OFAC
Office of Foreign Assets Control

SANCTIONS ADVISORY

Updated Guidance for Foreign Financial Institutions on OFAC Sanctions Authorities Targeting Support to Russia's Military-Industrial Base

June 12, 2024

In response to the Russian Federation's continued use of its military-industrial base to support its aggression against Ukraine, on December 22, 2023, the President issued Executive Order (E.O.) 14114, which amends E.O. 14024 and provides the Office of Foreign Assets Control (OFAC) with authorities to target foreign financial institutions for engaging in certain transactions. **Foreign financial institutions that conduct or facilitate significant transactions or provide any service involving Russia's military-industrial base run the risk of being sanctioned by OFAC. OFAC is revising the definition of "Russia's military-industrial base" to include all persons blocked under E.O. 14024, as amended.**

The United States and partners have put in place a sanctions and export controls regime that has severely restricted Russia's ability to import many of the items that directly support its brutal and unjustified war against Ukraine. As a result, Russia is increasingly using third countries to evade sanctions and continue its procurement of certain critical items. The United States and partners have published multiple advisories, including detailed red flags, to warn the private sector about Russian sanctions evasion in support of its war machine and to support compliance efforts. OFAC's targeting authorities, which are aimed at foreign financial institutions that provide services to, or engage in significant transactions relating to, Russia's military-industrial base, come as a natural evolution of OFAC's work to counter evasion and hold accountable those perpetuating Russia's war against Ukraine, including financial facilitators.

OFAC is issuing this revised advisory to provide updated guidance to foreign financial institutions in light of Russia's continued efforts to reorient its entire economy and government resources to support its war effort. This updated advisory includes practical guidance on how to identify sanctions risks and implement corresponding controls. For additional guidance, please see OFAC's frequently asked questions (FAQs) 1146, 1147, 1148, 1149, 1150, 1151, 1152, 1181, and 1182.

Sanctions Authorities Targeting Foreign Financial Institutions

E.O. 14024, as amended (E.O. 14024), allows OFAC to sanction foreign financial institutions that, among other things, have conducted or facilitated any significant transaction or transactions, or provided any service, involving Russia's military-industrial base. **On June 12, 2024, OFAC updated the definition of "Russia's military-industrial base" to include all persons blocked under E.O. 14024 (FAQ 1181 and 1151).** The updated definition reflects the Kremlin's increasing use of Russia's entire economy to support

its war in Ukraine.[1] Specifically, Russia's military-industrial base includes: (i) all persons blocked pursuant to E.O. 14024; and (ii) any person operating in the technology, defense and related materiel, construction, aerospace, and manufacturing sectors of the Russian Federation economy ("the specified sectors"). Russia's military-industrial base may also include persons that support the sale, supply, or transfer, directly or indirectly, to the Russian Federation of certain critical items ("the specified items"). **Accordingly, foreign financial institutions that conduct or facilitate any significant transaction or provide any service involving any person blocked pursuant to E.O. 14024 now risk being sanctioned by OFAC, unless they are solely facilitating permissible transactions such as those related to food, agriculture, medicine, energy, and telecommunications.**

Under these authorities, OFAC can impose full blocking sanctions on, or prohibit or restrict the maintenance of correspondent accounts in the United States for, foreign financial institutions. Please see E.O. 14024 for the full criteria upon which a foreign financial institution may be sanctioned and the type of sanctions that may be imposed.

Examples of Activity that Could Expose Foreign Financial Institutions to Sanctions Risk

The following are examples of activities that could expose foreign financial institutions to sanctions risk under E.O. 14024:

- Maintaining accounts, transferring funds, or providing other financial services (e.g., payment processing, trade finance, insurance) for any person blocked pursuant to E.O. 14024, including Russian financial institutions blocked pursuant to E.O. 14024, outside of the activities described below under "Permissible Activities."
- Maintaining accounts, transferring funds, or providing other financial services (e.g., payment processing, trade finance, insurance) for any persons, either inside or outside Russia, that otherwise support Russia's military-industrial base, including those that operate in the specified sectors.
- Facilitating the sale, supply, or transfer, directly or indirectly, of the specified items to Russian importers or companies shipping the items to Russia.
- Helping companies or individuals evade U.S. sanctions on Russia's military-industrial base. This includes:
  - offering to set up alternative or non-transparent payment mechanisms,
  - changing or removing customer names or other relevant information from payment fields,
  - obfuscating the true purpose of or parties involved in payments, or
  - otherwise taking steps to hide the ultimate purpose of transactions to evade sanctions.

