FinCEN & BIS Joint Alert

FIN-2023-Alert004 **May 19, 2023**

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

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 U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) and the U.S. Department of Commerce's Bureau of Industry and Security (BIS)[1] previously issued a joint alert[2] (2022 Alert) urging financial institutions[3] to be vigilant against efforts by individuals and entities to evade BIS export controls implemented in connection with the Russian Federation's (Russia) further invasion of Ukraine. This supplemental joint alert provides financial institutions additional information regarding new BIS export control restrictions related to Russia, as well as reinforces ongoing U.S. Government engagements and initiatives designed to further constrain and prevent Russia from accessing needed technology and goods to supply and replenish its military and defense industrial base.[4] This alert further details evasion typologies, highlights for financial institutions nine high priority

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. *See* FinCEN, "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" (2022 Alert) (June 28, 2022). For other FinCEN alerts related to Russia's invasion of Ukraine, *see* "FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts" (Mar. 7, 2022); "FinCEN Alert on Real Estate, Luxury Goods, and Other High-Value Assets Involving Russian Elites, Oligarchs, and their Family Members" (Mar. 16, 2022); and "FinCEN Alert on Potential U.S. Commercial Real Estate Investments by Sanctioned Russian Elites, Oligarchs, and Their Proxies" (Jan. 25, 2023). For further reference, *see also* FinCEN "Advisory on Kleptocracy and Foreign Public Corruption" (Apr. 14, 2022), which includes a discussion of Russian political corruption.
3. *See* 31 U.S.C. § 5312(a)(2); 31 C.F.R. § 1010.100(t).
4. *See* U.S. Department of the Treasury (Treasury) Press Releases, "Remarks by Assistant Secretary for Terrorist Financing and Financial Crimes Elizabeth Rosenberg at Program on International Financial Systems (PIFS) U.S. – Europe Symposium in Frankfurt, Germany" (May 11, 2023); "READOUT: Under Secretary Nelson's Travel to Europe" (Apr. 23, 2023); "Remarks by Under Secretary Brian Nelson at American Chamber of Commerce Austria Roundtable" (Treasury Under Secretary Nelson Remarks) (Apr. 21, 2023); "JOINT READ OUT: US-EU-UK Sanctions Evasion Meeting with Private Sector Participants" (Apr. 13, 2023); and "READOUT: G7 Enforcement Coordination Mechanism Deputies Meeting" (Apr. 27, 2023); and White House Press Release, "G7 Leaders' Statement" (Feb. 24, 2023). *See also* BIS Press Release, "Remarks as Prepared for Delivery by Assistant Secretary for Export Enforcement Matthew S. Axelrod to the 12th Annual Forum on U.S. Export & Re-export Compliance for Canadian Operations" (Jan. 31, 2023).

Harmonized System (HS) codes[5] to inform their customer due diligence, and identifies additional transactional and behavioral red flags to assist financial institutions in identifying suspicious transactions relating to possible export control evasion. Finally, this alert requests that financial institutions continue to use the existing SAR code (FIN-2022-RUSSIABIS) when submitting SARs specific to Russian export control evasion and reminds them of their Bank Secrecy Act (BSA) reporting obligations.

Impact of U.S. Sanctions and Export Controls Against Russia

The United States, along with the Global Export Control Coalition (GECC)[6], an international coalition of 39 nations from North America, Europe, and the Indo-Pacific region, has imposed sweeping sanctions, export controls, and other economic restrictions since the start of Russia's unprovoked war against Ukraine in 2022. As a result, Russia's military-industrial complex and defense supply chains have been significantly degraded by sanctions and export controls over the past year.[7] According to U.S. Government assessments, Russia has lost over 10,000 pieces of equipment on the battlefield and is struggling to replace them. This has resulted in Russia tasking its intelligence services with finding ways to circumvent sanctions and export controls to replace needed equipment.[8]

The U.S. Government has also brought several enforcement cases against entities and individuals who violated U.S. export controls against Russia.[9] Many of these actions were brought as part of Task Force KleptoCapture, an interagency law enforcement task force dedicated to enforcing the

