Preventing Illicit Transactions Related to Russian Advanced Conventional Weapon (ACW) Systems: An Operational Manual

2023

Preventing Illicit Transactions Related to Russian Advanced Conventional Weapon (ACW) Systems: An Operational Manual

Authors:
Bethany Banks and Akaki Saghirashvili

Contributors:
Giorgi Goguadze, Tamar Nadibaidze, Nikoloz Kipshidze

ABOUT THIS MANUAL

This manual was composed with the generous support of the U.S. Department of State, Office of Cooperative Threat Reduction.

The authors would like to thank ProCredit, Liberty Bank, PASHA Bank Georgia, GeorgienSpedition, Easy Charter, and Santa Trans Ltd for their engagement on best practices among Georgian firms. The authors would also like to thank Dr. Iryna Bogdanova and Dr. Daniel Salisbury for their insights.

ABOUT THE AUTHORS

Bethany Banks is a consultant and subject-matter expert in conventional weapons, trafficking and proliferation, and sanctions. She has over 10 years of experience working for the U.S. Department of State, where she advised on critical defense and political-military policy issues and led multilateral engagements on advanced conventional weapons threats. She also has a background in business development and international affairs. She holds a Master of Arts in Russian, East European, and Eurasian Studies from the University of Kansas and a Bachelor of Arts in International Affairs from the George Washington University.

Akaki Saghirashvili is a lawyer with over 15 years of professional experience. As former Deputy Minister of Justice and of Economy and Sustainable Development of Georgia, he has acquired first-hand experience in projects related to mergers, acquisitions, and large scale infrastructure projects within the Public Private Partnership framework. He has a deep understanding of and experience with public policies and regulatory frameworks, as well as procurement using international donor guidelines. Akaki is a former Deputy Minister of Economy, subject-matter expert with vast knowledge of the Georgian private sector as well as the logistics and energy networks operating in the country.

TABLE OF CONTENTS

OVERVIEW

Over the course of the last decade, sanctions are increasingly used by a range of countries and international organizations to target security threats, including non-state groups and state actors. Non-compliance with sanctions regimes is among the most significant risks many private sector entities currently face. This is particularly true of financial institutions, defense firms, transportation firms, and technology/electronics firms. While sanctions have long targeted transactions related to weapons of mass destruction (WMD) development (for example, those focused on North Korea and Iran) and terrorist organizations, the recent imposition of sanctions on Russia in response to its recent invasion of Ukraine (2022) has significantly expanded the use of this tool to target a state's ACW (advanced conventional weapons) program, restricting both its ability to acquire the relevant production materials and opportunity to export or sell conventional weapons.

In the wake of these developments, compliance with the ACW-related sanctions regimes has assumed paramount importance for private sector entities, particularly in Russia's neighboring states and other countries with major business relationships with Russia. A firm's ability to quickly and accurately identify illicit transactions and take appropriate steps to address the respective risks is critical to ensuring unhindered operation and avoiding grave consequences. Considering the significant effects of noncompliance – e. g., frozen assets, restricted or banned export, seized property, and denied visa travel – the private sector and financial institutions need to be vigilant in their compliance with these regimes. The targets of the sanctions are expansive and include not only financial institutions and direct recipients, but also professional service providers, including any other third parties acting as intermediaries between the sanctioned financial institution and its clients. Beyond business risks, ethical and reputational issues also merit consideration: evasion of sanctions will bear serious, real-world consequences – in this particular case, deliberate or inadvertent evasion of sanctions against Russia or any kind of engagement therein will have real and immediate consequences on Russia's ability to wage war in Georgia's neighborhood.

This manual will be focused on providing operational awareness of specific ACW components and systems as well as sanctions regimes, including the Countering America's Adversaries Through Sanctions Act (CAATSA) and others developed by the international community (including the EU, the UK, Australia, and Japan) to restrict Russia's access to the components and transactions required for ACW manufacture and distribution. For the purpose of this project, ACW systems will include Man-Portable Air Defense Systems (MANPADS) and Anti-Tank Guided Missiles (ATGMs); major weapons systems and heavy military equipment such as tanks, aircraft, and missiles; sensors and lasers; and precision-guided munitions.

UNDERSTANDING SANCTIONS AND ACW

Current Sanctions and Related Obligations

There are a number of bilateral and multilateral sanctions and export control regimes in effect today that impose obligations on private sector firms. Some, such as the Wassenaar Arrangement, are political agreements with little to no enforcement mechanisms, while others have significant and expansive enforcement mechanisms. Many prior weapons-related sanctions regimes have focused exclusively on WMD production materials. This includes the robust UN sanctions targeting North Korea's and, until recently, Iran's proliferation financing. Russia's annexation of Crimea in 2014, followed by its further invasion of Ukraine in 2022, dramatically altered the sanctions landscape, especially by imposing severe sanctions targeting individuals and entities engaged in ACW-related transactions.

The **United States** was the first to adopt sanctions against Russia after Russia's 2014 invasion of Crimea. These sanctions, implemented by the Office of Foreign Assets Control (OFAC), apply to specific sectors, prohibit transactions with designated nationals, and ban investments and export/import of goods related to Crimea. In 2017, the **Countering American Adversaries Through Sanctions Act (CAATSA)** went into force. Section 231, administered by the U.S. Department of State, addresses transactions with the Russian intelligence and defense sectors, allowing the United States to act against any individual or entity engaged in the manufacture, sale, or delivery of Russian advanced conventional weapons. Notably, unlike other sanctions regimes, CAATSA allows the United States to impose penalties on any entity – including non-American ones – if they engage with illicit entities. Currently, there are over 700 entities on the list of the Russian individuals companies, and other entities, and additions are periodically announced. The sanctions are intended to shrink the overall size and reduce the sophistication of Russia's economy, hindering the country's ongoing military modernization and impacting its ability to fund domestic arms production. Additionally, the sanctions include **an expanded ban on dual-use items (items with both civilian and military purposes) as well as a significantly expanded export control regime,** severely limiting the ability of Russian end users to acquire dual-use products or technology. The Department of Commerce's Bureau of Industry and Security (BIS), which administers licenses for controlled items, issued a new rule sharply restricting (having been reviewed "under a policy of denial") Russia's access to specific goods, including microelectronics, telecommunications items, sensors, navigation equipment, avionics, marine equipment, and aircraft components.

The **European Union** has imposed significant parallel sanctions against Russia, starting in 2014. As of December 2022, the EU had approved nine packages of sanctions against Russia. These sanctions target Russia generally, including its oil exports, and have a number of measures specifically targeting Russia's advanced conventional weapons industry. The EU sanctions are specifically aimed at limiting Russia's capacity to manufacture new weapons and repair the existing ones, as well as disrupting its ability to transport material. These sanctions target over 400 Russian entities to cut off their access to sensitive dual-use and advanced technology items. A number of other countries, including **the UK, Japan, and Australia,** have implemented sanctions against Russia.