1 https://ofac.treasury.gov/media/932446/download?inline.

The list of specified items can be found here. Treasury has identified the specified items because they are critical for Russia's war effort, including for the production of advanced precision-guided weapons and other critical items, and Russia is actively working to import them from third countries to fuel its war machine. **Foreign financial institutions should use this list of specified items for the purpose of mitigating sanctions risk under Treasury's sanctions authorities described in this advisory.**[2] If in the course of its due diligence, a foreign financial institution is unsure whether a particular item is the same as one identified on the list of specified items (or could otherwise potentially be linked to Russia's military-industrial base), the institution should conduct further due diligence regarding the particular customer and/or transaction and take appropriate mitigation measures, as described further below.

Identifying and Mitigating Sanctions Risks

To mitigate sanctions risk, foreign financial institutions should take steps to identify and minimize their exposure to activity involving Russia's military-industrial base and those that support it. These steps are in addition to baseline customer due diligence (CDD) procedures and other anti-money laundering (AML) controls, which can be critical for detecting, stopping, and reporting attempted or suspected sanctions evasion. OFAC recognizes that there is not a "one-size-fits-all" approach to identifying and mitigating exposure to activity involving Russia's military-industrial base, and thus foreign financial institutions may take various approaches to identifying and mitigating their relative sanctions risk. Each institution should implement controls commensurate with its risk profile and current exposure to Russia's military-industrial base and its supporters.

For example, small- and medium-size financial institutions located in jurisdictions that continue to engage in significant trade with Russia may present a particularly high risk of providing services involving Russia's military-industrial base. OFAC recommends that such financial institutions carefully review the examples of controls identified below to assess whether implementing one or more of these controls may assist in identifying and mitigating this risk.

Examples of controls to mitigate sanctions risk may include:[3]

- Screening transactions, customers, counterparties, and associated parties against relevant sanctions lists, such as OFAC's Specially Designated Nationals and Blocked Persons List (SDN List), to prevent the provision of any service to persons blocked pursuant to E.O.

2 Since Russia's further invasion of Ukraine, the United States and partners have identified key items that Russia is seeking to procure for its weapons programs. Such key items include all of the specified items described in this advisory, as well as the Common High Priority Items List, which describes a subset of items that are restricted from trade to Russia by the United States and its allies. The Common High Priority List is intended for exporters, reexporters, and customs officials, and identifies broad categories of items by Harmonized System (HS) Codes, which are the foundation of the import and export classification systems used in the United States and by many trading partners. In contrast, the list of specified items described in this advisory is intended for use by financial institutions in implementing controls to mitigate sanctions risks under OFAC's authorities.

3 The listed measures are illustrative only and do not account for obligations that a financial institution may have related to historical activities, such as filing reports of suspicious transactions in the applicable jurisdiction(s).

14024, outside of permissible transactions such as food, agriculture, medicine, energy, and telecommunications.

- Reviewing an institution's customer base to determine exposure to the following:
  - Any customers involved in the specified sectors or who conduct business with persons blocked pursuant to E.O. 14024.
    - EXAMPLE OF HIGHER RISK CUSTOMER: A microelectronics exporter formed in March 2022 located in a high-risk jurisdiction that has received repeated international wire transfers from possible shell companies in offshore financial centers.
    - EXAMPLE OF LOWER RISK CUSTOMER: A basic household goods company in a G7 country that has been the bank's customer for 20 years, has never been flagged for suspicious activity, whose activity has remained consistent and has never exported goods to Russia or received funds from Russia.
  - Any customers that may be involved in the sale, supply, or transfer of the specified items to Russia or to jurisdictions previously identified as posing a high risk of Russian sanctions evasion.
- Communicating compliance expectations to customers on a risk basis, including informing them that they may not use their accounts to do business involving Russia's military-industrial base. This may also include sharing the list of the specified items with customers, especially customers engaged in import-export activity, manufacturing, or any other relevant business lines.
- Sending questionnaires, on a risk basis, to customers known to deal in or export specified items to better understand their counterparties.
- Using open-source information and past transactional activity to inform due diligence and to conduct proactive investigations into possible sanctions and export control evasion.
  - Proactive investigations into suspected sanctions evasion are often conducted within a bank's anti-financial crime division, as they involve post-transaction reviews for typologies, networks, and/or suspicious activity, as opposed to real-time, list-based screening. Sanctions-related information (e.g., interaction with listed entities prior to designation) can serve as an input for these investigations. The results of these investigations could then be used to further identify risky customers and other sanctions related risks.
    - EXAMPLE: A bank initiates a review of customers who sent or received funds from persons blocked pursuant to E.O. 14024 prior to their designation. After an initial review, the bank takes no additional action on lower risk customers (e.g., retail banking customers who sent small funds transfers to family in Russia via now-blocked Russian banks, retail banking customers who participated in low-value e-commerce involving now-blocked Russian banks) and focuses on higher risk categories (e.g., customers who received large wire transfers from Russian companies, which appear to be payments