5. HS Codes are used globally to classify goods for export and are used by customs authorities when assessing duties and gathering statistics. The HS is administrated by the World Customs Organization and is updated every five years. It serves as the foundation for the import and export classification systems used in the United States and by many trading partners. The HS assigns specific six-digit codes for varying classifications and commodities. Countries are allowed to add longer codes to the first six digits for further classification. The United States uses a 10-digit code to classify products for export, known as a Schedule B number, with the first six digits being the HS number. There is a Schedule B number for every physical product. The Schedule B is administered by the U.S. Census Bureau's Foreign Trade Division. For more information, *see* International Trade Administration, U.S. Department of Commerce (Commerce), Harmonized System (HS) Codes.
6. The GECC includes Iceland, Liechtenstein, Norway, Switzerland, Australia, Canada, the 27 member states of the European Union (EU), Japan, the Republic of Korea, Taiwan, New Zealand, the United States, and the United Kingdom (UK). For more information *see generally*, Commerce Press Release, "Commerce Announces Addition of Iceland, Liechtenstein, Norway, and Switzerland to Global Export Controls Coalition" (Apr. 8, 2022).
7. *See* Treasury Press Release, "FACT SHEET: Disrupting and Degrading – One Year of U.S. Sanctions on Russia and Its Enablers" (Feb. 24, 2023). *See also* Department of Justice (DOJ) Press Release, "FACT SHEET: Justice Department Efforts in Response to Russia's February 2022 Invasion of Ukraine" (Feb. 24, 2023) and U.S. Department of State Press Release, "The Impact of Sanctions and Export Controls on the Russian Federation" (Oct. 20, 2022). *See also* BIS Press Release, "Remarks by Assistant Secretary Thea D. Rozman Kendler to the Association of Women in International Trade (WIIT)" (Mar. 2, 2023).
8. Treasury Under Secretary Nelson Remarks, *supra* note 4.
9. *See* DOJ Press Release, "Federal Court Orders Forfeiture of $826K in Funds Used in Attempt to Export Dual-Use High Precision Jig Grinder to Russia" (Apr. 5, 2023); BIS Press Release, "Microsoft to Pay Over $3.3M in Total Combined Civil Penalties to BIS and OFAC to Resolve Alleged and Apparent Violations of U.S. Export Controls and Sanctions" (Apr. 6, 2023); U.S Attorney's Office, Eastern District of New York Press Release, "United States Obtains Warrant for Seizure of Airplane Owned by Russian Oil Company Valued at Over $25 Million" (Mar. 8, 2023); BIS Press Releases, "BIS Takes Action Against Russian National and Related Company for Sending Controlled Counterintelligence Items to Russia and North Korea" (Feb. 24, 2023), and "Commerce Cuts Off Russia Procurement Network Evading Export Controls" (December 2022 BIS Enforcement Action) (Dec. 13, 2022).

sanctions and export controls and economic countermeasures that the United States has imposed, along with allies and partners, in response to Russia's unprovoked military invasion of Ukraine.[10]

In addition to Task Force KleptoCapture, on February 16, 2023, DOJ and Commerce announced the creation of the Disruptive Technology Strike Force, led by DOJ's National Security Division and BIS. The strike force brings together experts throughout government, including DOJ's National Security Division, the Federal Bureau of Investigation (FBI); the U.S. Department of Homeland Security, U.S. Immigration and Custom Enforcement's Homeland Security Investigations; and 14 U.S. Attorney's Offices in 12 metropolitan regions, to target illicit actors, strengthen supply chains and protect critical technological assets from being acquired or used by nation-state adversaries.[11] For example, on May 16, 2023, DOJ and Commerce announced the first five strike force enforcement actions.[12] One of those actions involved the arrest of a Greek national on May 9, 2023 involved in a procurement scheme to supply U.S.-origin military and dual-use technologies to Russia. The highly regulated and sensitive components included advanced electronics and sophisticated testing equipment used in military applications, including quantum cryptography and nuclear weapons testing, as well as tactical battlefield equipment. As described in the complaint, some of the Russian end users included nuclear and quantum research facilities, as well as the Russian Foreign Intelligence Service.[13]

Case Study: Two U.S. Citizens Arrested for Illegally Exporting Technology to Russia[14]

On March 2, 2023, two Kansas men were arrested on charges related to a years-long scheme to circumvent U.S. export controls that included the illegal export of aviation-related technology to Russia after Russia's unprovoked invasion of Ukraine on February 24, 2022 and the imposition of stricter restrictions on exports to Russia.

