Davis Polk

United States expands secondary sanctions and other restrictions on Russia

June 24, 2024 | Client Update | 17-minute read

In the past few weeks, the United States has announced several significant new restrictions targeting Russia, including expanded authority to impose secondary sanctions on foreign financial institutions that transact with sanctioned Russian entities, sanctions on key Russian financial infrastructure entities and a major Russian cybersecurity provider, and further restrictions on exports of goods and services.

The United States continues to expand sanctions on Russia in response to its invasion of Ukraine, with a number of important new measures announced this month. First, On June 12, the United States announced a series of new sanctions and export control restrictions, in accordance with G7 commitments to intensify pressure on Russia. At a high level, the new measures:

- Expand secondary sanctions targeting Russia by authorizing the Office of Foreign Assets Control (OFAC) to impose secondary sanctions on any foreign financial institutions (FFIs) that provide services involving persons blocked under Executive Order (EO) 14024 (a category that includes most Russian banks);
- Impose blocking sanctions on Russia's largest stock exchange, the exchange's central counterparty and clearing agent, and Russia's central securities depository;
- Effective September 12, 2024, prohibit the export from the United States or by a U.S. person of (1) IT consultancy and design services and (2) IT support services and cloud-based services for certain software to any person in Russia;
- Impose blocking sanctions on hundreds of additional individuals and entities linked to Russia's sanctions evasion and procurement networks and supply chains; and
- Expand export control restrictions for certain software and hundreds of other categories of items.

The new measures reflect the Administration's continued focus on third-country actors – including FFIs – that facilitate Russia's access to the global financial system and procurement networks. The expanded secondary sanctions for FFIs, in particular, appear designed to further narrow Russia's avenues to the global banking system, as OFAC will have authority to target FFIs with virtually any dealings involving sanctioned Russian banks (which include most of Russia's largest financial institutions). While the United States has historically been highly selective in imposing secondary sanctions, the new measures seem calibrated to have a broad deterrent effect on dealings with Russia and encourage de-risking by FFIs that still do business in the country (as well as U.S. and foreign institutions that maintain relationships with those FFIs).

The restrictions on the provision of IT services, paralleling those previously imposed by the EU and UK, expand on previous bans on services (including accounting and management consulting services and architecture and engineering services) that support Russia's economy and military-industrial base. Like the previous restrictions, the prohibition on exports of certain IT services covers a broad range of activities; however, it contains a number of carve-outs and limitations, and it does not apply to services provided to U.S.-owned entities. The exemptions are narrower for services provided to non-U.S. entities, however, meaning that firms that provide IT-related services in Russia should review their current practices for compliance. The IT services ban is accompanied by new software export restrictions announced by the Commerce Department's Bureau of Industry and Security (BIS).

Separately, on June 20 and 21, 2024, BIS and OFAC announced actions targeting major cybersecurity provider AO Kaspersky Lab (Kaspersky Lab) and its affiliates, as well as the imposition of blocking sanctions on key leadership of the company, after an investigation concluded that Kaspersky Lab facilitated the Russian government's cyber intelligence activities in the United States. The BIS actions include the first ever prohibition imposed under EO 13873 and its implementing Information and Communications Technology Supply Chain (ICTS) regulations, which will prohibit Kaspersky Lab from selling or updating anti-virus software in the United States

We provide below a summary of the new round of sanctions and export control restrictions and their implications.

Expanded secondary sanctions on foreign financial institutions

On June 12, OFAC updated the definition of "Russia's military industrial base" as used in EO 14114 to include all persons subject to blocking sanctions under EO 14024, rather than only those sanctioned persons operating in Russia's technology, defense, aerospace, construction and manufacturing sectors. The new provision broadens the scope of the secondary sanctions regime implemented in December 2023 (discussed in this client update) and reflects the Administration's ongoing focus on third-country actors that facilitate Russia's access to the global economy. While in principle EO 14024 itself provides authority to sanction persons that provide financial, material, or technological support for, or goods or services to or in support of, any person sanctioned under the order, OFAC's announcement appears intended to send a clear message to FFIs that, aside from limited categories of permissible activities,[1] continued engagement with sanctioned Russian actors (including sanctioned banks) will jeopardize the FFI's access to the U.S. financial system. This message is reinforced by OFAC's updated Advisory for Foreign Financial Institutions on Russia Sanctions Risks, which explains (in unusually prescriptive terms) the agency's compliance expectations for FFIs and provides examples of red flags and risk-mitigating controls.[2]