received for goods shipped to Russia). After applying mitigation measures (e.g., account restrictions, account closure, addition to "do not onboard" and/or "do not process" watchlists), the bank also reviews the associated parties of exited customers.

  - In addition, financial institutions can use information received through requests for information from U.S. and global correspondent banks, as well as data from commercial service providers or public data sources such as trade and customs data, to inform due diligence and proactive investigations.

- When appropriate, obtaining attestations from high-risk customers that they do not operate in the specified sectors, engage in any sales or transfers of the specified items to Russia, or otherwise conduct any transactions involving Russia's military-industrial base (including involving any person blocked pursuant to E.O. 14024).
- Taking appropriate mitigation measures for any customers or counterparties engaged in high-risk activity or who fail to respond to requests for information regarding activity of concern. These measures include restricting accounts, limiting the type of permissible activity, exiting relationships, and placing customers or counterparties on internal "do not onboard" or "do not process" watchlists.
- Incorporating risks related to Russia's military-industrial base into sanctions risk assessments and customer risk-rating criteria. This includes updating jurisdictional risk assessments as appropriate.
- Implementing enhanced trade finance controls related to the specified items, including monitoring information collected as part of documentary trade.

Examples of High-Risk Foreign Financial Institutions

For financial institutions that have already invested in effective risk-based compliance programs, particularly those located in jurisdictions with strong regulatory oversight that have implemented their own sanctions on Russia, the area of greatest risk may be in the foreign correspondent relationships they maintain for financial institutions continuing to engage in significant transactions involving Russia.

Examples of high-risk foreign financial institutions may include:

1 A small bank in a jurisdiction with a strong trading relationship with Russia has a high number of customers in the import-export and microelectronics sectors that continue to do business with Russia. This bank maintains relationships with multiple designated Russian banks for the purpose of facilitating trade with Russia in the local currency. The activity going through this bank's foreign correspondent relationships shows repeated linkages with Russia, a large volume of suspected shell company activity, and other general indicators of suspicious activity, such as wires with no clear business purpose involving high-risk jurisdictions.

2 A medium-sized bank in a jurisdiction with a strong trading relationship with Russia is reported in credible open-source media as taking steps to bring in new Russia-related business in order to capitalize on measures other banks have taken to reduce their Russia-related risk. These steps include opening a new representative office in Russia, expanding its Russian language promotional materials and website, and advertising in Russian-language media about services for Russian businesses.

3 A small bank frequently sends transactions through its foreign correspondent account for customers who are later blocked pursuant to E.O. 14024. The bank does not satisfactorily respond to a request for information from its correspondent about why so many of its customers were subsequently sanctioned by OFAC.

Previous Guidance on Russia Sanctions and Export Controls Evasion

Since Russia's further unlawful invasion of Ukraine, the U.S. Departments of the Treasury, Commerce,[4] and State have repeatedly highlighted how Russia seeks to evade sanctions and export controls in support of its war effort, such as using third-party intermediaries and transshipment points to circumvent restrictions.[5] These alerts have provided examples of red flags that can signal when and how third parties and intermediaries may be engaged in efforts to evade sanctions or export controls. OFAC encourages foreign financial institutions to review and incorporate such guidance into their risk-based controls to mitigate sanctions risks. OFAC also notes that both this advisory and previous guidance are intended to warn foreign financial institutions of sanctions risks and to provide practical suggestions on various ways they can identify and mitigate such risk. OFAC encourages financial institutions to allocate their compliance resources towards the areas of greatest risk, such as products, services, business lines, and locations most likely to be used to facilitate activity involving Russia's military-industrial base.