According to the indictment, the two men owned and operated KanRus Trading Company, which supplied Western avionics equipment (i.e., electronics installed in aircraft) to Russian companies and provided repair services for equipment used in Russian-manufactured aircraft. Since 2020, the defendants conspired to evade U.S. export controls by concealing and misstating the true end users, value, and end destinations of their exports and by transshipping items

10. *See* DOJ Press Release, "Attorney General Merrick B. Garland Announces Launch of Task Force KleptoCapture" (March 2, 2022); *see also* FinCEN Alert, "FinCEN Alert on Real Estate, Luxury Goods, and Other High-Value Assets Involving Russian Elites, Oligarchs, and their Family Members" (Mar. 16, 2022) at p. 7.
11. *See* DOJ-Commerce Joint Press Release, "Justice and Commerce Announce Creation of Disruptive Technology Strike Force" (Feb. 16, 2023).
12. *See* DOJ-Commerce Joint Press Conference, "Justice Department Announces Five Cases as Part of Recently Launched Disruptive Technology Strike Force" (May 16, 2023); *see also* DOJ Press Releases, "Assistant Attorney General for National Security Matthew G. Olsen Delivers Remarks Announcing Disruptive Technology Strike Force Cases" (May 16, 2023); and BIS Press Release, "BIS Takes Action Against Companies and Individuals for Attempting to Divert Electronics and Aircraft Parts to Russia" (May 16, 2023).
13. S*ee* DOJ Press Release, "Justice Department Announces Five Cases as Part of Recently Launched Disruptive Technology Strike Force" (May 16, 2023).
14. *See* DOJ Press Release, "Two U.S. Citizen Arrested for Illegally Exporting Technology to Russia" (Mar. 2, 2023).

through third-party countries. For example, between November 2020 and February 2021, the defendants received avionics equipment, including a computer processor bearing a sticker identifying Russia's Federal Security Service (FSB), from a Russian company for repair in the United States. The defendants concealed the true end user and end destination by providing a fraudulent invoice to the shipment company identifying the end destination as Germany.

As further alleged, on Feb. 28, 2022, the defendants attempted to export avionics to Russia. U.S. authorities detained the shipment, and the U.S. Department of Commerce informed the defendants that a license was required to export the equipment to Russia. In an April 2022 communication, one of the defendants expressed to a Russia-based customer that "things are complicated in the USA" and that "[t]his is NOT the right time for [more paperwork and visibility]." Subsequently, in May, June and July 2022, the defendants illegally transshipped avionics through Armenia and Cyprus to Russia without obtaining the required licenses.

New Export Control Restrictions Implemented Since Publication of the June 2022 Alert

Since the publication of the 2022 Alert, BIS has imposed additional export control restrictions to further cut off Russia's defense industrial base and military from critical items it seeks to obtain to sustain Russia's ongoing, unprovoked war against Ukraine.[15] Specifically, these restrictions, developed in concert with international allies and partners, aim to cut off Russia's access to critical components used for aircraft and tanks, semiconductors, other items needed for advanced military applications, and low-technology consumer goods needed for Russia to sustain its war effort.[16]

BIS implemented these additional restrictions, which also target third countries such as Iran and China, that have served as supply nodes to the Russian war machine, on the one-year anniversary of Russia's invasion. BIS continues to build and sustain the GECC, whose members impose substantially similar export controls on Russia, targeting third countries and impeding Russia's ability globally to obtain commercially available items, such as semiconductors.[17]

These new restrictions, comprised of four rules, revise the Export Administration Regulations (EAR)[18] to enhance the existing controls and add hundreds of low-level items to the United States' Russia export controls; bring the United States into further alignment with foreign partners; impose controls on specific items going to Iran, including semiconductors, that are components for Iranian Unmanned

15. For further information and resources related to BIS' first series of export control restrictions implemented in response to Russia's invasion of Ukraine in February 2022, *see* 2022 Alert, *supra* note 2.
16. *See* BIS Press Release, "Commerce Imposes Additional Export Restrictions in Response to Russia's Brutal War on Ukraine" (Feb. 24, 2023).
17. *Id.*
18. The EAR control certain exports, reexports, transfers (in-country) and other activities. For more information, *see* 15 C.F.R. §§ 730–774.