These bilateral regimes do not have the same extraterritorial enforcement mechanism as the CAATSA sanctions but do have specific provisions targeting Russia's conventional weapons program. UK sanctions, for example, target defense sector organizations' efforts to gain access to critical technologies. Japan's sanctions focus on restrictions of payments and capital transactions with designated individuals and entities (including from the defense sector) as well as on exports of controlled items and other dual-use goods such as semiconductors. Australian sanctions prohibit the sale of any goods or services related to Russian arms or military equipment.

ACW and Its Components

Current sanctions against Russia aim to **restrict Russia's ability to import critical system components** and high-performance machine tools, which will have a significant impact on Russia's ability to manufacture advanced conventional weapons. Russia and its allies, however, have **sophisticated networks** in place to circumvent sanctions and acquire weapons and components to allow continued manufacturing in its defense industrial complex.

The term ACW (advanced conventional weapons) covers a wide range of weapons systems, including Man-Portable Air Defense Systems (MANPADS) and Anti-Tank Guided Missiles (ATGMs); major weapons systems and heavy military equipment such as tanks, aircraft, and missiles; sensors and lasers; and precision-guided munitions. While certain types of firms may come across full or partial weapons systems, it is far more likely to run into challenges associated with the export, sale, or transfer of components.

The U.S. measures also target Russian military end-users through the addition of the latter to the Department of Commerce's Entity List, which has effectively blocked their access to nearly all items subject to the Export Administration Regulations (EAR), including certain electronics, sensors, and supplies for telecommunications and computer processing. The sanctions may also force Russian defense companies to face rising interest rates on loans and high prices for materials and components.

While sanctions may take a long time to exert a significant effect due to the long lead time usually required for the production of weapons systems, there are reasons to believe that the sanctions have impacted Russia's ability to manufacture key systems – e. g., precision-guided munitions. For example, according to the Russian media, the progress on the next-generation airborne early warning and control (AEW&C) aircraft, the A-100 Premier, has been stalled due to delays in the delivery of electronic components like microchips.

Some components are clearly intended for military purposes based on their type or grade; however, weapons may be manufactured using many dual-use components that are not initially designed for or do not appear to have nefarious purposes. Therefore, firms find these items particularly challenging in their attempts to identify illicit weapon-related transactions.

Broadly speaking, the types of components that could be used by military end-users for ACW and should be subject to additional scrutiny by firms include the following:

Type of component	Usage
Microelectronics/microchips	Communications equipment, UAS, precision long-range munitions
Semiconductors	Defense-related components (computers, sensors, switches, amplifiers)
Bearings	Tanks, aircraft, submarines, other military systems
Connectors, fasteners, transformers, casings, transistors, insulators	Basic components that constitute the electronics systems in a conventional weapon system
Engines, vehicle parts	Tanks, ACVs, aircraft
Composite material	Aircraft wings

According to an alleged list of priority items composed by Russian officials, Russia is actively seeking a range of dual-use electronic items for use in its defense industry. According to this report, most of the 25 items Russia is desperately seeking are microchips manufactured by U.S. firms - Marvell, Intel, Holt, ISSI, Microchip, Micron, Broadcom and Texas Instruments, as well as by Japanese firm Renesas, and Germany's Infineon; also microcircuits by American firm Vicor, and connectors by U.S. firm AirBorn.[1]

The U.S. Department of Commerce has also identified a list of commodities subject to export control requirements that are at higher risk for illicit export or re-export to Russia or Belarus, as these items can support Russia's military and defense capacity. The components, listed below, all require a license from BIS, which is likely to be denied:

Commodity	Export Control Classification Number
Aircraft Parts and Equipment	ECCN 9A991
Antennas	ECCN 7A994
Breathing Systems	ECCN 8A992
Cameras	ECCN 6A993
GPS Systems	ECCN 7A994
Inertial Measurement Units	ECCN 7A994
Integrated Circuits	ECCN 3A001, 3A991, 5A991
Oil Field Equipment	ECCN EAR99
Sonar Systems	ECCN 6A991
Spectrophotometers	ECCN 3A999
Test Equipment	ECCN 3B992

[1] **Sources:**
Zoya Sheftalovich and Laurens Cerulus, "The Chips Are Down: Putin Scrambles for High-Tech Parts as his ArsenaGoes up in Smoke," Politico, September 5, 2022, https://www.politico.eu/article/the-chips-are-down-russia-hunts-western-parts-to-run-its-war-machines/

Thrusters (Marine)	ECCN 8A992
Underwater Communications	ECCN 5A991
Vacuum Pumps	ECCN 2B999
Wafer Fabrication Equipment	ECCN 3B001, 3B991
Wafer Substrates	ECCN 3C001 through 3C006

Many of these components are made by companies in the U.S., Germany, the Netherlands, the U.K., Taiwan, and Japan among others, but could be found anywhere due to the prevalence of re-exporters and freight forwarding services.

Some sanctions regimes, such as those adopted by the EU, have specific bans on transactions involving certain dual use goods, including the following:

- toy/hobby drones
- complex generator devices
- laptop computers and computing components
- printed circuits
- radio navigational systems
- radio remote control apparatus
- aircraft engines and parts of engines
- cameras and lenses
- drone engines
- camouflage gear
- additional chemical/biological equipment
- riot control agents.

Procurement Networks

Russia has a sophisticated system of procurement networks. Because of its inability to source components through traditional means, Russia is being forced to turn to other sources, either other countries or opaque non-traditional networks.

Russia has sought to replace the components needed for the manufacture of its systems, including through sourcing parts from Chinese components manufacturers. This approach will likely have an impact on the long-term quality and viability of Russian systems. China also does not seem to have the access to high quality components, like micro-chips and semiconductors, which would make a

significant difference. Russia has historically relied heavily on Western technology for its weapons systems, which makes the use of the Chinese equivalents less effective.

There is also a growing concern that Russia will seek to acquire advanced conventional weapons, including ballistic missiles, surface-to-air missiles, and drones **from Iran,** which would be a violation of the 2015 UN Security Council resolution that endorsed the Iran nuclear deal, the Joint Comprehensive Plan of Action (JCPOA). The Biden administration has also implemented sanctions against any Iranian firms involved in this type of transfer or sale. The EU has banned the direct export of certain equipment, including drone engines, to Russia directly or to any third country (like Iran), from which it may be re-exported to Russia.