In addition to the specific mitigation measures detailed above and the alerts focused on Russia sanctions and export control evasion, OFAC encourages foreign financial institutions to review A Framework for OFAC Compliance Commitments and the alerts focused on Russia's sanctions and export control evasion for further guidance on the essential components of a risk-based sanctions compliance program. Best practices could include:

- Training staff on sanctions risks and common red flags. This includes not only compliance

4 Please see the Department of Commerce's Resources On Export Controls Implemented In Response To Russia's Invasion Of Ukraine for additional information. The Department of Commerce has imposed broad export controls on certain items subject to the Export Administration Regulations (EAR), including all items listed in the Commerce Control List (CCL) and certain EAR99 items identified by HS Code, for exports or reexports to Russia or Belarus.

5 Please see the following: Cracking Down on Third-Party Intermediaries Used to Evade Russia-Related Sanctions and Export Controls, Impact of Sanctions and Export Controls on Russia's Military-Industrial Complex, Department of Commerce's Resources On Export Controls Implemented In Response To Russia's Invasion Of Ukraine, Supplemental Alert: FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Continued Vigilance for Potential Russian Export Control Evasion Attempts, Trends in Bank Secrecy Act Data: Suspected Evasion of Russian Export Controls, Russia Business Advisory - United States Department of State, and Tri-Seal Compliance Note: Obligations of foreign-based persons to comply with U.S. sanctions and export control laws.

personnel but also front-line staff, senior management, and business lines (e.g., underwriters, relationship managers). It is especially important to train staff that while it is appropriate for customers to ask for guidance on how to comply with bank policies and sanctions, any request for assistance in evading sanctions should be treated as a serious red flag and result in appropriate mitigation measures.

- Ensuring any identified risks or issues are escalated quickly to the proper level (e.g., senior risk committee) and promoting a "culture of compliance."
- Communicating clearly and frequently with U.S. and other correspondent banks on their due diligence expectations and requests for information.
- Incorporating information and typologies from relevant FinCEN and OFAC alerts and advisories into automated and manual anti-money laundering controls. Of particular concern for Russian sanction evasion are:
  - Customers conducting business with newly formed Russian companies or newly formed companies in third countries known to be potential transshipment points for exports to Russia.
  - Companies or counterparties supposedly involved in production or import-export of sophisticated items with no business history or little-to-no web presence.
  - Customers or counterparties using unusual or atypical payment terms and methods, such as large cash payments, frequent or last-minute changes to end-users or payees, or routing payments through third countries not otherwise involved in the transaction.

Permissible Transactions

OFAC's targeting authorities under E.O. 14024 aim to reduce the ability of Russia's military-industrial base to circumvent sanctions to support its war aims and do not target otherwise permissible trade. Foreign persons do not risk the imposition of sanctions for engaging in transactions authorized for U.S. persons under general licenses issued under the Russian Harmful Foreign Activities Sanctions program or that are exempt. As previously stated in OFAC guidance, legitimate humanitarian activity and agricultural and medical trade are not the target of our sanctions.

OFAC maintains a broad authorization for transactions otherwise prohibited by E.O. 14024 related to the production, manufacturing, sale, transport, or provision of agricultural commodities, agricultural equipment, medicine, medical devices, replacement parts and components for medical devices, or software updates for medical devices. Please see Russia-related General License (GL) 6D and OFAC Food Security Fact Sheet: Russia Sanctions and Agricultural Trade. This authorization remains valid. Foreign financial institutions may engage in or facilitate transactions that would be authorized for U.S. persons

6 GL 6D does not relieve any person from compliance with any other federal laws or requirements of other federal agencies, including the Export Administration Regulations (EAR), 15 C.F.R. Parts 730–774, which are administered by the U.S. Department of Commerce.

under GL 6D without exposure to sanctions.[6]

OFAC also has authorizations in place for transactions related to energy (GL 8J), certain transactions in support of non-governmental organizations (GL 27), official business of third-country diplomatic or consular missions located in the Russian Federation (GL 20), telecommunications and internet-based communications (GL 25C), and official business of certain international organizations and entities by employees, grantees, or contractors thereof (31 CFR 587.510). Additionally, the importation or exportation of information or informational materials and transactions ordinarily incident to travel to or from any country are exempt under the International Emergency Economic Powers Act (IEEPA).

Contacting OFAC

OFAC welcomes continued engagement with the private sector in identifying best practices that are effective in preventing Russian sanctions evasion. We encourage financial institutions with questions or who wish to share information about best practices to contact OFAC.