Aerial Vehicles (UAVs) used by Russia in Ukraine; and add a number of entities to the BIS Entity List.[19] In addition, on April 12, 2023, and May 19, 2023, BIS added 30 entities under 34 entries to the Entity List as part of a wider third-country crackdown on Russian evasion.[20] Each of the entities was found to be acting contrary to U.S. national security and foreign policy interests and in support of Russia's military or defense industrial base.

Use of Third-Party Intermediaries and Transshipment Points to Evade Controls

In addition, on March 2, 2023, DOJ, Commerce, and Treasury issued a joint compliance note on Russia-related sanctions and export control evasion to highlight to private industry a common tactic used by illicit actors to evade Russia-related sanctions and export controls: the use of third-party intermediaries and transshipment points.[21] The joint compliance note highlights the use of this tactic to disguise the involvement of persons on Treasury's Office of Foreign Assets Control (OFAC) List of Specially Designated Nationals and Blocked Persons (SDN List),[22] or parties on the BIS Entity List in transactions and to obscure the true identities of Russian end users.

Attempts to obfuscate the involvement of SDNs or parties on the BIS Entity List in transactions and obscure the true identities of Russian end users may involve the use of shell and front companies.[23] For example, a Russian entity with ties to the defense sector may establish a front company in another country as well as various affiliates of the front company in third countries. Procurement agents, operating covertly on behalf of the Russian Government, will orchestrate purchases of goods by the front company from various suppliers, who in turn receive payment from the front company's non-Russian bank account, which may transmit funds through a U.S. correspondent bank account to route funds back to the supplier. The front company will then route the goods to Russia, often through permissive jurisdictions such as known transshipment points.[24]

19. *Id.* The BIS Entity List, which is found in Supplement No. 4 to Part 744 of the EAR, 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. The persons on the Entity List are subject to licensing requirements and policies supplemental to those found elsewhere in the EAR.
20. The entities are located in Armenia, Kyrgyzstan, the People's Republic of China, Malta, Russia, Singapore, Spain, Syria, Turkey, the United Arab Emirates, and Uzbekistan.
21. *See* DOJ Press Release, "Departments of Justice, Commerce and Treasury Issue Joint Compliance Note on Russia-Related Sanctions Evasion and Export Controls" (Mar. 2, 2023). As noted in footnote 21 of the 2022 Alert, 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. 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.
22. *See* OFAC, "Specially Designated Nationals and Blocked Persons List (SDN) Human Readable Lists" (Last Updated May 16, 2023).
23. *See* December 2022 BIS Enforcement Action, *supra* note 9.
24. *See supra* note 21.

Such a procurement network may also involve additional layering to create complexity and further obfuscate the buyer and end user. For example, an SDN or Entity List party may create a shell company that legally owns a front company used by the SDN to procure defense or dual-use items from a supplier. Both the shell and front companies may have foreign bank accounts, which are used to transmit funds back to the supplier and which may also involve the transmittal of funds through a U.S. correspondent bank.

In other instances, an SDN or Entity List party may use a non-designated Russian supplier to procure goods through a subsidiary of an authorized reseller of defense and dual-use items. Some authorized reseller subsidiaries may be less likely to conduct as much customer due diligence as their parent entities. Another obfuscation tactic may involve procurement agents creating both shell companies with foreign bank accounts and transshipment companies that may order and receive dual-use goods from multiple, but similar, suppliers. As a result, the shell company's foreign bank account may send a smaller-volume of transactions to multiple firms, with the intent to attract less attention than would large-volume transactions.

