Preventing Russian Export Control and Sanctions Evasion: Updated Guidance for Industry

Since 24 February 2022, Canada, France, Germany, Italy, Japan, the United Kingdom, the United States, and the European Union (collectively referred to as the "Group of 7" or "G7") have implemented unprecedented export controls and sanctions that restrict Russia's access to technologies and other materials required to sustain its military operations and illegal war campaign in Ukraine. The G7 has also coordinated these regulations with the Global Export Control Coalition (GECC), a 39-member coalition that has implemented substantially similar controls in response to Russia's unprovoked and unjustified invasion of Ukraine.[1]

The work of the G7 has impacted Russia's ability to access goods and technologies used for weapons development purposes. The coordinated application of export controls and sanctions has limited Russia's access to key markets it relied on for access to and purchase of technologies. The actions of the G7 have also degraded Russia's economy and Moscow's ability to generate revenue that could be used to purchase Western technologies.

In February 2023, the G7 announced the creation of a new Enforcement Coordination Mechanism (ECM) to bolster compliance and enforcement of multilateral export controls and sanctions and to deny Russia the benefits of G7 economies. In September 2023, the ECM established a Sub-Working Group on Export Control Enforcement, through which G7 representatives would exchange information and operational results, discuss trends in research and analysis, and share best practices.

As part of our coordinated efforts, a core principle of the G7 Sub-Working Group on Export Control Enforcement is to provide guidance to industry on preventing the diversion of controlled items to Russia, including through third countries. Our collective aim is to assist industry in identifying Russian evasion practices and complying with GECC controls, thereby protecting their technology from misappropriation, preventing reputational harm, and mitigating liability risk while supporting the continued success of our export controls and sanctions.

This guidance document contains:

1. A list of items which pose a heightened risk of being diverted to Russia,
2. Updated red flag indicators of potential export control and/or sanctions evasion,
3. Best practices for industry to address these red flags, and
4. Screening tools and resources to assist with due diligence.

[1] The GECC includes Australia, Canada, the 27 Member States of the European Union, Iceland, Japan, Liechtenstein, New Zealand, Norway, the Republic of Korea, Switzerland, Taiwan, the United Kingdom, and the United States.

Actions by Russia to Evade Export Controls and Sanctions

Russia has demonstrated that it relies on deceptive tactics capable of evading established export controls and sanctions enforcement. Russian proliferators operate as transshipment agents and divert dual use technologies and controlled goods from third countries to Russia.

Therefore, it is critical that all parties of the supply chain (e.g., exporters, re-exporters, manufacturers, distributors, resellers, and service providers such as financial institutions, logistics companies, transportation providers, freight forwarders, warehouse operators, and customs brokers) are aware of the diversion risks posed by Russia's illicit procurement efforts and adopt appropriate measures to mitigate any risks.

The Russian Government has taken the following actions to support these procurement efforts:

- On 25 April 2023, Russia issued Decree No. 302, authorizing the Federal Agency for the Administration of Public Property (Rosimuschestvo) to seize and manage Russian assets owned or managed by foreign legal or natural persons from "unfriendly states". These assets can include shares in Russian companies, property rights, or securities.
- On 1 May 2022, Russia signed Decree No. 250, which requires certain organizations, including GECC companies operating in the critical information infrastructure sector in Russia, to provide the Russian Federal Security Service (FSB) with unhindered access (including remote access) to their information resources for monitoring purposes. The decree could allow unauthorized access to proprietary information, including encryption software, which may be subject to export controls.
- On 29 March 2022, Russia passed Resolution Nos. 506 and 1532, which legalized "parallel imports". This allows Russian parties to maintain access to foreign intellectual property without the consent of the original trademark holders, thereby facilitating the theft of GECC technology in contravention of export controls and sanctions.
- On 5 March 2022 and 4 May 2022, respectively, Russia issued Decree Nos. 95 and 254, which restrict transfers of dividends to foreign bank accounts by persons from "unfriendly states". Payments may only be made in Russian rubles to a special type "C" account at a Russian bank. These restrictions are in place until at least 30 September 2024, pending an additional extension.
- On 8 September 2022, Russia signed Decree No. 618, which requires persons connected to "unfriendly states" to obtain approval from the Government Commission on Control over Foreign Investments for any direct or indirect transaction with participatory interests in, or resulting in obtaining management rights over, Russian limited liability companies.
- In 2014, Russia added "Information on the Russian export or import of dual-purpose products subject to export control, a premature dissemination of which may compromise national security" to the list of information regarded as a state secret. The list was first issued under Decree No. 1203 on 30 November 1995. This imposition on information sharing has since limited countries' ability to implement the compliance efforts necessary to support export control regulations.

