BUREAU OF INDUSTRY AND SECURITY
FREQUENTLY ASKED QUESTIONS
APPLICABLE LICENSE REQUIREMENTS
CURRENT AS OF MAY 2, 2022

Q1: What are the additional items that require a license for export, reexport, and transfer (in-country) to Russia and Belarus under the EAR?

A1:

I. Section 746.8 is the primary EAR section that imposes additional sanctions on Russia and Belarus. Pursuant to Section 746.8, items that are subject to the EAR and have an Export Control Classification Number (ECCN) in all Categories on the CCL are subject to a license requirement. This license requirement excludes deemed exports and reexports of technology and/or source code or software that are destined for Russian or Belarusian persons in the United States or in a third country. (see §§ 746.8, 734.13(a)(2), and 734.14(a)(2) of the EAR)

II. Any item "subject to the EAR" if you have "knowledge" that the item is intended, entirely or in part, for a 'military end use' or 'military end user' in Russia or Belarus. Note that Russian and Belarusian 'military end users' that were previously listed in supplement 7 to part 744 have been added to the Entity List in supplement no. 4 to part 744 pursuant to recent Russia-related rules and are subject to more stringent requirements regarding certain foreign-produced items as set forth in § 746.8(a)(3) of the EAR. This is discussed further below. (see §§ 744.11 and 744.21 of the EAR)

III. Certain foreign-produced items that
   a) Have greater than a *de minimis* level of U.S.-origin controlled content (see §§ 734.4 and 746.8(a)(5) of the EAR); or
   b) Are the "direct product" of U.S.-origin "technology" or "software" subject to the EAR, or that are produced using items that are the "direct product" of U.S.-origin "technology" or "software" subject to the EAR. (see § 734.9(f) and (g) of the EAR)

IV. All items destined to the so-called Donetsk People's Republic (DNR) and Luhansk People's Republic (LNR) regions of Ukraine that are subject to the EAR, except food or medicine designated EAR99 and software necessary to enable personal communications over the Internet. This requirement is consistent with the license requirements for the Crimea region of Ukraine that were imposed in 2015 in response to Russia's 2014 occupation of the Crimea region. (see § 746.6 of the EAR - Crimea Region of Ukraine and Covered Regions of Ukraine)

V. Items identified in § 746.5(a)(1) and in supplement no. 4 to part 746 the EAR, for use in the oil industry sector. (see § 746.5(a)(1)(i) and (ii) of the EAR)

VI. 'Luxury goods' subject to the EAR and identified in supplement no. 5 to part 746 of the EAR that are exported, reexported or transferred (in-country) to Russia or Belarus, and to certain Russian and Belarusian oligarchs and malign actors identified in § 746.10 of the EAR, wherever they are located.

Q2: Do EAR99 items need a license for export, reexport or transfer (in-country) to Russia and Belarus?

A2: Items that are subject to the EAR and designated EAR99 do not require a license for export, reexport or transfer (in-country) to Russia or Belarus at this time UNLESS they are:

- 'Luxury goods' subject to the EAR and identified in supplement no. 5 to part 746 of the EAR;
- Items subject to the EAR that is for use in the Russian oil industry sector and identified in supplement nos. 2 and 4 to part 746 of the EAR;
- Items destined to prohibited end uses and end users listed in part 744 of the EAR;* or,
- Items destined to the Crimea region of Ukraine, or to the Donetsk and Luhansk regions of Ukraine (the so-called Donetsk People's Republic (DNR) or the Luhansk People's Republic (LNR)), except for EAR99 food, medicine, or software necessary to enable personal communications over the Internet.

*Prohibited entities listed in part 744 include entities listed on the Entity List in supplement no. 4 to part 744. The License Requirement column of the Entity List specifies which items require a license for export, reexport, or transfer (in-country) to each listed entity, and the License Review Policy indicates whether a license is likely to be granted for that entity. Also note that for entities listed on the Entity List that have a footnote 3 designation, "items subject to the EAR" includes foreign-produced items that are subject to the EAR under § 734.9(g) of the EAR.

Q3: Does the download of software that is subject to the EAR and controlled on the Commerce Control List (i.e., software that is not designated EAR99) in Russia and Belarus require a license?