A more challenging case that merits attention is Russia's procurement of ACW components through **third countries, known as transshipment hubs.** A recent analysis [2] by the UK think tank RUSI indicates that Russia is developing clandestine networks involving third-country transshipment hubs to secure access to microelectronics. This includes the use of a range of front companies and fraudulent end users, which poses a particular challenge because, often, these organizations legitimately acquire microelectronics or other components and then send them on to the sanctioned end users in Russia. Microelectronic third-party distributors and wholesalers often operate from intermediary jurisdictions, which restricts the ability of sellers and manufacturers to correctly identify and avoid firms associated with sanctioned end-users. This highlights the need for a robust internal compliance system and procedures, as outlined later in this manual. A recent example of this involved OFAC sanctioning three individuals and a Hong Kong company named EMC Sud Limited for allegedly covert procurement of electronics from the U.S., Japan, and Europe to benefit Russia's defense industrial base.

Arms Sales

Outside of oil and gas exports, Russia's advanced conventional weapons systems constitute its more lucrative export, which has seen a decline in recent years with the rise in the political and reputational costs of purchasing the Russian weapons. Revenue from arms exports is an important source of export earnings for the Russian economy broadly, and arms sales and arms exports are an important aspect of Russian foreign policy as well. The United States and other countries have aggressively lobbied against the purchase of the Russian systems by Allies and other countries, including, for example, Indonesia and Morocco. Russia has sought to avoid the U.S. sanctions aimed at the sale of its systems by accepting payments in other currencies or goods.[3]

[2] James Byrne, Gary Somerville, Joe Byrne, Jack Watling, Nick Reynolds, and Jane Baker, "Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine," RUSI, August 2022, https://static.rusi.org/RUSI-Silicon-Lifeline-final-updated-web_1.pdf

[3] John Parachini and Ryan Bauer, "Sanctions Targeting Russia's Defense Sector: Will They Influence Its Behavior," The RAND Blog, May 20, 2021, https://www.rand.org/blog/2021/05/sanctions-targeting-russias-defense-sector-will-they.html

There is not a significant, if any, market for Russian ACW in Georgia. However, firms can run afoul of sanctions related to Russian arms sales by:

a. **Financing the Russian arms or dual use goods:** financial institutions need to be vigilant about financial transactions that could be used to finance the purchase of Russian weapons or dual use goods by third parties, either state or non-state.

b. **Involvement in the transportation of Russian arms or dual use goods:** financial institutions and firms specializing in shipping, air, or ground transportation could be subjected to sanctions related to the transportation of certain goods.

Firms also need to keep a wary eye on potential purchasers of Russian advanced conventional weapons systems. Industry experts predict India, China, Egypt, Algeria, and Iraq as likely customers of the Russian arms industry in the coming years. Russia's growing association with Turkey may also continue. Russia may also use sales to reinforce old alliances, such as its military alliances with Iran, Syria, and Venezuela.[4]

Relevant Entities and Individuals

Sanction regimes, including CAATSA, address a significant number of entities and individuals. Critically, the list contains all major elite Russian conventional weapons manufacturers.

- **Almaz-Antey Air and Space Defense Corporation JSC:** one of the world's largest defense industry complexes, specializing in the development of anti-air, anti-missile and space defense systems, notably Russia's S-400 Surface-to-Air Missiles (SAMs).
- **Research and Production Corporation Uralvagonzavod JSC:** a large machine building corporation and the only military tank manufacturer in Russia.
- **Russian Helicopters JSC:** a state-owned holding company that oversees the design, manufacturing, testing, and maintenance of helicopters for Russia's military.
- **Tactical Missiles Corporation JSC:** a large, state-owned Russian defense conglomerate that produces materials in support of Russia's defense-industrial base, including missiles and other airborne weapons, naval weapons, digital computers, and radar systems.
- **United Aircraft Corporation:** an aerospace and defense corporation engaged in the manufacture, design and sale of military, civilian, transport, and unmanned aircraft.
- **United Shipbuilding Corporation:** the largest shipbuilding company in Russia, responsible for building warships, submarines, frigates and mine sweepers for the Russian military.

[4] David Hutchins, "Russia's Advanced Conventional Weapons Trade and Associated Sanctions," Global Risk Intel, March 23, 2020, https://www.-globalriskintel.com/insights/russias-advanced-conventional-weapons-trade-and-associated-sanctions

- The above-listed manufacturers have tried to evade the sanctions against them on numerous occasions. One prime example is the recent report by **Research and Production Corporation Uralvagonzavod JSC:** a large machine building corporation and the only military tank manufacturer in Russia.

Reuters, according to which Almaz-Antey bypassed German export control restrictions and procured more than $10 million's worth of high-precision metalworking machines between 2015 and 2018. The export-license papers claimed the machinery was destined for other civilian uses, while they were actually delivered to an Almaz-Antey facility.

There are **other significant Russian companies** that are sanctioned due to their role in the Russian defense industry, and, in this regard, Rostec and Rosoboronexport are of particular note. According to the U.S. Department of State, Rostec is the "cornerstone" of Russia's defense, industrial, technology, and manufacturing sectors. Accordingly, the sanctions are imposed both on the firm and its board of directors. Rosoboronexport, on the other hand, is Russia's state-controlled agency for exporting and importing a wide range of military, defense, and dual-use products, technologies, and services.

U.S. sanctions have also targeted Russia's largest **financial institutions** and restricted dealings with banks representing 80 percent of the Russian banking sector assets. These sanctions extend to branches of Russian banks in foreign countries. For example, the Georgian branch of the Russian bank VTB was sanctioned by the U.S. and ultimately withdrew operations from Georgia.

The U.S. and the EU sanctions regimes also target **individuals,** with consequences ranging from travel bans to asset freezes. Importantly, individuals and entities located outside the sanctioning country who have sought to procure goods and technology for the Russian military-industrial complex and intelligence services can be subjected to sanctions as well. Sanctioned individuals may include owners of the sanctioned businesses with ACW-related military end-users. For example, OFAC designated Yury Yuryevich Orekhov, a Russian procurement agent, and two of his companies, NDA GmbH and Opus Energy Trading - for purchasing microprocessors and semiconductors used in fighter jets, smart munitions, hypersonic and ballistic missiles, satellites and radars from U.S. manufacturers.

While it is possible that Georgian firms may come across transactions associated with the above companies, it is far more likely that ACW-related transactions would be implemented through shell companies or networks of legitimate companies with ties to the Russian military end users. Importantly, for U.S. sanctions, property and interests in property of entities directly or indirectly owned 50 percent or more in the aggregate by one or more blocked persons are considered blocked. For example, as a demonstration of how important it is to understand networks, the sanctions imposed on the Russian defense company Tactical Missiles Corporation JSC (known as KTRV) also included its general director, Boris Viktorovich Obsonov, and 28 additional entities that are part of KTRV's structure. According to the U.S. Department of the Treasury, these entities design and manufacture diverse products in support of Russia's defense-industrial base, such as ammunition, radar systems, missile systems, and other military equipment. Additionally, any

other entities owned 50 percent or more, directly or indirectly, by KTRV are subject to blocking, even if not identified in the list of the 28 entities[5]. Further, 28 entities of the United Shipbuilding and 15 associated entities of Russian Helicopters were also sanctioned.