1) The Common High Priority List (CHPL)

The European Union, Japan, the United Kingdom, and the United States developed the CHPL to highlight for industry that these items pose a heightened risk of illicit diversion to Russia because of their importance to Russia's war efforts. These items have been retrieved from Russian weapons found on the battlefield or have been identified as essential items for Russia to manufacture its own military equipment.

The CHPL shall aid industry in conducting necessary due diligence. As of this document's publication, the CHPL includes 50 tariff lines that Russia seeks to procure for its war effort. The 50 tariff lines are identified by six-digit Harmonized System (HS) Codes, a standardized numerical method of classifying goods, known to every exporter, shipper, and freight forwarder around the world. The CHPL may be found here. A link is also available under "Additional Resources".

TIER 1	Integrated circuits (also referred to as microelectronics). These items have a critical role in production of advanced Russian precision-guided weapons systems, due to lack of domestic production and limited global manufacturers.
TIER 2	Additional electronics (e.g., related to wireless communications) items for which Russia may have some domestic production capability but prefers to use technology originating from G7 or GECC partners in its military equipment.
TIER 3.A	Further electronic components used in Russian weapons systems, with a broader range of suppliers.
TIER 3.B	Mechanical and other components utilized in Russian weapons systems.
TIER 4.A	Manufacturing, production, and quality testing equipment for electric components, circuit boards, and modules.
TIER 4.B	Computer Numerically Controlled (CNC) machine tools and components. Russia's military industrial complex relies heavily on technology originating from G7 or GECC countries to manufacture advanced weaponry.

2) Red Flag Indicators

The G7 has identified the following **red flags indicators of potential export control and sanctions evasion**.

We encourage industry to use these red flag indicators to conduct necessary due diligence prior to export and to be alert for other possible indicators not listed below.

Sudden changes in business activity after 24 February 2022, or after subsequent changes in export controls/sanctions, *including but not limited to:*	• New importers or exporters of Common High Priority List (CHPL) items, especially parties located at the same address as a sanctioned entity. • An existing importer of CHPL items has a significant increase in import value and/or volume. • An existing exporter/re-exporter of CHPL items shipped primarily to Russia prior to 24 February 2022 and began shipping to new parties in a third country or third countries after 24 February 2022.
False, inaccurate, or missing documentation, *including:*	• False declarations of export authorization. • Misclassification of goods, to include use of a non-CHPL HS code to conceal CHPL item(s). • Undervaluation of goods. • Using one HS code when exporting an item and a different HS code when the item arrives in a third country. • Documents claim civil end use for items destined for companies traditionally known to be, or known be associated with, military entities.

Concealing the end user, *for example by:*	• Circumventing shipments through a third country or multiple third countries, which may include the use of:
	  ○ Shell companies, front companies, intermediaries, brokers, and/or layered letters of credit.
	  ○ Multiple third-country freight forwarders and/or shippers.
	• Listing a freight forwarder or an operator of charter aircraft as the end user.
	• Using an unclear transportation route for an exported item.
	• Transporting an item through Russia to an end user in a third country.
	• Circuitous routing of goods or financial flows.
	• Changing an item's shipping instructions when the item arrives at a freight forwarder, without the knowledge of the exporter.

Inconsistencies in the transaction, *including but not limited to:*	• Shipping route is abnormal for product and/or destination. • The volume and value of goods do not match the volume of payments. • Transaction includes unusually high quantities of goods. • Inconsistent information in trade documents and financial flows, such as names, companies, addresses, and/or final destination.

Vague details and/or incomplete information, *such as:*

- Customer provides incomplete information, especially regarding the end user and/or end use.
- Customer or vendor is resistant to providing additional information, including end use assurances, when sought.

Dividing an invoice value into smaller amounts to remain under value limits of sanctioned goods or export controls.

- Often used for luxury goods.
- Items may arrive in small, frequent shipments to a central location, such as a warehouse in a third country, where they are combined into one shipment.

Suspicious customer information, *such as:*

- Addresses do not appear consistent with the business, e.g., a business address is a residence.
- Goods ordered do not match the customer's industry.
- Customer has little to no internet presence. Customer's company website does not function and/or contains limited information.
- Customer's website has changed since 2022 to eliminate links to Russia but customer has not attested that they no longer export to Russia.
- IP address does not match customer's reported location. For example, a company in a third country may host websites from a Russian IP address.
- Personnel, address, or telephone number match or are suspiciously similar to information found on sanctions lists or watchlists.