A3: Generally, yes, although in some cases a license exception, such as License Exception Consumer Communications Devices (CCD), may be available (see License Exceptions below). A download from the Internet of software subject to the EAR is an export from the U.S. (or a reexport from a third country) to the country in which the download occurs. (See §§ 734.13(a)(1) and 734.14(a)(1) of the EAR.) Such downloads would require export or reexport licenses to Belarus or Russia under Section 746.8 of the EAR if the software is listed on the CCL. These license requirements also apply to the export or reexport of software subject to the EAR for storage on a cloud server when that server is physically located in Russia or Belarus, as well as to the download of software updates for software subject to the EAR located in either country, unless the transaction qualifies for a license exception as described below.

Q4: Do we need a license to export, reexport or transfer (in-country) items that are controlled for anti-terrorism (AT) reasons only to a Russian commercial company customer, which is not a military end user, and not on any prohibited parties lists or in any way associated with the Russian government? Do we need a license to export, reexport or transfer (in-country) such items if we are selling them on an electronic marketplace (e.g., eBay)?

A4: Yes, items that are subject to the EAR and listed on the CCL, including items classified under AT-only ECCNs (*i.e.*, ECCNs that have only AT specified in the "reason for control" paragraph), require a license for export, reexport, or transfer (in-country) to Russia and Belarus, except for deemed exports or reexports of technology, software, and/or source code to Russian and Belarusian persons in the United States or in a third country. Note that these license requirements are also applicable to transactions that originate on eBay or other online sales sites.

BUREAU OF INDUSTRY AND SECURITY
FREQUENTLY ASKED QUESTIONS
LICENSE APPLICATION REVIEW POLICY
CURRENT AS OF MAY 2, 2022

Q1: What is the license application review policy for the items that require a license under the regulations to Russia and Belarus and to individuals who are Russian and Belarusian persons?

A1: The license review policy relies on the facts and circumstances of each transaction as follows:

I. License applications for items that are classified under ECCNs on the CCL will be reviewed under a policy of denial, except as specified below.

II. License applications for all items intended, entirely or in part, for a 'military end use' or 'military end user' in Russia or Belarus are reviewed under a policy of denial. (see § 744.21(e) of the EAR)

III. License applications for 'luxury goods' destined to any end user in Russia or Belarus and to certain Russian and Belarusian oligarchs and malign actors, wherever they are located, are reviewed under a policy of denial. (see § 746.10 and supplement no. 5 to part 746)

IV. License applications for transactions subject to the two license requirements set forth in § 746.5 of the EAR (Russian industry sector sanctions) will generally be reviewed under a policy of denial. (see § 746.5 (a)(1)(i) and (ii) of the EAR).

V. License applications for items destined to Crimea or to the so-called Donetsk People's Republic (DNR) and Luhansk People's Republic (LNR) regions of Ukraine (Covered Regions of Ukraine), are reviewed under a policy of denial, except that applications for transactions authorized under OFAC Ukraine-Related General Licenses will be reviewed on a case-by-case basis. (see § 746.6 of the EAR)

VI. With respect to new § 746.5(a)(1)(ii) (oil refinery-related equipment), applications for export, reexport, or transfer (in-country) of items that may be necessary for health and safety reasons will be reviewed under a case-by case license review policy. (Note that this license application review policy continues to apply to applications that fall within the scope of § 746.5(a)(1)(i).)

VII. License applications for licenses required under § 746.8(a)(1) and (2) in the following scenarios will be reviewed on a case-by-case basis. The case-by-case review will take into consideration whether the transaction in question would benefit the Russian or Belarusian government or defense sector:

a) applications related to safety of flight;
b) applications related to maritime safety;
c) applications for civil nuclear safety;
d) applications to meet humanitarian needs;
e) applications that support government space cooperation;
f) applications for items destined to:

- wholly-owned U.S. subsidiaries,
- foreign subsidiaries of U.S. companies that are joint ventures with other U.S. companies,
- joint ventures of U.S. companies with companies headquartered in countries from Country Group A:5 and A:6 in supplement no. 1 to part 740 of the EAR,
- wholly-owned subsidiaries of companies headquartered in countries from Country Group A:5 and A:6 in supplement no. 1 to part 740, and
- joint ventures of companies headquartered in Country Groups A:5 and A:6 with other companies headquartered in Country Groups A:5 and A:6;

g) applications for companies headquartered in Country Groups A:5 and A:6 to support civil telecommunications infrastructure; and
h) applications involving or in support of government-to-government activities.