High Priority Items List by Harmonized System Code[25]

In addition to the commodities of concern first highlighted in the 2022 Alert,[26] BIS, in partnership with the EU, the UK, and Japan, has identified nine HS codes covering critical U.S. components that Russia relies on for its weapons systems (the High Priority Items List). These HS codes are listed in Supplement No. 7 to Part 746 of the EAR, meaning a license is required for any items associated with these HS codes destined to Russia, Belarus, the Crimea region of Ukraine, or Iran, including certain foreign-produced items.[27]

This High Priority Items List is primarily based on the HS code classification of Russian weapons system components recovered on the battlefield in Ukraine. Items described by these HS codes have been found in multiple Russian weapons systems used against Ukraine, including the Kalibr cruise missile, the Kh-101 cruise missile, and the Orlan-10 UAV. Treasury and BIS assess that Russia is specifically using evasive methods to acquire these items. The High Priority Items List is not an exhaustive list of all items Russia is attempting to procure, but provides prioritized targets for customs and enforcement agencies around the world and has informed discussion in international engagements conducted by BIS and Treasury leadership as well EU and UK counterparts.[28]

25. *See supra* note 5.
26. *See* 2022 Alert, *supra* note 2 at p. 3.
27. *See* 15 C.F.R. Part 746, Supp. No. 7.
28. *See* Treasury Press Release, "READOUT: Senior Treasury and Commerce Department Officials Travel to Kazakhstan" (Apr. 27, 2023). *See also*, "Remarks by Assistant Secretary for Terrorist Financing and Financial Crimes Elizabeth Rosenberg at Media Engagement in Astana, Kazakhstan" (Apr. 27, 2023).

High Priority Items List

HS Code	HS Description and Representative Part
8542.31	Electronic integrated circuits: Processors and controllers, such as microcontrollers
8542.32	Electronic integrated circuits: Memories, such as SRAM
8542.33	Electronic integrated circuits: Amplifiers, such as op amps
8542.39	Electronic integrated circuits: Other, such as FPGAs
8517.62	Machines for the reception, conversion and transmission or regeneration of voice, images, or other data, such as wireless transceiver modules
8526.91	Radio navigational aid apparatus, such as GNSS modules
8532.21	Tantalum capacitors
8532.24	Multilayer ceramic capacitors
8548.00	Electrical parts of machinery or apparatus, not specified or included elsewhere, such as EMI filters

Applying a Risk-Based Approach to Trade Finance

As noted in the 2022 Alert, financial institutions, particularly banks, 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 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 includes 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.[29]

Financial institutions are also strongly encouraged to conduct due diligence when encountering one of the nine listed HS codes to identify possible third-party intermediaries and attempts at evasion of U.S. export controls. HS codes can be found on trade documents including commercial invoices, packing slips, airway bills, sea bills, or other supporting trade documentation.

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

In reviewing U.S. export data related to these nine HS codes, BIS has identified three fact patterns associated with importers in non-GECC countries that raised diversion concerns:

- The company never received exports prior to February 24, 2022;
- The company received exports that did not include any of the nine HS Codes prior to February 24, 2022; or
- The company received exports involving the nine HS Codes prior to February 24, 2022, but also saw a significant spike in exports thereafter.

Accordingly, FinCEN and BIS are requesting that financial institutions conduct due diligence. Specifically, when opening accounts for new customers engaged in trade, especially those located in non-GECC countries, such as the transshipment countries identified in the 2022 Alert,[30] financial institutions are urged to conduct due diligence, including:

- Evaluating the customer's date of incorporation (*e.g.*, incorporation after February 24, 2022),
- Evaluating the end user and end use of the item (*e.g.*, whether the customer's line of business is consistent with the ordered items), and
- Evaluating whether the customer's physical location and public-facing website raise any red flags (*e.g.*, business address is a residence, no website is available).

For existing customers, financial institutions should pay particular attention to anomalous increases in the volume or value of orders, including by requesting additional information about end-use and end-user, or inconsistencies between the items ordered and customer's line of business. These flags are included in the following section.

Select Red Flag Indicators of Export Control Evasion

FinCEN and BIS are providing an additional select list of potential red flag indicators of export control evasion, including flags derived from recent BSA reporting, that may be relevant to financial institutions and other covered institutions or persons.[31] These red flags should be read in conjunction with those set out in the 2022 Alert. Consideration of these indicators and those set out in the 2022 Alert, 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.[32] As no single red flag is necessarily indicative of illicit or suspicious activity, all the surroundng facts and circumstances should be considered before determining whether a specific transaction is suspicious or associated with potential export control evasion.