Non-Russian regional firms

Of potentially greater risk than doing business with a sanctioned Russian firm, which may be more easily avoided, is the potential for transactions and business relationships with **regional firms in the Caucasus and Central Asia that serve as transshipment points** between third party countries and the sanctioned Russian end-users. In a recent FINCEN/BIS joint alert, Georgia, Armenia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan were all identified as "common transshipment points through which restricted or controlled exports have been known to pass before reaching destinations in Russia or Belarus." In 2022, trade between Russia and several countries in the Caucasus and Central Asia has increased for a variety of reasons, both political and economic. For example, Armenia's trade with Russia grew 49% in the first half of 2022, with the corresponding figure standing at 40% for Kyrgyzstan, 32% for Georgia, 29% for Uzbekistan, 20% for Tajikistan, 17% for Azerbaijan and 5% for Kazakhstan[6].

Diverse factors in the Caucasus make **Armenia and Azerbaijan** desirable locations for attempts to side-step the sanctions and the export control requirements. Both countries have significant numbers of expats in Russia with connections in the Caucasus. There are also large quantities of Russian enterprises operating in both Armenia and Azerbaijan. The list of Russian enterprises in the Caucasus, as well as the list of Russian entrepreneurs doing business in the Caucasus is extensive, both of which can provide the type of connections that will enable the evasion of the imposed sanctions. One recent example, in 2022, involved OFAC designating Milur Electronics, the Armenia-based affiliate of Milandr, a Russian microelectronics company that has been described as part of the Russian military research and development structure defense technology firm. Milur and its CEO were accused of placing orders from foreign factories, producing integrated microchips, and conducting sales overseas on behalf of Milandr.[7]

Central Asia has a long history of close political and economic ties to Russia, particularly to Russia's defense industry, providing Russia with military equipment and technology for years. The domestic legislative environment and close ties to the Russian defense sector make several countries of Central Asia prime locations for sanctions evasion. Many also lack an effective mechanism for imposing secondary sanctions for cooperation with the Russian sanctioned businesses. In June 2022, the U.S. sanctioned the Uzbekistani firm Promcompleklogistic Private Company for shipping

5 See complete list from U.S. Department of Treasury. "U.S. Treasury Sanction Russa's Defense-Industrial Base, the Russian Duma and its Members, and Sberbanks CEO," U.S. Department of the Treasury Press Release, March 24, 2022, https://home.treasury.gov/news/press-releases/jy0677

6 Alexey Eremeko and Henry Smith, "Managing Rising Sanctions Risks Across the South Caucasus and Central Asia," Control Risks, https://www.controlrisks.com/our-thinking/insights/managing-rising-sanctions-risks-across-the-south-caucasus-and-central-asia

7 "Treasury Sanctions Global Russian Military Supply Chain, Kremlin-linked Networks, and Elites with Western Fortunes," U.S. Department of Treasury, November 14, 2022, https://home.treasury.gov/news/press-releases/jy1102

goods to a sanctioned electronics maker in Russia, Radioavtomatika, which specializes in procuring foreign items for Russia's defense industry. The U.S. Department of State said "the designation of Promcomplektlogistic Private Company should serve as a warning to commercial stakeholders worldwide: If you do business with sanctioned entities or individuals, you risk exposure to sanctions." There are also examples of Kyrgyz enterprises developing and supplying armaments for submarines and surface ships, as well as a Kazakh company producing components for Russian-designed aircrafts and helicopters.[8]

Threats in the Georgian context

There have been claims, though without significant substantiation, that sanctioned Russian individuals or firms use the Georgian financial system, banks, and companies to process transactions and evade sanctions. Even without any specific evidence, it is reasonable to assume that Georgia – like its neighbors – would be a desirable location to conduct such activities, requiring significant vigilance on the part of the Georgian financial and private sectors.

Georgia has a legal framework in place to prevent certain types of illicit transactions, called "Law of Georgia on Facilitating the Prevention of Money Laundering and the Financing of Terrorism." This law is focused on UN Security Council Resolutions imposing sanctions related to money laundering, foreign terrorist financing, and proliferation financing, as these sanctions regimes are legally binding and apply to Georgia. A governmental commission on these resolutions is led by the Ministry of Justice and sanctioned persons and entities can be found on the Ministry's website. This does not, however, apply to bilateral (non-UN) sanctions, like the sanctions and controls discussed in this manual.

There are a number of ways that goods can be transported between Georgia and Russia. Currently, Georgia and Russia are linked **by road**, with the only operational border crossing point functioning in Kazbegi. As per statistical data, the transportation rate along that route has increased significantly in recent years, nearly doubling since 2019. Detection of the sanctioned goods along this route is mainly left to the Georgian customs service, as most Georgian road transportation companies have little understanding of the sanctions regimes. A recent report by a Georgian NGO (non-governmental organization) - Institute for the Development of Freedom of Information (IDFI)[9] - highlights some of the challenges faced by Georgia based on the official records obtained from Georgian officials. From February to August 2022, the Revenue Service turned away a total of 204 cargo shipments destined for Russia and Belarus, including a shipment

8 Yevgeniya Gaber, Yurii Poita, Gela Vasadze, "Support of the Sanctions Regime Against Russia by Turkiye and Countries of the South Caucasus and Central Asia," Ukrainian Prism Foreign Policy Council, http://prismua.org/en/sacntions2467/

9 Institute for Development of Freedom of Information, "Georgia's Implementation of International Sanctions Imposed on Russia (February-August)," 2022 https://bit.ly/3z0BPbE

of drones headed for Russia. The Georgian Minister of Finance, Mr. Lasha Khutsishvili, stated that, "more than 1000 transactions have been suspended and canceled because there was a risk of violating sanctions"[10] from February 24, 2022 to January 23, 2023. According to the registration cards, the countries sending the sanctioned cargo (or the cargo of a sanctioned person) included Turkey (39%) in the first place, Armenia (35%), and – in 15 cases (7%) – Georgia. **Rail transportation** of goods is less common, as there is no direct rail connectivity between Georgia and Russia. Rail transportation does occur via Azerbaijan though, whose rail service is operated and maintained by the Russian industry. There are no direct flight connections between Georgia and Russia, however, the cargo can be transported **by air** via connecting flights from Minsk, Yerevan, or Istanbul. Georgian air companies display better understanding of sanctions and a process in place to detect and prevent illicit transactions.