VIII. The license review policy for license applications for Russian and Belarusian entities that are listed on the Entity List pursuant to 744.11 are set forth in the license review policy column on the entity List in supplement no. 4 to part 744 of the EAR.

FinCEN & BIS Joint Alert

FIN-2022-Alert003 **June 28, 2022**

FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts

Suspicious Activity Report (SAR) Filing Request:
FinCEN requests financial institutions reference this alert in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the following key term: "**FIN-2022-RUSSIABIS**".

The Financial Crimes Enforcement Network (FinCEN) and the U.S. Department of Commerce's Bureau of Industry and Security (BIS)[1] are issuing a joint alert[2] urging financial institutions[3] to be vigilant against efforts by individuals or entities to evade BIS export controls implemented in connection with the Russian Federation's (Russia) further invasion of Ukraine. This joint alert provides financial institutions with an overview of BIS's current export restrictions; a list of commodities of concern for possible export control evasion; and select transactional and behavioral red flags to assist financial institutions in identifying suspicious transactions relating to possible export control evasion. This alert further reminds financial institutions of their Bank Secrecy Act (BSA) reporting obligations and details how suspected export control evasion activity may also be reported to BIS enforcement authorities.

Overview of Recent BIS Actions in Response to the Invasion of Ukraine

Since February 24, 2022, BIS has implemented a series of stringent export controls that restrict Russia's access to specific technologies and other items that it needs to sustain its military activity in Ukraine.[4] These controls primarily target Russia's defense, aerospace, and maritime sectors. They also include other targets such as Russia's energy production sector as well as luxury goods used by Russian

1. BIS advances U.S. national security, foreign policy, and economic objectives by ensuring an effective export control and treaty compliance system, and by promoting continued U.S. leadership in strategic technologies. *See generally*, Bureau of Industry and Security | U.S. Department of Commerce.
2. For previous FinCEN alerts related to Russia's invasion of Ukraine, *see* "FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts," (FinCEN Alert on Russian Sanctions Evasion) (March 7, 2022) and "FinCEN Alert on Real Estate, Luxury Goods, and Other High-Value Assets Involving Russian Elites, Oligarchs, and their Family Members," (March 16, 2022). For further reference, *see also* FinCEN "Advisory on Kleptocracy and Foreign Public Corruption," (April 14, 2022), which includes a discussion of Russian political corruption.
3. *See* 31 U.S.C. § 5312(a)(2); 31 CFR § 1010.100(t).
4. Information on the numerous actions taken by BIS in response to Russia's invasion of Ukraine is available here: Resources on Export Controls Implemented in Response to Russia's Invasion of Ukraine (last updated June 24, 2022).

elites. These controls are aligned with export controls implemented by 37 U.S. allies and partners[5] and represent the most comprehensive application of Commerce's export authorities targeting a single country.[6] The United States has also applied restrictions to Belarus in response to its substantial enabling of Russia's war effort.[7] These actions are part of a coordinated international endeavor to apply economic pressure on Russia and Belarus to degrade the military capabilities that Russia uses to wage its war, and to restrict Russia's access to items that can support the country's defense industrial base and military and intelligence services.[8] They also increase the costs on Russian and Belarusian persons who support the government of Russia and its invasion of Ukraine.[9]

These recent BIS actions also build on export restrictions that the United States previously established following Russia's occupation of Crimea in 2014,[10] and in response to other malign Russian activities. Some of these prior restrictions remain in effect, while others have been expanded in scope through BIS's recent regulatory actions. These actions have imposed controls on a range of items subject to the Export Administration Regulations (EAR)[11] that had not previously required export licenses when destined for Russia or Belarus. The new controls place significant restrictions on (i) U.S. exports, reexports, and in-country transfers to Russia, and (ii) products destined for Russia and manufactured abroad with certain U.S. technology, software, or tooling. BIS imposed similar controls on items subject to the EAR and destined for Belarus, including broad in-country transfer controls. With this joint alert, FinCEN is partnering with BIS to assist U.S. financial institutions in identifying customers and transactions that may pose elevated risks of attempted export control evasion.