30. *See* 2022 Alert, *supra* note 2.
31. All of the red flag indicators highlighted in the 2022 Alert remain valid. BIS also 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.
32. 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 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.

New Transactional and Behavioral Red Flags:

1. Transactions related to payments for defense or dual-use products from a company incorporated after February 24, 2022, and based in a non-GECC country.
2. A new customer whose line of business is in trade of products associated with the nine HS codes, is based in a non-GECC country, and was incorporated after February 24, 2022.
3. An existing customer who did not receive exports associated with the nine HS codes prior to February 24, 2022, but who is receiving such items now.
4. An existing customer, based outside the United States, received exports associated with one or more of the nine HS codes prior to February 24, 2022, and requested or received a significant increase in exports with those same codes thereafter.
5. A customer lacks or refuses to provide details to banks, shippers, or third parties, including about end users, intended end-use, or company ownership.
6. Transactions involving smaller-volume payments from the same end user's foreign bank account to multiple, similar suppliers of dual-use products.
7. Parties to transactions listed as ultimate consignees or listed in the "consign to" field do not typically engage in business consistent with consuming or otherwise using commodities (e.g., other financial institutions, mail centers, or logistics companies).
8. The customer is significantly overpaying for a commodity based on known market prices.
9. The customer or its address is similar to one of the parties on a proscribed parties list, such as the BIS Entity List, the SDN List, or the U.S. Department of State's Statutorily Debarred Parties List.[33]

33. This list includes entities and individuals prohibited from participating directly or indirectly in the export of defense articles, including technical data and defense services. Pursuant to the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR), the AECA Debarred List includes persons convicted in court of violating or conspiring to violate the AECA and subject to "statutory debarment" or persons established to have violated the AECA in an administrative proceeding and subject to "administrative debarment. *See* U.S. Department of State, Directorate of Defense Trade Controls, Statutorily Debarred Parties List.

Reminder of Relevant BSA Obligations for U.S. Financial Institutions[34]

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.[35] All statutorily defined financial institutions may voluntarily report suspicious transactions under the existing suspicious activity reporting safe harbor.[36]

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.[37] 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.[38] 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

34. For additional relevant guidance, see *Reminder of Relevant BSA Obligations and Tools for U.S. Financial Institutions* from FinCEN's Mar. 16, 2022 Russia-related alert, *supra* note 2.
35. See 31 C.F.R. §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320. All financial institutions subject to 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.
36. *See* 31 U.S.C. § 5318(g)(3).
37. *See* 31 C.F.R. §§ 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).
38. *Id; see also* FinCEN, "Suspicious Activity Report Supporting Documentation" (June 13, 2007).

American Industry Code(s) (NAICs) for the involved product, or the appropriate financial instrument or payment mechanism in field 46..

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).[39]

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.[40]

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.[41] These include obligations related to the Currency Transaction Report (CTR),[42] Report of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300),[43] Report of Foreign Bank and Financial Accounts (FBAR),[44] Report of International Transportation of Currency or Monetary Instruments

39. 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.
40. *See* 31 C.F.R. §§ 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).
41. 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).
42. 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 C.F.R. §§ 1010.310-313, 1020.310-313, 1021.310-313, 1022.310-313, 1023.310-313, 1024.310-313, 1026.310-313.
43. 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 C.F.R. §§ 1010.330, 1010.331 (Clerks of the Court).
44. 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 C.F.R. § 1010.350 and FinCEN Form 114.

(CMIR),[45] Registration of Money Services Business (RMSB),[46] and Designation of Exempt Person (DOEP).[47] 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.[48] 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.

45. Each person (i.e., an individual or legal entity), as defined in 31 C.F.R. § 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 C.F.R. § 1010.340.
46. Report for a business required to register with FinCEN as a money services business, as defined in 31 C.F.R. § 1010.100(ff) or renewing the registration. 31 C.F.R. § 1022.380.
47. Report for banks, as defined in 31 C.F.R. § 1010.100(d), to exempt certain customers from currency transaction reporting in accordance with 31 C.F.R. § 1010.311. *See* 31 C.F.R. § 1020.315.
48. For filing instructions related to Form 8300, *see* FinCEN/IRS Form 8300 Filing Instructions (Rev. 9-2014).