The IDFI report also outlines several steps taken by the National Bank of Georgia to ensure compliance with the sanctions regimes among the Georgian financial institutions. These include the following:

- Cessation of all transactions and provision of foreign currency to a sanctioned bank (the Georgian arm of the Russian bank, VTB banks);
- Development of additional reporting forms for commercial banks and tax service providers requiring detailed information on clients/transactions related to Russia, Belarus, and other high-risk countries;
- Creation of a department for the oversight of the implementation of international sanctions;
- Instructing the commercial banks to update their respective sanctions procedures;
- Creation of on-site inspection mechanism and an evaluation methodology.

A review of the practices adopted by the Georgian financial firms revealed a high degree of understanding of the implications of sanctions regimes on bank operations. Georgian banks report keen awareness of the international sanctions against Russia, monitoring of transactions and open-source information, and focused due diligence on Russian firms or individuals. Some banks require additional identification and origin documents to confirm the individual or organization is not enlisted as a sanctioned person or entity. Other banks reported a limited understanding of ACW and its components, as well as difficulty in identifying transactions that may be related to the sanctioned individuals or entities.

10 ლაშა ხუციშვილი - 2022 წლის 24 თებერვლის შემდეგ 1000-ზე მეტი ოპერაციაა შეჩერებული და გაუქმებული, რადგან არსებობდა სანქციების დარღვევის რისკი - შესაძლებელია, ევროკავშირის ბევრ ქვეყანაშიც ვერ ხორციელდებოდეს ასეთი კონტროლი, Interpress News, January 23, 2023, https://bit.ly/3nckZE5

Interviews with Georgian transportation companies reveal a general awareness of sanctions, with less specific understanding of sanctions requirements related to advanced conventional weapons. Transportation companies in Georgia tend to avoid risk by not cooperating with Russian companies or newly registered companies that may have less clear ties to Russia. Some transportation companies report efforts to determine whether the goods being transported are of dual use; they are also trying to identify senders, recipients, and shipment funders. Georgian firms report a desire for more easily searched and comprehensive lists of the sanctioned individuals, companies, and items related to ACW.

Case studies

The following case studies were chosen to highlight both the real-world implications of the failure to identify illicit ACW-related financial transactions and the role that shell and intermediary companies can play in these transactions.

1. Rad-Hard chips to Russia, via Bulgaria.[11]

Case description: Ilias Sabirov, a longtime Russian supplier of U. S.-produced weapons-grade electronics, including high-performance computer chips, to the Russian defense sector, was subject to post-2014 sanctions and export control restrictions. His company allegedly sourced "rad-hard" chips (critical components in missiles and military satellites) from a company in Austin, Texas, called Silicon Space Technology Corp, or SST, which were shipped to Russia via a firm in Bulgaria to evade the U.S. export control laws. Investigators discovered a complex network of suppliers, front and shell companies and false claims in export forms that specialized Western components were intended for civilian rather than military use. SST claimed that it believed the shipments were going to Bulgaria for use in Europe, having received a valid end user certificate that the end user was not in Russia. Sabirov and the Bulgarian intermediaries, Dimitar and Milan Dimitrov, were indicted in 2020 by U.S. authorities, accused of money laundering and illegally exporting rad-hard chips to Russia. The U.S. company, SST, was fined $497,000 last year by the U.S. Department of Commerce's Bureau of Industry and Security in a separate enforcement action.

2. Advanced microelectronics from Germany to Russian defense companies [12]

Case description: R&S Electronics Gb, a German private partnership, has allegedly sold semiconductor components made in Western countries to Russian import and export firms and

11 David Gauthier-Villars, Steve Stecklow, John Shiffman, "Special Report: How Military Technology Reaches Russia in Breach of U.S. Export Controls," Reuters, April 29, 2022, https://www.reuters.com/article/us-ukraine-crisis-russia-sanctions-idAFKCN2ML19M)

12 Peter Maroulis and Robert Kim, "German Partnership Supplied Western Dual-Use Technology to Rusian Defense Companies, Kharon: The Brief, November 1, 2022, https://bit.ly/3LOQAGi

technology companies, before and after the 2022 Russian invasion of Ukraine and the imposition of the related sanctions and export restrictions. An investigation by the financial crimes think tank Kharon revealed two transactions with loopholes that challenged the effective sanctions targeting the ACW components. First, while one of R&S Electronics' main customers is a Russian company that supplies semiconductor components to sanctioned military end users in Russia, the organization itself is neither sanctioned nor appears on the export control lists of the EU or BIS. R&S Electronics has also allegedly supplied equipment to a U.S. and U.K.-designated Russian limited liability companies that supply telecommunications and other electronic equipment to sanctioned Russian state-owned entities.

3. U.S. technology for a Russian state-owned defense firm[13]

Case description: MMZ Avangard, a state-owned firm that produces advanced Russian missile systems (including the S-400), has been subject to strict U.S. sanctions since 2014. According to an investigation by Reuters, publicly traded American technology company, Extreme Networks, was providing MMZ Avangard with computer networking equipment for its IT systems. Extreme claims the equipment was sold without its knowledge by an intermediary in Russia that supplied its products to sanctioned end users via a front company. The products included high-speed switches and software. Reuters obtained an internal complaint filed by Extreme's employee, alleging that the company was selling to various military manufacturers in Russia and that their IT equipment was in use on Russian warships. Furthermore, after concerns were raised about the potential end-user, the Extreme compliance team requested a self-certification that there was no military end user, that the equipment would not be resold for any military purpose, and that it would not be transferred to any sanctioned company.

4. U.S. technology and equipment in Russian ACW used in Ukraine[14]

Case description: A 2022 study by the UK defense and security think tank RUSI took an in-depth look at 27 different Russian conventional weapons systems, including cruise missiles, UAVs, and communications equipment, and discovered at least 450 different kinds of unique foreign-made components, including a majority from U.S. companies that are suppliers of the U.S. military. Of these, at least 80 different kinds of components were subject to export controls by the US, showing Russia's historic and current ability to evade restrictions.