5. For a list of countries who have committed to implementing substantially similar export controls on Russia and Belarus under their domestic laws, *see* 15 CFR, Supplement No. 3 to Part 746.
6. *See* BIS Press Release, "Commerce Implements Sweeping Restrictions on Exports to Russia in Response to Further Invasion of Ukraine," (February 24, 2022).
7. *See* BIS Press Release, "Commerce Imposes Sweeping Export Restrictions on Belarus for Enabling Russia's Further Invasion of Ukraine," (March 2, 2022).
8. *See* White House, "Executive Order on Prohibiting Certain Imports, Exports, and New Investment with Respect to Continued Russian Federation Aggression," (March 11, 2022); White House, "FACT SHEET: United States, European Union, and G7 to Announce Further Economic Costs on Russia," (March 11, 2022); "Joint Statement by the G7 Announcing Further Economic Costs on Russia," (March 11, 2022); *see also*, Commerce & BIS, "Russia and Belarus Rule Fact Sheet," (March 7, 2022); U.S. Department of the Treasury (Treasury) Press Releases (Treasury Press Release), "Treasury Prohibits Transactions with Central Bank of Russia and Imposes Sanctions on Key Sources of Russia's Wealth," (February 28, 2022).
9. *See* BIS Press Release, "Commerce Restricts the Export of Luxury Goods to Russia and Belarus and to Russian and Belarusian Oligarchs and Malign Actors in Latest Response to Aggression Against Ukraine," (March 11, 2022).
10. For more information *see* Resources on Russia-Related Export Controls, *supra* note 4.
11. The EAR are issued by BIS pursuant to laws relating to the control of certain exports, reexports, and activities. For more information, *see* 15 CFR §§ 730–774.

Commodities of Concern

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

Item	Export Control Classification Number[12]	Item	Export Control Classification Number
Aircraft Parts/ Equipment	9A991	Sonar Systems	6A991
Antennas	7A994	Spectrophotometers	3A999
Breathing Systems	8A992	Test Equipment	3B992
Cameras	6A993	Thrusters	8A992
GPS System	7A994	Underwater Communications	5A991
Inertial Measurement Units	7A994	Vacuum Pumps	2B999
Integrated Circuits	3A001, 3A991, 5A991	Wafer Fabrication Equipment	3B001, 3B991
Oil Field Equipment	EAR99	Wafer Substrates	3C00x

BIS remains concerned about exports that support the development of maritime technology, microelectronics, and other technologies that can be used to support Russia's military and defense sector. As such, all of the items listed above require a BIS license prior to export or reexport to Russia or Belarus. Additionally, the use of certain of these items by third countries to create final products that may be subsequently exported to Russia or Belarus is also prohibited. This is not a complete listing of commodities sought by or prohibited for end-users in Russia and Belarus,[13] but this list of commodities that present special concern can assist in the risk-based screening of export-related financial transactions.[14]

12. *See generally*, International Trade Administration, Export Control Classification Number (ECCN) and Export Administration Regulation (EAR99).
13. For a full list of items that now require a license if destined for Russia or Belarus, *see* 15 CFR Part 746, Supp. Nos. 2, 4, and 5, and Part 774, Supp. No. 1.
14. To support risk-based screening of export-related financial transactions, financial institutions may refer to the *Consolidated Screening List* (CSL) search engine maintained by the U.S. Department of Commerce's International Trade Administration (ITA), available online here: https://www.trade.gov/consolidated-screening-list. The CSL is a list of parties for which the United States Government maintains restrictions on certain exports, reexports, or transfers of items and includes multiple export screening lists of the Departments of Commerce, State, and Treasury.

Applying a Risk-Based Approach to Trade Finance

Export-Related Financial Activity Potentially Visible to Financial Institutions

A financial institution may have visibility into various aspects of export-related financial activity, including:

1. **Its customer (exporter) receives a letter of credit from its customer (the importer),**
2. **The financial institution issues a line of credit to its customer (exporter) to facilitate the transaction, or**
3. **The importer's wire transfer payment for the export is received by the exporter's financial institution or handled as part of a correspondent banking transaction.**

Financial institutions, particularly banks but also credit card operators and foreign exchange dealers, may be involved in providing financing, processing payments, or performing other services associated with international trade. These services include, but are not limited to, processing payments for exported goods, issuing lines of credit for exporters, providing or handling the payments supported by letters of credit, processing payments associated with factoring of accounts receivables by an exporter, providing general credit or working capital loans, and issuing or paying insurance on the shipping and delivery of goods to protect the exporter from nonpayment by the buyer.