Customer has connections of concern, *for example:*

- Customer has business ties to Russia, such as:
  - A branch, subsidiary, or parent company in Russia.
  - One or more Russian or Belarussian shareholders.
  - Customer does business with a Russian company.
  - Customer is associated with people or entities related to the Russian defense sector.
- Customer is co-located at the same address as an entity designated or sanctioned by a G7 member state.
- New customer is co-located with and has a mutual shareholder and/or secretarial firm as an entity designated or sanctioned by a G7 member state.
- Customer has previously had dealings or maintains relationships with individuals or entities now subject to sanctions.
- Customer is associated with companies that are suspected or known to be selling sanctioned goods and/or technology to Russia.

Concerning business practices, *such as:*

- Customer is involved in the supply, sale, purchase, or delivery of restricted or high-risk goods, particularly CHPL items.
- Customer exports once and disappears from trade.

Last-minute changes to parties involved with the transaction from an entity in Russia or Belarus to an entity in another country.

Payments from entities located in third countries that are not otherwise involved with the transactions, particularly through a sanctioned country.

Customer unwilling to provide certification that it will not sell items to Russia or sanctioned parties in third countries.

3) Best Practices

When you encounter these or any other red flag indicators, you should conduct additional risk-based customer and transactional due diligence to possibly clear these red flags and thus mitigate attempts to evade the GECC's respective export controls and/or sanctions. As no single red flag is 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 and/or sanctions evasion. There is no "one-size-fits-all" approach.

The G7 calls on responsible traders to improve export compliance systems and exercise enhanced due diligence. Specifically, **we strongly encourage you to follow these steps upon encountering these or any other red flag indicators**:

Run transaction parties against applicable public sanctions lists (see "Additional Resources" for a compendium of G7 websites to search against). This includes separately running both the name and address against such lists. If relevant, run transaction parties against information collected by nonprofit organizations identifying companies that present a high risk of future diversion.

- Where a "hit" against an address but not a company name occurs, additional due diligence as noted below is recommended.
- An address which matches one or more public sanctions lists may indicate the use of shell companies or trust and company service providers (commonly referred to as company secretaries).

Conduct additional due diligence. You may wish to:

- Inquire further regarding the end use, end user, and/or ultimate country of destination for the items.
- Request more information from the customer regarding their history, business practices, etc.
- Conduct open-source research on the customer, including leveraging public business registries and commercially available trade databases.
- Request that customers sign written certification that items will not be transferred to parties in Russia or Belarus or sanctioned parties in third countries.
- Update distributor agreements to require distributors implement heightened due diligence measures as noted in this guidance document.

Analyze the risk of export control and/or sanctions circumvention. Reevaluate the red flag indicators and all available information after conducting further due diligence.

- Can you explain or justify the red flags?
- Can you establish bona fides of the party?
- Can you confirm the legitimacy of the transaction?

If you continue to have reason for concern after your inquiry, you should:

- Refrain from the transaction
- Disclose information to the appropriate export control/compliance/customs agency in your country.

4) Additional Resources

Screening Tools:

Consolidated Canadian Autonomous Sanctions List

European Union (EU) Consolidated List of Financial Sanctions

United Kingdom Sanctions List

United States Consolidated Screening List

Guidance Documents:

Canada:

- Restricted Goods and Technologies List
- Special Economic Measures (Russia) Regulations

European Commission:

- List of Common High Priority List Items
- European Commission Guidance for EU Operators
- Sanctions webpages (Opinions, FAQs)

Export Enforcement Five (E5):

- Guidance for Industry and Academia

Germany:

- "Sanktionsumgehung –Hinweispapier zur Unterstützung der Unternehmen beim Umgang mit warenverkehrsbezogenen Sanktionen"
- "Sanktionsumgehung – Hinweis: Kriegsrelevante Güter gelangen vermehrt von ausländischen Tochtergesellschaften von EU-Unternehmen nach Russland"

Japan:

- Guidelines, Explanatory Materials, Related Regulations (Japanese)
- Regulated Items, Sanctioned Entities, Application Forms, FAQs (Japanese)

United Kingdom:

- Notice 2023/08: Russia Sanctions – Trade Sanctions Circumvention
- National Economic Crime Centre: Red Alert – Exporting High Risk Goods

United States:

- Best Practice: Certification to Prevent Diversion to Russia of Highest Priority Items
- Guidance to Prevent Evasion of Prioritized Harmonized System Codes to Russia
- Bureau of Industry and Security: Russia-Belarus Export Controls Resources