The advisory in particular now notes that that small- and medium-size financial institutions based in jurisdictions that continue to engage in significant trade with Russia may present a particularly high risk in terms of their customer base and correspondent relationships. OFAC recommends that those FFIs, as well as larger international financial institutions that deal with such FFIs, implement appropriate risk-based controls, which may include, among other things, enhanced screening procedures, reviewing an institution's customer base, communicating compliance expectations to customers, sending questionnaires and requiring compliance attestations, and implementing enhanced trade finance controls (e.g., monitoring and review of trade documents).

To date, OFAC has not targeted any FFI under EO 14114, though media reports suggest that there have been active deliberations within the U.S. government regarding use of the authority. Historically, the U.S. government has been highly selective about its use of secondary sanctions authorities, and it primarily has used such authorities as tools to support outreach and diplomatic engagement to get FFIs to agree to cease or limit sanctionable transactions. While this likely remains the primary goal of EO 14114 as well, OFAC's announcement is a stark reminder of the threat underlying such outreach, and FFIs that continue to have direct or indirect relationships with sanctioned Russian parties should recognize that doing so will create substantial sanctions risk going forward.

Targeting financial infrastructure

The latest round of sanctions also targeted key Russian financial infrastructure, as OFAC imposed full blocking sanctions on Moscow Exchange (MOEX), Russia's largest stock and foreign currency exchange, as well as its subsidiaries including National Clearing Center (NCC), its central counterparty and clearing agent, and Non-Bank Credit Institution Joint Stock Company National Settlement Depository (NSD), Russia's central securities depository. MOEX and its subsidiaries were designated under EO 14024, meaning that transactions with those entities fall within the scope of the expanded secondary sanctions regime (and FFIs would risk exposure for trading activities). Immediately after the designation, MOEX suspended trading in euros and dollars.

To facilitate the wind-down of transactions directly with these entities as well as the divestment of Russian securities held in custody by them or traded through them, OFAC issued two general licenses (GLs) authorizing certain transactions involving MOEX, NCC, and NSD until 12:01 a.m. eastern daylight time on August 13:[3]

- GL 99 authorizes transactions ordinarily incident and necessary to the wind down of transactions involving MOEX, NCC, and NSD, as well as certain transactions related to the divestment to non-U.S. persons of debt or equity issued or guaranteed by, or derivative contracts involving, those entities. For example, GL 99 "would authorize a U.S. person to divest their equity in MOEX to a non-blocked non-U.S. person."[4]

– GL 100 authorizes certain transactions for the divestment to non-blocked, non-U.S. persons of debt or equity, or for the conversion of currencies, involving MOEX and its subsidiaries solely as a securities, trade, or settlement depository, central counterparty or clearing house, or public trading market. GL 100 is intended to cover "the divestment of debt or equity of non-blocked companies that may be traded on or through one of" MOEX and its subsidiaries. For example, "GL 100 would authorize a U.S. person to divest their equity in a non-blocked Russian company that is being traded on MOEX to a non-blocked, non-U.S. person."[5]

OFAC also amended GL 8J, which authorizes certain transactions related to energy, to include NCC as one of the Russian financial institutions covered by the license.[6]

Following the expiration of GL 100, assuming the authorization is not extended, the sanctions on these entities will effectively prohibit U.S. persons from engaging in further transactions (including divestitures) involving even non-blocked Russian securities, which generally are held through NSD, as well as instruments traded on MOEX.

Ban on export of specified IT services

What do the new measures prohibit?

OFAC has authority under EO 14071 to prohibit the export, reexport, sale, or supply of designated categories of services to persons in Russia. OFAC has previously used this authority to ban, among other things, the export of accounting, trust and corporate formation, and management consulting services (discussed in this client update), as well as architecture and engineering services (discussed in this client update). On June 12, OFAC expanded the services restrictions through a determination that prohibits the provision of (1) IT consultancy and design services; and (2) IT support services and cloud-based services for enterprise management software and design and manufacturing software, to any person located in the Russian Federation, from the United States, or by a U.S. person (the IT Services Ban). The scope of the restrictions (and the software covered) broadly aligns with measures imposed by the EU and UK, which currently prohibit the export to Russia of IT consultancy services and enterprise management, design, and manufacturing software. The IT Services Ban will take effect at 12:01 a.m. eastern daylight time on September 12, 2024.

