

August 16, 2022

Commodity, End-user, and Transshipment Country Red Flag FAQs

Q1: What are the primary commodities which BIS is concerned may be subject to unauthorized export to Russia and/or Belarus in furtherance of the Russian war effort?

A1:

Based upon historical information and current developments, BIS has identified the following commodities as presenting a special concern because of their potential diversion to and end use by Russia and Belarus to further their military and defense capabilities-

Aircraft Parts and Equipment – ECCN 9A991

Antennas – ECCN 7A994

Breathing Systems – ECCN 8A992

Cameras – ECCN 6A993

GPS Systems – ECCN 7A994

Inertial Measurement Units – ECCN 7A994

Integrated Circuits – ECCN 3A001, 3A991, 5A991

Oil Field Equipment – ECCN EAR99

Sonar Systems – ECCN 6A991

Spectrophotometers – ECCN 3A999

Test Equipment – ECCN 3B992

Thrusters (Marine) – ECCN 8A992

Underwater Communications – ECCN 5A991

Vacuum Pumps – ECCN 2B999

Wafer Fabrication Equipment – ECCN 3B001, 3B991

Wafer Substrates – ECCN 3C001 through 3C006

These commodities are of special concern because they support the development of maritime technology, microelectronics, and other technologies that can be used to support Russia's military and defense sector. These items were identified based on historical and current trends in Russia's procurement efforts on behalf of their defense industrial base. Most of these items were previously easily obtainable by Russia-based entities prior to the imposition of more stringent export controls in response to the invasion of Ukraine. After the imposition of those controls, all of the items listed above require a BIS license prior to export or reexport to Russia or Belarus. The above list is not exhaustive of all commodities requiring a license for export to Russia and/or Belarus. For a full list of items that now require a license if destined to Russia or Belarus, *see* 15 CFR Part 746, Supp. Nos. 2, 4, and 5, and Part 774, Supp. No. 1.

Q2: What are some “Red Flags” that may be indicative of attempts to evade Russia/Belarus sanctions?

A2:

Illicit actors use a variety of methods when trying to acquire items controlled under the EAR. To evade scrutiny, illicit actors often attempt to procure EAR99 items – a category generally referring to low-tech consumer goods not specified on the Commerce Control List that do not require a license for export, re-export, or transfer to most destinations. Illicit actors also will engage complicit shippers (or customs brokers) to obscure either the nature of the goods or their ultimate destinations, similar to procurement efforts involving other illicit goods. The below is a select list of potential red flags which may indicate export control evasion-

RF1: A customer in the maritime industry transports commodities of concern and uses trade corridors known to serve as possible transshipment points for export to Russian and Belarus.

RF2: The nature of a customer’s underlying business (specifically military or government-related work), type of service(s) or product(s) offered, and geographical presence pose additional risks of involvement in the evasion of export controls for Russia and Belarus.

RF3: A customer acquires new vessels for no apparent economic or business purpose or for use in shipping corridors involving one or more of the identified transshipment countries.

RF4: A customer purchases or sells vessels or other properties and goods identified as having been involved with or being blocked property under U.S. or partner country sanctions.

RF5: Transactions involving entities with little to no web presence.

RF6: Transactions involving a change in shipments or payments that were previously scheduled to go to Russia or Belarus, or a company located in Russia or Belarus, but that are now going to a different country/company.

RF7: Transactions involving payments being made from entities located in third-party countries not otherwise involved with the transactions and known to be a potential transshipment point for exports to Russia and Belarus.

RF8: Last-minute changes to transactions associated with an originator or beneficiary located in Russia or Belarus.

RF9: Parties to transactions with addresses that do not appear consistent with the business or are otherwise problematic (e.g., either the physical address does not exist, or it is residential).

RF10: Transactions involving consolidated shipments of luxury goods that previously would have been destined for Russia or Belarus, but are now destined for a transshipment country or a country without restrictions on exports/re-exports to Russia or Belarus.