5. Venezuelan Oil, Russian Military Equipment[15]

13 Aram Rosten and David Gauthier-Villars, "Special Report: U.S. Firm Supplied Networking Tech to Maker of Russian Missiles," Reuters, October 12, 2022, https://www.reuters.com/technology/how-us-firm-supplied-networking-technology-maker-feared-russian-missiles-2022-10-12/

14 James Byrne, Gary Somerville, Joe Byrne, Jack Watling, Nick Reynolds, and Jane Baker, "Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine," RUSI, August 2022, https://static.rusi.org/RUSI-Silicon-Lifeline-final-updated-web_1.pdf

15 "Justice Department Announces Charges and Arrests in Two Cases Involving Export Violation Schemes to Aid Russian Military," Justice News, October 2022, https://www.justice.gov/opa/pr/justice-department-announces-charges-and-arrests-two-cases-involving-export-violation-schemes

Case description: In October 2022, the U.S. Department of Justice indicted several Russian nationals, alleging they "orchestrate[d] a complex scheme to unlawfully obtain U.S. military technology and Venezuelan sanctioned oil through a myriad of transactions involving shell companies and cryptocurrency." In addition to smuggling hundreds of millions of barrels of oil from Venezuela, the accused used a front company to source and purchase sensitive military and dual-use technologies from U.S. manufacturers, including advanced semiconductors and microprocessors used in Russian fighter aircraft, missile systems, smart munitions, radar, satellites, and other military applications. Payments for these illicit activities were routed through U.S. financial institutions, using fictitious companies, falsified "know your customer" documentation, and cryptocurrency transfers to launder the funds.

6. Circumventing Export Control Restrictions with the Involvement of the Russian Government[16]

Case description: In December 2022, the U.S. Department of Justice charged five Russian nationals and two U.S. nationals for allegedly conspiring to obtain military-grade and dual-use technologies from U.S. companies for Russia's defense sector, and to smuggle sniper rifle ammunition in violation of U.S. sanctions. The defendants "unlawfully purchased and exported highly sensitive and heavily regulated electronic components, some of which can be used in the development of nuclear and hypersonic weapons, quantum computing and other military applications." The defendants operated a network of shell companies and bank accounts to conceal the involvement of the Russian government and the identities of sanctions end users. The defendants – allegedly operating under orders from the Russian government – fabricated shipping documents and invoices and reshipped the items to intermediate destinations.

Key takeaways

- Firms need to be aware of **multiple sanctions regimes** - bilateral or multilateral - to ensure compliance. Certain regimes have extra-territorial enforcement mechanisms, others require several aspects of the transaction to take place inside certain territories;
- There are many **component parts of ACW** (tables X and X) that may not immediately appear designated but are subject to sectoral sanctions or specific bans;
- Compliance with the sanctions against Russia also require vigilance about transactions involving firms and materials in other countries due to **sophisticated procurement networks** aimed at circumventing the sanctions;
- The sanctions target **major Russian ACW manufacturers**, as well as other major defense companies and military end users. **Certain individuals** associated with the defense industry are also subject to sanctions.

16 "Russian Military and Intelligence Agencies Procurement Network Indicted in Brooklyn Federal Court," Justice News, December 13, 2022, https://www.justice.gov/opa/pr/russian-military-and-intelligence-agencies-procurement-network-indicted-brooklyn-federal

IMPLEMENTING AN EFFECTIVE AND COMPLIANT RESPONSE TO SANCTIONS

Any business that operates across multiple jurisdictions, in financial or banking services, or in certain defense and equipment-related sectors must be wary of the risk posed by non-compliance with sanctions or export control regimes. The rapid expansion of enforcement mechanisms now compels all businesses, regardless of sectors, to consider the risks posed by sanctions enforcement and adopt the relevant compliance regime. Some types of firms, such as logistics, finance, and goods manufacturers, are more vulnerable than others. Because Russia relies on access to the formal financial system to raise and gain access to funds, conduct payments, and facilitate illicit activities, it is contingent on private sector firms to assess the risk posed by their customers and specific transactions, as well as monitor and report illicit activities. Georgian firms have likely not had the requirement to be vigilant about these types of transactions until recent years, so some companies may not be aware of certain restrictions on goods and services offered to Russian firms. Firms that produce high-specification goods and that are prone to being targeted by illicit procurement processes are often small and medium-sized enterprises. Though many firms, particularly in the financial services and banking sector may have some form of compliance program in place, many firms lack the resources and understanding to assess risks and apply the appropriate risk-based approach to countering illicit transactions associated with ACW.

ACW-specific Sanctions Compliance Programs in Georgia

There are multiple types of firms that need to have effective sanctions compliance programs in place. These include the following:

- Financial institutions: According to BIS/FINCEN, these types of firms may be involved in providing financing, processing payments, issuing lines of credit, factoring accounts receivable by exporting, providing capital loans, and providing insurance for shipping and delivery of goods or paying insurance fees. **In Georgia, this includes commercial and electronic banks, credit card operators, and foreign exchange dealers;**

- Electronics firms: Electronics exporters and resellers face particular challenges in terms of compliance with sanctions and export control regimes, particularly involving the sale of components that could be used in ACW production. Many electronics exporters sell at high volume to a range of customers, and their business activity usually focuses on off-the-shelf components. A key part of preventing illicit sales is understanding the end user, which is difficult considering the great and changing number of customers. Compliance is easier for firms that specialize in particularly sensitive electronics, such as those for the defense sector, because they tend to have a more limited range of repeat customers. **In Georgia, this type of firm includes importers and exporters of electronics and other technology;**

- Transportation firms: the U.S. sanctions and export control enforcement has increasingly focused on supply chain risks, targeting firms involved in the transportation, forwarding, or movement of the sanctioned goods. This can be particularly challenging, given the limitations of screening tools for the detection of the sanctioned parties in supply chains. **In Georgia, these types of firms include air cargo companies, freight forwarders, railways, shopping lines, and road transport operators;**

- Defense sector: In some countries, the defense sector – either state-owned or private – can be engaged in the import/export of military grade components. **Similar transactions related to Russian ACW are unlikely to occur in Georgia given the lack of relations between the Georgian and Russian military and security institutions.**

An effective sanctions compliance program must be able to adapt to constantly changing sanctions requirements. This is particularly true for policies aimed at deterring illicit transactions related to Russia and ACW, given the evolving nature of this particular set of sanctions and export control requirements.

A basic sanctions compliance program typically includes a set of internal policies and procedures, typically outlined in a compliance manual. These policies typically include[17] the following questions:

- What sanctions pose a risk to the firm in question?
- Why it is important for the firm to comply with sanctions?
- What controls exist to ensure the firm's compliance?
- What obligations exist for individual employees?
- What are the consequences of non-compliance?

Tailoring Risk Assessments to ACW

A risk assessment (RA) allows organizations to set priorities and processes in order to understand and estimate the risks related to ACW and the respective sanctions. The RA is at the core of any effective sanctions compliance program. Without a risk assessment, the best practices noted below (internal controls (including due diligence and screening), policies and procedures, and training) will not be effective. Not all aspects of RA will be applicable to all types of firms, but it is unlikely that a firm can meet its sanctions-related obligations without a full insight into the risks it may be exposed to.