The IT Services Ban does not apply to the export of services to entities that are owned or controlled by U.S. persons, nor does it prohibit U.S. persons from providing services to Russian-owned entities located outside of Russia, as long as the "benefit of the services" is not "ultimately received" by a person in Russia and the services will not be further exported or reexported to persons located in the Russia.[7] For example, a U.S. company would be permitted to provide IT support services to its own subsidiaries, or to design a website or software for the subsidiary of a Russian company located in a third country, provided those services will "not be reexported to the Russian parent company."[8] However, it would be prohibited for a U.S. person to design and deliver covered software to a third-country software re-seller "knowing that it would be supplied to a Russian company," or to design software for a Russian-owned entity in a third country that in turn intends to supply the software to its parent.

What are the affected services?

The IT Services Ban applies to the export, reexport, sale, or supply, directly or indirectly, from the United States or by a U.S. person of (1) IT consultancy and design services for applications, and (2) IT support services and cloud-based services for enterprise management software and design and manufacturing software (which have specific meanings under the IT Services Ban).

IT consultancy and design services

IT consultancy services includes "providing advice or expert opinion on technical matters related to the use of information technology" (e.g., advice on software requirements or system integration), while IT design and development services for applications includes "services of designing the structure and/or writing the computer code necessary to create and/or implement a software application" (e.g., designing, structuring, or writing code for a website, database, or custom software, or customizing and installing existing applications).[9] For example, a U.S. person would be prohibited from assisting a Russian company in upgrading its IT systems, modifying web applications, or designing bespoke software.[10] However, IT consultancy and design services would not include the retail sale of off-the-shelf software (although export control restrictions may separately apply).

IT support services and cloud-based services

The IT Services Ban also prohibits the provision of IT support services and cloud-based services for "enterprise management software" (e.g., enterprise resource planning, customer relationship management, or business intelligence software)[11] and "design and manufacturing software," which is defined to include building information modelling, computer aided design, computer-aided manufacturing, and engineer to order software.[12] IT support services include the provision of "technical expertise to solve problems for the client in using software, hardware, or an entire computer system" – for example, technical support or customer support. Cloud-based services, meanwhile, are defined to include the "delivery of software via the internet or over the cloud, including through Software-as-a-Service (SaaS), or SaaS cloud services in relation to such software" – for example, selling a cloud-based software subscription.[13] In parallel, BIS has imposed export bans on U.S.-origin software in the same categories, as described below. These definitions are consistent with those adopted by the EU and UK in their respective bans on IT support services. Other categories of software are not included in the scope of the IT Services Ban.

The IT Services Ban includes several other notable exceptions. First, the IT Services Ban does not apply to services for software that would be eligible for a license exception or otherwise authorized for export or reexport to Russia by the BIS; as noted below, that includes exports to many subsidiaries of U.S. and allied countries.[14] In addition, the measures do not prohibit internet access or the delivery of internet-based communications services, consistent with OFAC's GL 25D.[15] Similarly, GL 6D authorizes transactions related to certain agricultural and medical activities involving the provision of information technology and software-related services.[16] More broadly, the export of information or informational materials are exempt from the scope of sanctions under the International Emergency Economic Powers Act.[17] Finally, the IT Services Ban does not apply to services related to the wind down or divesture of entities in Russia, provided that the entities are not owned by Russian persons.

Other Restrictions

Export control restrictions

Concurrent with the new rounds of sanctions, BIS issued a new rule[18] that broadens controls on exports to Russia and Belarus. In particular, to align with the IT Services Ban, BIS imposed licensing requirements on key categories of enterprise management software and design software, including software designated as EAR99. These restrictions do not apply, however, to wholly owned subsidiaries or branches of entities based in the United States or a number of close allies.[19] In addition, BIS expanded controls on more than 500 additional 6-digit Harmonized Tariff System codes for export, reexport, or transfer (in-country) to Russia and Belarus, which expands licensing requirements for a broad range of goods including chemicals, oil and gas, and defense products.

According to BIS, following the numerous rounds of export control restrictions, "most remaining trade with Russia is limited to agricultural or medical sectors."[20] As the United States continues to broaden export controls and sanctions on Russia, and given the widespread de-risking in the private sector, we would expect this trend to continue.