Financial institutions with customers in maritime or export/import industries should rely on the financial institutions' internal risk assessments to employ appropriate risk mitigation measures consistent with their underlying BSA obligations. This approach to compliance with the BSA may include appropriate due diligence policies and procedures as required by law and regulation, such as, where applicable, FinCEN's customer due diligence and beneficial ownership requirements.[15]

Financial institutions directly involved in providing trade finance for exporters also may have access to information relevant to identifying potentially suspicious activity. This may include their customers' end-use certificates, export documents, or other more extensive documentation associated with letters of credit-based trade financing. Or it may include information about the other parties to the transactions that may be contained in payment transmittal orders they receive or handle as an intermediary institution, such as Society for Worldwide Interbank Financial Telecommunications (SWIFT) messages, which are increasingly associated with open account trade transactions. For other export-related financial activity potentially visible to financial institutions, see the text box above.

15. *See*, for example, customer identification program requirements established in 31 CFR § 1010.220 as applicable to specific types of financial institutions in 31 CFR § 1020.220 (banks), § 1023.220 (broker-dealers), § 1024.220 (mutual funds), and § 1026.220 (futures/commodities). *See also* the beneficial ownership requirements for legal entity customers established in 31 CFR § 1010.230.

Select Red Flag Indicators of Export Control Evasion

Illicit actors use a variety of methods when trying to acquire items controlled under the EAR.[16] 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[17] 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 efforts with other illicit goods.[18]

FinCEN and BIS are providing a select list of potential red flag indicators of export control evasion that may be relevant to financial institutions and other covered institutions or persons, including flags derived from recent BSA reporting.[19] Consideration of these indicators, in conjunction with conducting appropriate risk-based customer and transactional due diligence, will assist in determining whether an identified activity may be connected to export control evasion.[20] As no single financial red flag is necessarily indicative of illicit or suspicious activity, all the surrounding facts and circumstances should be considered before determining whether a specific transaction is suspicious or associated with potential export control evasion.

Transactional and Behavioral Red Flags:

1. A customer in the maritime industry transports commodities of concern and uses trade corridors known to serve as possible transshipment points[21] for exports to Russia and Belarus.

16. *See* FinCEN "Advisory to Financial Institutions on Filing Suspicious Activity Reports regarding Trade-Based Money Laundering," (February 18, 2010); *see also* FinCEN Alert on Russian Sanctions Evasion, *supra* note 2.
17. All items on the Commerce Control List (CCL) require export licenses when destined for Russia or Belarus. For more information, *see* BIS's webpage on the Commerce Control List.
18. For information on common deceptive shipping practices and general approaches to tailor due diligence and sanctions compliance policies and procedures, *see* U.S. Department of State, U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), and the U.S. Coast Guard, "Sanctions Advisory for the Maritime Industry, Energy and Metals Sectors, and Related Communities," (May 14, 2020).
19. BIS has a general website available with red flags for identifying efforts to evade export restrictions and other controls. *See* Commerce Department BIS, Red Flag Indicators.
20. Consistent with these existing regulatory obligations, financial institutions should take reasonable, risk-based steps to identify and limit any exposure they may have to funds and other assets associated with Russian or Belarussian export control evasion. Such reasonable steps should not, however, put into question a financial institution's ability to maintain or continue appropriate relationships with customers or other financial institutions and should not be used as the basis to engage in wholesale or indiscriminate de-risking of any class of customers or financial institutions.
21. BIS has identified certain common transshipment points through which restricted or controlled exports have been known to pass before reaching destinations in Russia or Belarus. These points 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. The recent export controls and restrictions on Russia and Belarus may lead to changes in historical transshipment patterns, and BIS is actively monitoring relevant information, including BSA reporting, to identify any such changes. As such, the list is not inclusive of all potential transshipment points, but can assist in the risk-based screening of export-related financial transactions.

2. 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 unintentional involvement in the evasion of export controls for Russia and Belarus.

3. 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.

4. 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.

5. Transactions involving entities with little to no web presence.

6. 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.

7. 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.

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

9. 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).

10. 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.

11. Rapid shifts to new purchasers of transactions involving restricted luxury goods.

12. Transactions involving freight-forwarding firms[22] that are also listed as the product's final end customer, especially items going to traditional Russian transshipment hubs.