[17] Zia Ullah and Victoria Turner, "Principled Guide to Sanctions Compliance Programmes," Global Investigations Review, July 8, 2022, https://bit.ly/3lEghi4

The RA is a product that identifies, analyzes, and understands the sanctions-related risk, with a view to mitigating that risk. Risk assessments should have a broad scope and should include the assessment of:

- customer risk;
- product and services risk;
- geography-related (organization and customers) risk;
- transaction risk;
- delivery risk;
- risk from mergers and acquisitions;
- supply chain risk;
- risk from intermediaries; and
- networks or systems risk.

Many firms, particularly banks and financial institutions, will already have a robust system in place to identify the risks associated with money laundering (AML) or terrorist financing (CTF), many of which can be adapted to address the risks related to ACW and sanctions. Some firms may also have RAs related to proliferation financing, a subset of financial crime focused on violations of the UN Security Council's resolutions aimed at countering the acquisition of WMD and the associated materials.

The existing risk assessments can and should be adapted to also address sanctions targeting other weapons, including ACW. This can be achieved by:

- including an analysis of the firm's exposure to clients in the geographic area of highest risk, in this case, Russian or Belarussian clients;
- identifying clients, partners, or other relationships that are involved in potentially risky sectors, including defense, shipping, freight forwarding, financial services, and electronics;
- scoping risk assessments to include exposure to risk in supply chains and other transactions that may involve a sanctioned end user.

Best Practices for complying with Russia-related sanctions and export control

Developing a compliance program that can detect illicit transactions associated with ACW can be challenging, due to the required multi-tier visibility of goods and transactions, including their origin, transit, and destination countries. There are, however, some clear best practices that firms,

both financial institutions and others, can implement to put themselves in an advantageous position for detecting transactions and showing the enforcement authorities that they do so in good faith. A number of open-source tools are listed in Annex A to assist with this type of due diligence.

None of the below practices should operate in isolation: due diligence and risk assessment requirements must be aligned with the screening tool for this system to prove effective. Ultimately, a firm's risk assessment should inform how a screening solution is utilized, what is screened and when.

Due Diligence (Know Your Customer/Supplier): Firms should ensure due-diligence is performed on potential customers, business partners, and goods through the use of public information such as early warning lists, red-flag checklists, and questionnaries. A basic requirement for a sanctions compliance program is to be clear on the ownership and control structure of the organization. Due diligence may need to extend beyond the immediate customers to also cover the clients' clients[18] to detect the intricate networks associated with the ACW components. Sanctions enforcement agencies increasingly expect firms to know about compliance risks posed by their suppliers and ensure that their respective procedures mitigate the risk. Due diligence can range from basic internet searches of entities and identifiers to ensuring goods requested are appropriate for the stated end-use.

Customs officials have developed a useful list of behavioral red flags for customer interactions in proliferation financing that can be applied to screening of customers with ACW-associated risks. The red flags may include:

- Your firm is approached by a customer whose identity is not clear;
- The customer has little or no business background;
- The customer is usually involved in military-related business;
- The customer or their address is similar to the ones listed in the sanctioned entity lists;
- The customer is reluctant to offer information about the end-use of the goods;
- The customer requests shipment or labelling of goods that are inconsistent with usual shipping and labelling practices;
- The customer is unfamiliar with the product's performance characteristics but still wants the product;
- The customer declines routine installation, training, or maintenance services;
- When questioned, the customer is evasive and unclear about whether the product is for domestic use, export, or re-export.[19]

18 Alexey Eremeko and Henry Smith, "Managing Rising Sanctions Risks Across the South Caucasus and Central Asia," Control Risks, https://www.controlrisks.com/our-thinking/insights/managing-rising-sanctions-risks-across-the-south-caucasus-and-central-asia

19 "Sanctioned Lists and Red Flags: United National Security Council (UNSC) Sanctions," Singapore Customs, https://www.customs.gov.sg/businesses/strategic-goods-control/sanctioned-lists-and-red-flags

List-Based Screening: Conducting sanctions screening is the major tool for financial service companies to ensure that they are not engaging in transactions subject to the sanctions regimes. List-based screening can often be automated and can be useful in identifying suspicious transactions. However, there are limits to this approach. A few of these lists are designed for exporters rather than financial firms, and lists are often updated infrequently. They can also give a false sense of security.

Targeted screening: In order to make screening more effective, firms can take a number of steps, including focusing on specific companies and areas of operation, taking stock of current threats, and investigating the known networks.

Internal policies: Firms should also clarify their policy on maintaining relationships with Russian banks or businesses and determine the extent to which the organization in question operates in Russia-related jurisdictions.

Training: A routine training program should also be part of a compliance program to ensure that all members of an organization understand the limitations that the sanctions create and the ways in which the respective risks can be identified.[20]

Existing best practices can and should be adapted to also address sanctions targeting other weapons, including ACW. This can be achieved by the following:

- Including questions relevant to sanctions and conventional weapons/components in their due diligence process – whether at the onboarding stage or over the course of the client relationship;
- Ensuring that the due diligence procedures of their clients – particularly of those involved in the manufacturing and trade of defense or related items - are comprehensive and the clients have a clear idea of both their business partners and the potential end-use of their products;
- Investigating weapons and components networks – and ties of specific clients to these networks – to reveal a possible connection to the firm.

Identifying ACW Transactions of Concern

It can be challenging to identify transactions or goods/services that would expose a firm to the risks related to the sanctions and export control enforcement due to the veiled nature of procurement networks for ACW and its components.

20 Alexey Eremeko and Henry Smith, "Managing Rising Sanctions Risks Across the South Caucasus and Central Asia," Control Risks, https://www.controlrisks.com/our-thinking/insights/managing-rising-sanctions-risks-across-the-south-caucasus-and-central-asia

According to BIS/FINCEN,[21] there are specific transactions financial institutions may have access to that would alert them to potentially suspicious activities related to ACW components:

- Customers' end-use certificates, export documents, or other more extensive documentation associated with letters of credit-based trade financing;
- Information about the other parties to the transactions that may be contained in payment transmittal orders they receive or handle as an intermediary institution;
- Letters of credit exporters receive from their customers (the importer);
- The line of credit to its customer (exporter) to facilitate the transaction;
- 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.

Government officials have created "red flag indicators" to help exporters identify behavior or transactions of concern. A full list of the red flags is included in Annex C. Some specific red flags related to ACW and components include:

- Large dollar or volume purchases of items from wholesale electrical/industrial merchants, electrical parts and equipment providers, or electronic parts providers.
- A customer transports commodities of concern and uses trade corridors known to serve as possible transshipment points for exports to Russia and Belarus.[22]
- The nature of a customer's underlying business/services/products relate to military or government work.
- 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.
- Transactions identified through the activities of a correspondent bank that seems connected to Russian sellers of electronic and other similar goods.
- Transactions involving payments 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.