Other new sanctions designations

In addition to the designation of MOEX, the Administration imposed hundreds of new sanctions designations, with a notable focus on third-country actors. As discussed in recent client updates, the United States and its allies have increasingly focused on narrowing Russia's avenues to evade sanctions and export controls and have targeted hundreds of third-country facilitators and intermediaries. The United States has similarly targeted entities in key sectors that support Russia's economy and supply chains. Consistent with that strategy, on June 12, OFAC and the State Department imposed blocking sections on over 300 entities, across numerous jurisdictions, linked to sanctions evasion schemes and transnational supply chains, as well entities found to support Russia's oil and gas, metals and mining, technology, and manufacturing sectors.

Actions against Kaspersky Lab

On June 20, BIS took a number of actions targeting Kaspersky Lab and its affiliates, after a BIS investigation concluded that Kaspersky Lab cooperated "with Russian military and intelligence authorities in support of the Russian government's cyber intelligence objectives."[21] In particular, BIS issued a Final Determination that will prohibit Kaspersky Lab, Inc., the U.S. subsidiary of Kaspersky Lab, as well as its affiliates and parent companies from providing anti-virus software and cybersecurity products or services in the United States or to U.S. persons.[22] Kaspersky will be prohibited from entering new agreements with U.S. customers effective 12:00 a.m. on July 20, 2024. To provide current U.S. users time to find an alternative product, Kaspersky Lab will be permitted to provide software updates and to operate its cloud-based

cybersecurity network for U.S. users until 12:00 a.m. on September 29, 2024. The Final Determination is the first determination that BIS has issued under EO 13873 and the ICTS, which empower BIS to investigate transactions to determine if they present a national security risk and prohibit the transaction or impose mitigation measures.[23]

Concurrent with the issuance of the Final Determination, BIS added Kaspersky Lab and affiliates to the Commerce Department's Entity List. On June 21, OFAC followed these designations by imposing sanctions on twelve members of the executive leadership of Kaspersky Lab.[24] The U.S. government's national concerns with Kaspersky Lab are not a recent development, as the Department of Homeland Security previously issued a directive in 2017 that required Federal Executive Branch departments and agencies to discontinue use of Kaspersky Lab products and remove Kaspersky software from federal systems.

Summer Associate William Weightman contributed to this client update.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Kendall Howell
+1 202 962 7068
kendall.howell@davispolk.com

Paul Marquardt
+1 202 962 7156
paul.marquardt@davispolk.com

Will Schisa
+1 202 962 7129
will.schisa@davispolk.com

Charles Marshall Wilson
+1 202 962 7130
charles.wilson@davispolk.com

[1] OFAC has clarified that FFIs do not risk exposure for engaging in transactions that would be authorized under a general or specific license were they conducted in the United States – e.g., humanitarian activity and certain transactions related to agriculture, medicine or medical devices, energy, or telecommunications and internet-based communications. *See* OFAC, FAQ 1181 (June 12, 2024), available at: https://ofac.treasury.gov/faqs/1182.

[2] See OFAC, Updated Guidance for Foreign Financial Institutions on OFAC Sanctions Authorities Targeting Support to Russia's Military-Industrial Base (June 12, 2024), https://ofac.treasury.gov/media/932436/download?inline.

[3] *See* GL 99, available at https://ofac.treasury.gov/media/932941/download?inline; GL 100, available at: https://ofac.treasury.gov/media/932946/download?inline.

[4] OFAC, FAQ 1183.

[5] *Id.*

[6] GL 8J, available at: https://ofac.treasury.gov/media/932926/download?inline.

[7] See OFAC, FAQ 1188 (June 12, 2024), available at: https://ofac.treasury.gov/faqs/1188.

[8] *Id.*

[9] See OFAC, FAQ 1187 (June 12, 2024), available at: https://ofac.treasury.gov/faqs/1187. OFAC provides the following definitions, which align with the United Nations' Central Product Classification (CPC) Codes 83131 and 83141, respectively:
"**IT consultancy services**" includes providing advice or expert opinion on technical matters related to the use of information technology, such as: (a) advice on matters such as hardware and software requirements and procurement; (b) systems integration; (c) systems security; and (d) provision of expert testimony on IT related issues.
"**IT design and development services for applications**" includes services of designing the structure and/or writing the computer code necessary to create and/or implement a software application, such as: (a) designing the structure of a web page and/or writing the computer code necessary to create and implement a web page; (b) designing the structure and content of a database and/or writing the computer code necessary to create and implement a database; (c) designing the structure and writing the computer code necessary to design and develop a custom software application; (d) customization and integration, adapting (modifying, configuring, etc.) and installing an existing application so that it is functional within the clients' information system environment.