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

14. Transactions involving entities whose website or business registration states the entities work on "special purpose projects."[23]

15. 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.[24]

22. A freight forwarder is a person or company that loads, or charters and loads, any form of transport or a person whose business is to receive and forward goods. The goods are often sent in a container for multimodal transport. *See generally* BIS, Freight Forwarder Guidance.
23. The phrase "special purpose projects" is a Russian designation that typically means for military use.
24. Companies will typically display this certificate on the Russian language version of their website.

16 Transactions involving companies that are physically co-located with or have shared ownership with an entity on the BIS Entity List[25] or the Department of the Treasury's Specially Designated Nationals and Blocked Persons List.[26]

17 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.

18 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.

19 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.[27]

20 Export transactions identified through correspondent banking activities involving non-U.S. parties that have shared owners or addresses with Russian state-owned entities or designated companies.

21 Use of business checking or foreign exchange accounts by U.S.-based merchants 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.

22 Transactions identified through correspondent banking activities connected to Russian petroleum-related firms or firms that resell electronics and other similar items to Russian firms.

25. The BIS Entity List is a list of certain foreign persons—including businesses, research institutions, government and private organizations, individuals, and other types of legal persons—that are subject to specific license requirements for the export, reexport and/or transfer (in-country) of specified items. These persons comprise the Entity List, which is found in Supplement No. 4 to Part 744 of the EAR. The persons on the Entity List are subject to licensing requirements and policies supplemental to those found elsewhere in the EAR.
26. Addresses may be searched via the *Consolidated Screening List* search engine. *See supra* note 14.
27. 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 Unitarnoye Predpriyatiye), which designates a Russian Federal State Unitary Enterprise; GK (Gorsudarstvennaya 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.

Reminder of Relevant BSA Obligations for U.S. Financial Institutions[28]

Suspicious Activity and Other BSA Reporting

A financial institution is required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity, or attempts to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity, including sanctions or export control evasion.[29] All statutorily defined financial institutions may voluntarily report suspicious transactions under the existing suspicious activity reporting safe harbor.[30]

When a financial institution files a SAR, it is required to maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR.[31] Financial institutions must provide any requested SAR and all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency.[32] When requested to provide supporting documentation, financial institutions should take special care to verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency. A financial institution should incorporate procedures for such verification into its BSA compliance or AML program. These procedures may include, for example, independent employment verification with the requestor's field office or face-to-face review of the requestor's credentials.

SAR Filing Instructions

FinCEN requests that financial institutions reference this alert by including the key term "**FIN-2022-RUSSIABIS**" in SAR field 2 (Filing Institution Note to FinCEN) and the narrative to indicate a connection between the suspicious activity being reported and the activities highlighted in this alert. Financial institutions may highlight additional advisory or alert keywords in the narrative, if applicable. FinCEN also requests that financial institutions check box 38(z) (Other Suspicious Activity) and note "Russia Export Restrictions Evasion". If known, please also indicate in field 45(z) (Other Product Types) the appropriate North American Industry Code(s) (NAICs) for the involved product, and/or the appropriate financial instrument or payment mechanism in field 46.

28. For additional relevant guidance, *see Reminder of Relevant BSA Obligations and Tools for U.S. Financial Institutions* from FinCEN's second Russia-related Alert, *supra* note 2.
29. *See* 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320. All financial institutions with these SAR filing requirements also may file a SAR regardless of the amount involved (if any) and regardless of whether the transaction was completed or only attempted.
30. *See* 31 U.S.C. § 5318(g)(3).
31. *See* 31 CFR §§ 1020.320(d), 1021.320(d), 1022.320(c), 1023.320(d), 1024.320(c), 1025.320(d), 1026.320(d), 1029.320(d), 1030.320(d).
32. *Id; see also* FinCEN, "Suspicious Activity Report Supporting Documentation," (June 13, 2007).

