Sweeping New U.S. Sanctions and Export Controls Intensify Pressure on Russia and Belarus As Russia Transitions to a Full War Economy

25 June 2024

The United States has substantially expanded economic sanctions and export controls targeting Russia and Belarus, imposing new restrictions that could have a major impact on companies with business activities in or relating to Russia.

Joint action by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), the U.S. Department of Commerce's Bureau of Industry and Security (BIS) and the U.S. Department of State on June 12, 2024, seeks to reduce Russia's access to third-country financial services and supplies needed to support its wartime economy. Affected companies should carefully assess the increased risks and compliance challenges.

BIS also took action to prohibit Kaspersky Lab, Inc., the U.S. subsidiary of a Russia-based antivirus software and cybersecurity company, AO Kaspersky Lab, and its affiliates, parents and subsidiaries (collectively, Kaspersky), from providing software to U.S. customers based on a Determination that the company's continued operations in the United States presented a national security risk. U.S. users of Kaspersky products are strongly encouraged to expeditiously transition to new vendors. In addition, OFAC imposed blocking (asset freeze) sanctions on certain executives and senior leaders at AO Kaspersky Lab, the Russian parent of Kaspersky Lab, Inc.

At a Glance: Key Points From the New Sanctions and Export Control Measures

The new sanctions:

- Prohibit companies, effective September 12, 2024, from supplying to Russia certain:
  - IT consultancy and design services.
  - IT support services and cloud-based services.
- Significantly expand OFAC's authority to impose sanctions on foreign financial institutions (FFIs) who transact with or provide services involving Russia's military-industrial base, effective June 12, 2024.
- Impose blocking sanctions on hundreds of parties together with the U.S. Department of State.

The new export control measures:

- Introduce significantly expanded export controls on supply to or within Russia and Belarus of several types of software not specifically identified on the Commerce Control List (CCL).These expanded controls take effect September 16, 2024.
- Control for supply to Russia and Belarus a significant number of items not on the CCL, effective June 12, 2024.
- Narrow the list of consumer goods eligible for license-free supply to or within Russia and Belarus, effective June 12, 2024.
- Supplement, for the first time, the BIS Entity List with addresses, rather than entity names, to combat diversion.

A Closer Look: The New Sanctions and Export Controls in More Detail

1. New Prohibition on Supply of Services

OFAC issued a new Determination under the authority of Executive Order 14,071 that, effective September12, 2024, will prohibit U.S. persons—including anyone in the United States—to provide the following to persons located in Russia, with limited exceptions:

- IT consultancy and design services (technical expertise to solve problems for the client in using software, hardware or an entire computer system), and
- IT support services and cloud-based services (via the internet or the cloud, including through Software-as-a-Service) for "Covered Software," defined to include:
    - Enterprise management software:
        - Enterprise resource planning.
        - Customer relationship management.
        - Business intelligence.
        - Supply chain management.
        - Enterprise data warehouse.
        - Computerized maintenance management system.
        - Project management.
        - Product lifecycle management software.
    - Design and manufacturing software:
        - Building information modelling.
        - Computer-aided design.
        - Computer-aided manufacturing.
        - Engineer to order.

A new OFAC FAQ provides guidance on the meaning of IT consultancy and design services, IT support services and cloud-based services.

The limited exceptions include providing services:

- To U.S.-owned or -controlled entities located in Russia,
- In connection with winding down or divestiture of non-Russian-owned or -controlled entities located in Russia, and

- For software that is authorized for exports to Russia by the U.S. Department of Commerce or that would be authorized if it were subject to U.S. export controls.

The prohibition does not cover providing services to Russian-owned or -controlled persons located in a third country as long as the services will not be further exported or made available to persons located in Russia. In addition, supplying services incident to telecommunications and Internet-based communications, including instant messaging, chat and email, social networking, collaboration platforms and video conferencing remains authorized under an updated general license.

What Companies Should Know or Consider Doing

- Software and tech companies should closely evaluate their customer bases to assess the impact of the new prohibitions on their operations.
- Companies supplying the relevant services to parties in Russia or entities owned or controlled by parties in Russia may need to adjust their compliance programs.
- Absent OFAC guidance as to what falls within the scope of Covered Software, companies should carefully consider whether their software-related services might fall into one or more of the prohibited categories.

2. Expansion of Secondary Sanctions Authorization on FFIs

In December 2023, as explained in our previous alert, the U.S. government authorized sanctions on FFIs determined to have knowingly or unknowingly supported Russia's military-industrial base, which included persons operating in specified sectors of the Russian economy and those supporting the supply of certain items critical to Russian warfare.

Effective June 12, 2024, OFAC expanded the definition of "Russia's military-industrial base" to include all persons blocked pursuant to Executive Order 14,024, including numerous sanctioned Russian banks, such as Sberbank, VTB, Sovcombank, Otkritie and many others.

As a result, FFIs that engage in transactions or provide services involving such persons are exposed to the risk of U.S. secondary sanctions, which include blocking sanctions and a prohibition on opening or restrictions on maintaining correspondent accounts or payable-through accounts in the United States. According to OFAC, FFIs do not risk the imposition of sanctions for engaging in transactions that are authorized for U.S. persons under OFAC general licenses.

OFAC updated guidance is recommending that FFIs:

- Review their customer base and update diligence practices and customer risk-rating criteria.
- Take mitigation measures for high-risk customers or counterparties.
- Evaluate the sufficiency of existing compliance programs.

OFAC highlighted nested correspondent banking relationships as a particular risk. In other words, even an FFI with no direct relationships with Russian sanctions targets may face risk under the new sanctions if it provides foreign correspondent account services to other banks, which in turn engage in significant transactions involving Russia through those correspondent accounts.