[10] See OFAC, FAQ 1185 (June 12, 2024), available at: https://ofac.treasury.gov/faqs/1185.

[11] The term enterprise management software means the following types of software: enterprise resource planning, customer relationship management, business intelligence, supply chain management, enterprise data warehouse, computerized maintenance management system, project management, and product lifecycle management software. *See* OFAC, FAQ 1187.

[12] OFAC, FAQ 1187.

[13] See OFAC, FAQ 1186, available at: https://ofac.treasury.gov/faqs/1186; OFAC, FAQ 1187. In particular, the definition of "information technology support services" includes: (i) providing technical expertise to solve problems for the client in using software, hardware, or an entire computer system, such as: (a) providing customer support in using or troubleshooting the software; (b) upgrading services and the provision of patches and updates; (c) providing customer support in using or troubleshooting the computer hardware, including testing and cleaning on a routine basis and repair of IT equipment; (d) technical assistance in moving a client's computer system to a new location; (e) providing customer support in using or troubleshooting the computer hardware and software in combination; and (ii) providing technical expertise to solve specialized problems for the client in using a computer system, such as: (a) auditing or assessing computer operations without providing advice or other follow-up action including auditing, assessing and documenting a server, network or process for components, capabilities, performance, or security; (b) data recovery services, i.e. retrieving a client's data from a damaged or unstable hard drive or other storage medium, or providing standby computer equipment and duplicate software in a separate location to enable a client to relocate regular staff to resume and maintain routine computerized operations in event of a disaster such as a fire or flood; and (c) other IT technical support services not elsewhere classified. *See id.*

[14] See OFAC, FAQ 1184 (June 12, 2024), available at: https://ofac.treasury.gov/faqs/1184.

[15] General License 25D authorizes certain transactions ordinarily incident and necessary to the receipt or transmission of telecommunications involving the Russian Federation and the provision of certain services incident to the exchange of communications over the internet, subject to certain restrictions. *See* OFAC, General License 25D, available at: https://ofac.treasury.gov/media/932931/download?inline.

[16] *See* OFAC, General License 6D, available at: https://ofac.treasury.gov/media/932921/download?inline.

[17] 50. U.S.C. § 1702(b)(3).

[18] BIS, Implementation of Additional Sanctions Against Russia and Belarus Under the Export Administration Regulations (EAR) and Refinements to Existing Controls, 89 Fed. Reg. 51644 (June 18, 2024), available at: https://www.govinfo.gov/content/pkg/FR-2024-06-18/pdf/2024-13148.pdf.

[19] 15 CFR 746.8(a)(12)(ii).

[20] Press Release, U.S. Dep't of Commerce , Department of Commerce Announces Additional Export Restrictions to Counter Russian Aggression (June 12, 2024), https://www.bis.gov/press-release/department-commerce-announces-additional-export-restrictions-counter-russian.

[21] Press Release, U.S. Dep't of Commerce, Commerce Department Prohibits Russian Kaspersky Software for U.S. Customers (June 20, 2024), https://www.bis.gov/sites/default/files/files/KL-press_release-CLEAN.pdf.

[22] *See* BIS, Final Determination: Case No. ICTS-2021-002, Kaspersky Lab, Inc., 89 Fed. Reg. 52434 (June 24, 2024), https://www.govinfo.gov/content/pkg/FR-2024-06-24/pdf/2024-13532.pdf.

[23] See Exec. Order No. 13873, 84 Fed. Reg. 22689 (May 15, 2019), https://www.govinfo.gov/content/pkg/FR-2019-05-17/pdf/2019-10538.pdf.

[24] Press Release, U.S. Dep't of the Treasury, Treasury Sanctions Kaspersky Lab Leadership in Response to Continued Cybersecurity Risks (June 21, 2024), https://home.treasury.gov/news/press-releases/jy2420.