Guidance to Prevent Evasion of Prioritized Harmonized System Codes to Russia

On May 19, 2023, 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] issued a new joint alert providing additional information regarding new BIS export control restrictions related to Russia, as well as reinforcing 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.[2]

As a supplement to this alert, BIS is issuing this guidance for exporters and reexporters that provides further details on evasion typologies, highlights nine high priority Harmonized System (HS) codes[3] to inform their customer due diligence, and identifies additional transactional and behavioral red flags to assist exporters and reexporters in identifying suspicious transactions relating to possible export control evasion.

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

The United States, along with the Global Export Control Coalition (GECC)[4], 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

---

[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 https://www.fincen.gov/news/news-releases/supplemental-alert-fincen-and-us-department-commerces-bureau-industry-and. 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. 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), or parties on the BIS Entity List in transactions and to obscure the true identities of Russian end users. https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3241-tri-seal-final-clean/file

[3] 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, s*ee* International Trade Administration, U.S. Department of Commerce, Harmonized System (HS) Codes.

[4] 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).

controls over the past year.[5] 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.

The U.S. Government has also brought several enforcement cases against entities and individuals who violated U.S. export controls against Russia.[6] Many of these actions were brought as part of Task Force KleptoCapture, an interagency law enforcement task force dedicated to enforcing the 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.[7]

In addition to Task Force KleptoCapture, on February 16, 2023, the Departments of Justice (DOJ) and Commerce (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.[8] For example, on May 16, 2023, DOJ and Commerce announced the first five strike force enforcement actions.[9] One of those actions involved the arrest on May 9 of a Greek national 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

---

[5] *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* 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).

[6] *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" (April 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 Release, "BIS Takes Action Against Russian National and Related Company for Sending Controlled Counterintelligence Items to Russia and North Korea," (Feb. 24, 2023); and BIS Press Release, "Commerce Cuts Off Russia Procurement Network Evading Export Controls" (December 2022 BIS Enforcement Action) (Dec. 13, 2022).

[7] *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.

[8] *See* DOJ-Commerce Joint Press Release, "Justice and Commerce Announce Creation of Disruptive Technology Strike Force" (Feb. 16, 2023).

[9] *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).

users included nuclear and quantum research facilities, as well as the Russian Foreign Intelligence Service.[10]

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.[11] 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.[12]

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.[13]

These new restrictions, comprised of four rules, revise the Export Administration Regulations (EAR)[14] 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 Aerial Vehicles (UAVs) used by Russia in Ukraine; and add a number of entities to the BIS Entity List.[15] 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.[16] 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.

---

[10] *See* DOJ Press Release, "Justice Department Announces Five Cases as Part of Recently Launched Disruptive Technology Strike Force" (May 16, 2023).

[11] 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, s*ee* 2022 Alert, *supra* note 2.

[12] *See* BIS Press Release, "Commerce Imposes Additional Export Restrictions in Response to Russia's Brutal War on Ukraine" (Feb. 24, 2023).

[13] *Id*.

[14] The EAR control certain exports, reexports, transfers (in-country) and other activities. For more information, *see* 15 C.F.R. §§ 730–774.

[15] *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.

[16] 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.

High Priority Items List by Harmonized System Code[17]

In addition to the commodities of concern first highlighted in the June 2022 alert,[18] 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.[19]

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.[20]

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

[17] See *supra* note 3.
[18] *See* 2022 Alert, *supra* note 2 at p. 3.
[19] *See* 15 C.F.R. Part 746, Supp. No. 7.
[20] *See* Treasury Press Release, "READOUT: Senior Treasury and Commerce Department Officials Travel to Kazakhstan" (Apr. 27, 2023).

Applying a Risk-Based Approach to Exporting

Exporters and reexporters are 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.

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, BIS is requesting that exporters and reexporters 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,[21] exporters and reexporters 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, exporters and reexporters should pay particular attention to anomalous increases in the volume or value of orders, including by requesting additional information about the end-use and end-user, or inconsistencies between the items ordered and the customer's line of business. These flags are included in the following section.

Select Red Flag Indicators of Export Control Evasion

BIS is providing an additional select list of potential red flag indicators of export control evasion, including flags derived from recent Bank Secrecy Act reporting, that may be relevant to exporters and reexporters.[22] 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

[21] *See* 2022 Alert, *supra* note 2.

[22] 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.

evasion. As no single 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.

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, is exporting such items now to known transshipment points.[23]
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.[24]

*****

CASE STUDY

Two U.S. Citizens Arrested for Illegally Exporting Technology to Russia[25]

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

---

[23] *See supra* note 22.

[24] This list include 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.

[25] *See* DOJ Press Release, "Two U.S. Citizen Arrested for Illegally Exporting Technology to Russia" (Mar. 2, 2023).

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 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.