What Companies Should Know or Consider Doing

Expanded secondary sanctions authority will likely cause further withdrawal by global banks from Russia-related business.

3. New Blocking Sanctions

OFAC and the U.S. Department of State also have imposed blocking sanctions on hundreds of individuals and entities deemed to be contributing to Russian warfare, including the Moscow Exchange (MOEX). According to OFAC, MOEX attracts investments in Russian sovereign debt, Russian corporations and leading Russian defense entities. In addition, OFAC designated dozens of Russian defense and military enterprises, companies in the transnational supply chain for materials used for warfare, and sanctions evasion networks participants based in and outside of Russia. Finally, implementing the G7's resolve to limit Russia's future revenue from liquefied natural gas (LNG), OFAC designated three LNG projects being developed by Russia and companies involved in construction of gas production sites, development of geological exploration of mineral deposits, and construction of specialized LNG tankers, along with seven such tankers. OFAC issued three general licenses (GL 98, GL 99 and GL 100) authorizing the wind-down and divestment transactions with some of the newly designated parties through certain dates.

What Companies Should Know or Consider Doing

U.S. persons are prohibited from transacting or dealing with blocked persons and entities 50-percent-or-more owned by them, directly or indirectly, absent authorization from OFAC.

4. New Export License Requirements on Software Supplied to or Within Russia or Belarus

Effective September 16, 2024, subject to limited exceptions, it will be prohibited to supply to or within Russia or Belarus without a licensed Covered Software that is subject to the Export Administration Regulations (EAR) and classified "EAR99" (meaning that the software does not fall within any export control classification number on the CCL). The prohibition also covers software updates for previously supplied EAR99-classified Covered Software.

The limited exceptions include supply of EAR99 Covered Software to entities exclusively operating in the medical or agricultural sectors and to certain categories of civil end-users that include U.S. subsidiaries and subsidiaries of allied country companies.

What Companies Should Know or Consider Doing

In the absence of BIS guidance as to what falls within the scope of Covered Software, companies should carefully consider whether their software might fall into one or more of the categories and adjust their supply of software accordingly to remain in compliance with U.S. export control requirements.

5. New Hardware Items Subject to Licensing Requirement When Supplied to or Within Russia or Belarus

Effective June 12, 2024, BIS added license requirements for supplying items in more than 500 additional six-digit Harmonized Tariff System (HTSUS) codes to or within Russia and Belarus. This action is intended to forestall the avoidance of preexisting Russia and Belarus license requirements by altering the HTSUS classifications to similar HTSUS codes not covered by the preexisting license requirements.

What Companies Should Know or Consider Doing

Companies should carefully consider if their hardware may now be subject to an export license requirement when supplied to or within Russia or Belarus.

6. Reduction of License Exception Eligibility for Certain Consumer Goods Supplied to or Within Russia or Belarus

Effective June 12, 2024, BIS narrowed the list of consumer goods eligible for license-free supply to or within Russia or Belarus under License Exception Consumer Communications Devices (CCD). Items that are no longer eligible for license-free supply to or within Russia and Belarus under License Exception CCD include:

- Consumer disk drives and solid-state storage equipment.
- Graphics accelerators and graphics coprocessors.
- Modems, network interface cards, routers and switches, as well as WiFi access points and drivers, communications and connectivity software for such hardware.
- Network access controllers and communications channel controllers.
- Memory devices.
- Digital cameras (including webcams) and memory cards.
- Television and radio receivers, set top boxes, video decoders and antennas.
- Recording devices.

What Companies Should Know or Consider Doing

Companies should carefully consider if their consumer goods supplied to or within Russia or Belarus may no longer be eligible for License Exception CCD.

7. Addition of Addresses to Entity List

For the first time, BIS has added eight *addresses* (all in Hong Kong) to the Entity List it administers in an attempt to prevent diversion via shell companies.

Entities added to the Entity List generally require a license to supply most, if not all, items subject to the EAR. Now companies also will need a license to supply items that are subject to the EAR and appear on the CCL or in Supplement No. 7 to EAR Part 746 to any entity operating at any of the eight listed addresses.

What Companies Should Know or Consider Doing

Companies should review and adjust their supply practices as necessary to account for the Entity List prohibitions based on addresses to remain in compliance with U.S. export control requirements.

8. Kaspersky Software Ban

BIS has prohibited, with limited exceptions, Kaspersky from directly or indirectly providing antivirus software and cybersecurity products or services in the United States or to U.S. persons starting on June 20, 2024, and to provide updates to software already in use starting on September 29, 2024. This is the first action by BIS's Office of Information and Communications Technology and Services under Executive Order 13,873, Securing the Information and Communications Technology and Services Supply Chain, and its implementing regulations. BIS also added three Kaspersky entities to the Entity List.

OFAC imposed blocking sanctions, under Executive Order 14,024, on twelve individuals in executive and senior leadership roles at Kaspersky for operating in the technology sector of the Russian economy, but not on AO Kaspersky Lab or any of its affiliates or its Chief Executive Officer.

What Companies Should Know or Consider Doing

U.S. users of Kaspersky software are strongly encouraged to expeditiously transition to new vendors to limit exposure of personal or other sensitive data. BIS clarified that persons continuing to use existing Kaspersky products and services will not face legal penalties but should be prepared to assume all the cybersecurity and associated risks of doing so. U.S. persons are prohibited from transacting or dealing with Kaspersky executives blocked by OFAC and entities 50-percent-or-more owned by them, directly or indirectly, absent authorization from OFAC.