21 "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," FinCEN & BIS Join Alert, June 28, 2022, https://www.fincen.gov/sites/default/files/2022-06/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf

22 "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," FinCEN & BIS Join Alert, June 28, 2022, https://www.fincen.gov/sites/default/files/2022-06/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf

- Delivery dates are vague, or deliveries are planned for out of the way destinations.
- The product's capabilities do not match the buyer's line of business (for example, an order for sophisticated computers for a small bakery).
- The ordered product is incompatible with the industrial level of the country it is being shipped to (for example, semiconductor manufacturing equipment shipped to a country that has no electronics industry).
- The shipping route is abnormal for the product and destination.
- The freight forwarding firm is listed as the product's final destination.
- Packaging is inconsistent with the stated method of shipment or destination.[23]

Illicit transactions may also occur by intentionally misidentifying the controlled item as "EAR99", a class of consumer goods that do not require a license for export/transfer. Items could also end up with sanctioned end users by intentionally obscuring the nature or destination of goods via complicit shippers or brokers.

Key Takeaways

- Private sector firms – particularly in the financial services, electronics, transportation, and defense sectors – should have **robust sanctions compliance programs that are tailored to identify transactions related to ACW components.**
- It is unlikely that a firm can meet its sanctions-related obligations without the full insight into the potential risks, which should be outlined in its **risk assessment** document.
- There are **specific transactions and red flag indicators** that financial institutions and exporters should be aware of and incorporate into their compliance sanctions programs.
- There are a number of **best practices for sanctions compliance programs** – including due diligence, screening, internal policies, and training – that firms can tailor to ACW related sanctions and export controls.

23 "Sanctioned Lists and Red Flags: United National Security Council (UNSC) Sanctions," Singapore Customs, https://www.customs.gov.sg/businesses/strategic-goods-control/sanctioned-lists-and-red-flags

ANNEX A: Resources for additional support

- OFAC List of Specially Designated Nationals and Blocked Persons (SDN List): OFAC publishes lists of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries.

- Bureau of Industry and Security (BIS) at U.S. Department of Commerce Entity List: The Export Administration Regulations (EAR) contain a list of names 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.

- U.S. Department of State, CAATSA Section 231(e) List: The Department of State maintains a list identifying persons that are part of, or operate for or on behalf of, the defense or intelligence sectors of the Government of the Russian Federation for the purposes of CAATSA Section 231.

- Office of Financial Sanctions Implementation (OFSI) of HM Treasury in the United Kingdom: The UK government publishes the UK Sanctions List, which provides details of those designated under regulations made under the Sanctions Act.

- European Union: the EU maintains a list of sanctioned individuals and entities. The list is subject to constant revisions and periodic updates by the Council.

- Australian Department of Foreign Affairs and Trade: The Australian government maintains a consolidated list of sanctioned individuals and entities.

- Japan's Ministry of Economy, Trade, and Industry (METI): The Japanese government issues an End User List, providing exporters with information on entities that may be involved in activities related to WMDs and other items.

- Russian tax registry, Clearspending NGO, e-justice system: These sites provide information on businesses registered in Russia, their structures, and court cases related to businesses.

ANNEX B: Additional Transactional and Behavioral Red Flags:[24]

- A customer transports commodities of concern and uses trade corridors known to serve as possible transshipment points for exports to Russia and Belarus.
- 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 against Russia and Belarus.
- Transactions involving entities with little to no web presence.
- Transactions involving a change in shipments or payments that were previously scheduled to go to Russia or Belarus, or to a company located in Russia or Belarus, but are now going to a different country/company.
- 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.
- Last-minute changes to transactions associated with an originator or beneficiary located in Russia or Belarus.
- 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).
- Transactions involving freight-forwarding firms that are also listed as the product's final end customer, especially items going to traditional Russian transshipment hubs.
- Transactions associated with atypical shipping routes for a product and destination.
- Transactions involving entities whose website or business registration documents state the entities work on "special purpose projects."
- Transactions involving companies that are physically co-located or have shared ownership with an entity on the BIS Entity List or the Department of the Treasury's Specially Designated Nationals and Blocked Persons List.
- 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.

24 "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," FinCEN & BIS Join Alert, June 28, 2022, https://www.fincen.gov/sites/default/files/2022-06/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf

- 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.

- 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.

- 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.

- 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.

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

ANNEX C: Template for Assessing ACW Sanctions Compliance Program [25]

I. Senior Management Commitment

- ☐ Does your firm have a sanctions compliance program (SCP) manual? Has Senior Management reviewed and approved the SCP?
- ☐ Does your firm have a dedicated sanctions compliance officer and the appropriate technology for screening?
- ☐ Is there a "culture of compliance" at your firm?

II. Risk Assessment

- ☐ Has your firm created a risk assessment for sanctions related to Russia?
- ☐ Does your firm know your customers and third parties?
  - ☐ Have individuals and entities been checked against sanctions lists?
  - ☐ Do you have visibility into the controlling interests behind individual customers, suppliers or other third parties?
- ☐ Does your firm know your product or service?
  - ☐ Does the product or service have a dual-use or military application?
  - ☐ Does the product or service require an export license?
  - ☐ Is the product or service subject to an embargo?
- ☐ Does your firm know the receiving country?
  - ☐ Is the receiving country Russia?
  - ☐ If not Russia, is the country a known facilitator for Russia?
- ☐ Does your firm know the end-use and end user?
  - ☐ Have you confirmed the intended end-use of the product or services?
  - ☐ Are there sanctions that might apply to that end-use?

25 Sources for Checklist include: LexisNexis Sanctions Risk Checklist, https://www.lexisnexis.com/community/cfs-file/__key/telligent-evolution-components-attachments/01-74-00-00-00-04-56-36/US_2D00_EDDM_2D00_Sanctions-Risk-Checklist-_2800_1_2900_.pdf; A Framework for OFAC Compliance Commitments, https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf

- [ ] Do you have an end-use/user statement and sanctions clause built into your sales contracts?
- [ ] Can you verify whether the end user and its ultimate beneficiary are subject to sanctions?

- [ ] Does your firm know the transaction?
  - [ ] Is this an allowable transaction under sanctions and export control requirements?
  - [ ] Are there any sanctions applicable to the location of the delivery?
  - [ ] Will third parties, such as agents acting on your company's behalf or transporters moving your products, be involved in the transaction?

III. Internal Controls

- [ ] Does your firm have written policies and procedures outlining the SCP?
  Has your firm clearly communicated the SCP's policies and procedures to staff?

IV. Testing and Auditing

- [ ] Does your firm have a process to test and audit SCP policies and procedures?

V. Training

- [ ] Does your firm provide training to employees and stakeholders on sanctions compliance?