RF11: Rapid shifts to new purchasers in transactions involving restricted luxury goods.

RF12: Transactions involving freight-forwarding firms that are also listed as the product's final end customer, especially items going to traditional Russian transshipment hubs.

RF13: Transactions associated with atypical shipping routes for a product and destination.

RF14: Transactions involving companies that are physically co-located with or have shared ownership with an entity on the BIS Entity List or the Department of the Treasury's Specially Designated Nationals and Blocked Persons List. Addresses may be searched via the [Consolidated Screening List search engine](#) maintained by the Department of Commerce, International Trade Administration.

RF15: New or existing accounts and transactions by individuals with previous convictions for violating U.S. export control laws, particularly if appearing to involve export and import activities or services.

RF16: When combined with other derogatory information, large dollar or volume purchases, including through the use of business credit cards, of items designated as EAR99 (or large volume or dollar purchases at wholesale electrical/industrial merchants, electrical parts and equipment providers, or electronic parts providers), in the United States or abroad, especially if paired with purchases at shipping companies.

RF17: Companies or individuals with links to Russian state-owned corporations (including shared ownership, as well as branches of, subsidiaries of, or shareholders in

such state-owned corporations) involved in export-related transactions or the provision of export-related services.¹

RF18: Export transactions involving non- U.S. parties that have shared owners or addresses with Russian state-owned entities or designated companies.

RF19: Transactions involved in the import and export of electronic equipment where transactions are conducted with third country- based electronics and aerospace firms that also have offices in Russia or Belarus.

RF20: Transactions connected to Russian petroleum-related firms or firms that resell electronics and other similar items to Russian firms.

RF21: Transactions involving entities whose website or business registration states the entities work on “special purpose projects.” The phrase “special purpose projects” is a Russian designation that typically means for military use.

RF22: Transactions involving companies that display a certificate from the Federal Security Service of the Russian Federation (FSB RF), which allows these companies to work on projects classified as a state secret. Companies will typically display this certificate on the Russian language version of their website.

¹ Companies linked to the Russian state may have the following designations within their business name: RAO (Rossiyskaya Aktsionernaya Kompaniya), which designates a Russian joint stock company; FGUP/FSUE (Federal'noye Gosudarstvennoye Unitamoye Predpriyatiye), which designates a Russian Federal State Unitary Enterprise; GK (Gosudarstvennaya Korporatsiya), which designates a Russian State Corporation; SPRE/NIPP (Nauchno-Issledovatel'skoye Proizvodstvennoye Predpriyatiye), which designates a Russian Scientific Research Production Enterprise; and NPO/GNPO (Gosudarstvennyy Nauchno-Proizvodstvennyy Tsentr), which designates a Russian State Research and Production Center.

The list is not exhaustive but may be helpful in risk assessment. All such indicators should be considered in conjunction with all surrounding facts and circumstances as part of a comprehensive approach to risk assessment. The presence of a red flag, in isolation, does not necessarily render a transaction suspicious.

Q3: What countries are especially prone to being used as transshipment points to mask sanctions evasion?

A3:

BIS has identified several countries as transshipment points through which restricted or controlled exports have been known to pass before reaching destinations in Russia or Belarus. These countries have been identified through analysis of historical and current trends, relying heavily of export and re-export data, as well as changes identified through compliance efforts in the field. These locations include, but are not limited to, Armenia, Brazil, China, Georgia, India, Israel, Kazakhstan, Kyrgyzstan, Mexico, Nicaragua, Serbia, Singapore, South Africa, Taiwan, Tajikistan, Turkey, United Arab Emirates, and Uzbekistan. In some instances, controlled U.S. items may be legally exported to these and other jurisdictions as inputs for the production of other finished goods. However, further export to Russia or Belarus of those finished products and goods, potentially through additional transshipment points, may be prohibited.