 663 6511