Financial institutions wanting to expedite their report of suspicious transactions that may relate to the activity noted in this alert should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).[33]

Financial institutions should include any and all available information relating to the products or services involved in the suspicious activity, including all available transportation and trade financing documentation, accounts and locations involved, identifying information and descriptions of any legal entities or arrangements involved or associated with beneficial owners, and any information about related persons or entities (including transportation companies or services) involved in the activity. Financial institutions also should provide any and all available information regarding other domestic and foreign financial institutions and businesses or persons involved in the activity. Where appropriate, financial institutions should consider filing a SAR jointly on shared suspicious activity.[34]

Other Relevant BSA Reporting Requirements

Financial institutions and other covered institutions or persons also may have other relevant BSA reporting requirements that provide information in connection with the subject of this alert.[35] These include obligations related to the Currency Transaction Report (CTR),[36] Report of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300),[37] Report of Foreign Bank and Financial Accounts (FBAR),[38] Report of International Transportation of Currency or Monetary Instruments (CMIR),[39] Registration of Money Service Business (RMSB),[40] and

33. The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.
34. *See* 31 CFR §§ 1020.320(e)(1)(ii)(A)(2))(i), 1021.320(e)(1)(ii)(A)(2)), 1022.320(d)(1)(ii)(A)(2), 1023.320(e)(1)(ii)(A)(2)(i), 1024.320(d)(1)(ii)(A)(2), 1025.320(e)(1)(ii)(A)(2), 1026.320(e)(1)(ii)(A)(2)(i), 1029.320(d)(1)(ii)(A)(2), 1030.320(d)(1)(ii)(A)(2).
35. BSA reporting refers to legal requirements that financial institutions and certain businesses and persons report certain financial transactions (such as large-dollar cash transactions), suspicious activity, or other information (such as information on a taxpayer's foreign bank and financial accounts) to FinCEN "that are highly useful in (A) criminal, tax, or regulatory investigations, risk assessments, or proceedings; or (B) intelligence or counterintelligence activities, including analysis, to protect against terrorism;" 31 U.S.C. § 5311(1).
36. A report of each deposit, withdrawal, exchange of currency or other payment or transfer, by, through, or to the reporting financial institution which involves a transaction in currency of more than $10,000, in aggregate per business day. 31 CFR §§ 1010.310-313, 1020.310-313, 1021.310-313, 1022.310-313, 1023.310-313, 1024.310-313, 1026.310-313.
37. A report filed by any U.S. person engaged in a trade or business on the receipt of more than $10,000 in currency in one transaction or two or more related transactions involving the trade or business. Such transactions are required to be reported on joint FinCEN/IRS Form 8300 when not otherwise required to be reported under the CTR requirements. 31 CFR §§ 1010.330, 1010.331 (Clerks of the Court).
38. A U.S. person that has a financial interest in or signature authority over foreign financial accounts must file an FBAR if the aggregate value of the foreign financial accounts exceeds $10,000 at any time during the calendar year, as specified in 31 CFR § 1010.350 and FinCEN Form 114.
39. Each person (i.e., an individual or legal entity), as defined in 31 CFR § 1010.100(mm), that transports, ships, or mails more than $10,000 of currency or other monetary instruments into or out of the United States must file a CMIR. 31 CFR § 1010.340.
40. Report for a business required to register with FinCEN as a money services business, as defined in 31 CFR § 1010.100(ff), or renewing the registration. 31 CFR § 1022.380.

Designation of Exempt Person (DOEP).[41] These standard reporting requirements may not have an obvious connection to Russia-related illicit finance, but may ultimately prove highly useful to law enforcement.

Form 8300 Filing Instructions

Covered institutions or persons may file a Form 8300 voluntarily for any suspicious transaction, even if the total amount does not exceed $10,000.[42] When filing a Form 8300 involving a suspicious transaction relevant to this alert, FinCEN requests that the filer select ***Box 1b*** ("suspicious transaction") and include the key term "**FIN-2022-RUSSIABIS**" in the "**Comments**" section of the report.

Additional Reporting Options for Suspected Export Control Evasion

In addition to filing a SAR, financial institutions may wish to consider reporting suspected export control evasion activity directly to BIS through its web-based confidential Enforcement Lead/Tip form, located at the following webpage:

https://bis.doc.gov/index.php/component/rsform/form/14-reporting-violations-form?task=forms.edit.

Alternatively, suspected violations may be reported via email to EELEAD@bis.doc.gov or to the BIS Enforcement Hotline: 800-424-2980.

For Further Information

Questions or comments regarding the contents of this alert should be sent to the FinCEN Regulatory Support Section at frc@fincen.gov.

41. Report for banks, as defined in 31 CFR § 1010.100(d), to exempt certain customers from currency transaction reporting in accordance with 31 CFR § 1010.311. *See* 31 CFR § 1020.315.
42. For filing instructions related to Form 8300, *see* FinCEN/IRS Form 8300 Filing Instructions (Rev. 9-2014).