

**Preventing Illicit Transactions Related to Advanced  
Conventional Weapon (ACW) Systems:  
An Operational Manual (2024)**



2024



---

Preventing Illicit Transactions Related to Advanced  
Conventional Weapon (ACW) Systems:  
An Operational Manual (2024)

**Authors:**

Bethany Banks, Sadiga Mehdiyeva

**Contributors:**

Giorgi Gogvadze, 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. This document is produced in collaboration with the Institute for Development and Democracy (IDD). Center for Strategy and Development extends its gratitude to IDD for their invaluable contributions to its creation.

The views and opinions expressed in the document belong to the Center for Strategy and Development (CSD) and do not necessarily reflect or represent the views and opinions of the U.S. Department of State.

# TABLE OF CONTENTS

<b>OVERVIEW</b>	<b>01</b>
<b>UNDERSTANDING OBLIGATIONS AND ACW</b>	<b>02</b>
ACW AND COMPONENTS	02
PROCUREMENT NETWORKS	03
OBJECTS OF PROLIFERATION	04
PATTERNS OF PROLIFERATION	05
<b>ACW-RELATED REQUIREMENTS IN AZERBAIJAN</b>	<b>06</b>
<b>OVERVIEW OF POLICY AND OBLIGATIONS</b>	<b>09</b>
▶ License and Permissions	09
▶ Control of import, export and transit shipments	10
▶ Control of Financial Transactions	12
▶ Application of International Sanctions	12
▶ Extraterritorial Application of Sanctions	13
<b>NATIONAL LAW REQUIREMENTS BY SECTORS</b>	<b>14</b>
▶ Arms Production, Volume, Procurement, Sales, and International Trade	14
▶ Shipping and logistics	15
▶ Financial Institutions	16
<b>IMPLEMENTING AN EFFECTIVE AND COMPLIANT RESPONSE TO SANCTIONS</b>	<b>18</b>
ACW-SPECIFIC SANCTIONS COMPLIANCE PROGRAMS IN AZERBAIJAN	18
TAILORING RISK ASSESSMENTS TO ACW	19
BEST PRACTICES FOR COMPLYING WITH SANCTIONS AND EXPORT CONTROL REGIMES	20
IDENTIFYING ACW TRANSACTIONS OF CONCERN	22
KEY TAKEAWAYS	24
<b>ANNEX A: RESOURCES FOR ADDITIONAL SUPPORT</b>	<b>25</b>
<b>ANNEX B: ADDITIONAL TRANSACTIONAL AND BEHAVIORAL RED FLAGS:</b>	<b>26</b>
<b>ANNEX C: TEMPLATE FOR ASSESSING ACW SANCTIONS COMPLIANCE PROGRAM</b>	<b>28</b>

# OVERVIEW



Over the course of the last decade, sanctions have increasingly become a tool used by countries and international organizations to target security threats, including non-state groups and state actors. Non-compliance with sanctions regimes is now one of the most significant risks posed to many private sector entities, particularly financial institutions, defense firms, transportation firms, and technology/electronics firms. While sanctions have long targeted transactions related to material associated with the development of weapons of mass destruction (WMD) (focused on, for example, North Korea and Iran), as well as transactions associated with terrorist organizations, the recent use of sanctions against Russia as a result of its 2022 invasion of Ukraine has significantly expanded the use of this tool to target a state’s advanced conventional weapons program, including its ability to acquire the components necessary for the production of those systems.

As a result of these developments, it has never been as important for private sector entities to ensure their compliance with sanctions regimes as they relate to advanced conventional weapons systems. The ability of a firm to quickly and accurately identify illicit transactions and take appropriate steps to address risk is critical to ensuring the ability of the firm to continue operations and avoid consequences. Given the significant consequences of noncompliance – include asset freezes, restricting exports, seizing property, and denying visa travel – the private sector and financial institutions need to be vigilant in their compliance with these regimes. The targets of sanctions are expansive, to include not only financial institutions and direct recipients, but also professional service providers, and any other third parties acting as intermediaries between the financial institution and clients. Beyond business risk, there are ethical and reputational considerations as well – there are significant, real-world consequences to states being able to evade sanctions.

This manual will be focused on providing operational awareness of specific ACW components and systems and sanctions regimes that seek to restrict the ability of proliferating states to access the components and transactions required to manufacture and distribute ACW.

# UNDERSTANDING OBLIGATIONS AND ACW

There are a number of existing bilateral and multilateral sanctions regimes in effect today, as well as bilateral and multilateral export control regimes, that impose obligations on private sector firms. Many prior sanctions regimes targeting weapons systems have focused exclusively on materiel required to produce WMD, such as the robust UN sanctions regimes targeting proliferation finance out of North Korea or, until recently, Iran. Russia's 2014 invasion of Crimea, followed by its expanded invasion of Ukraine in 2022, dramatically altered the sanctions landscape, including by imposing significant sanctions targeting individuals and entities engaged in transactions that support the production of advanced conventional weapons systems. Additional obligations include national-level export control regimes.

## ACW AND COMPONENTS

Advanced conventional weapons (ACW) represent a broad category of modern technological instruments designed for conventional warfare. While there not a universal definition, advanced conventional weapons may include, but are not limited to, man-portable air-defense systems (MANPADS), anti-tank guided missiles (ATGM), other major weapons systems and heavy military equipment (such as tanks, aircraft, and missiles), sensors and lasers, and precision guided munitions.<sup>1</sup> Increasingly, ACW may include lethal autonomous weapon systems (LAWS), such as unmanned aerial vehicles (UAV), unmanned ground vehicles (UGV), uncrewed surface vessels (USV), and uninhibited underwater systems (UUS). Ballistic and cruise missiles, which are usually considered delivery means of weapons of mass destruction (WMD), are increasingly used in conventional attack weapons.

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. Some components are clearly for military purposes, either due to the type of component or the grade, however there are many components that can be used to manufacture weapons systems that are dual-use, and may not initially appear to have a nefarious purpose. These present a challenge for firms attempting to identify illicit transactions related to the manufacture of weapons.

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

---

<sup>1</sup> Advanced Conventional Weapons, the U.S. Department of State, <https://2001-2009.state.gov/t/isn/acw/#:~:text=The%20U.S.%20strives%20to%20control,important%20in%20their%20development%20and> (archived).

TYPE OF COMPONENT	USAGE
Microelectronics/microchips	Communications equipment, UAS, precision long-range munitions
Semi-conductors	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



The pool of subjects (actors) involved in the proliferation of advanced conventional weapon components can include malicious actors, unwitting actors, and accomplices.

**Malicious actors** are states and/or non-state entities that are directly engaged in the process of proliferation on both of its supply and demand ends through the transfer or exchange of weapons, technologies, or related expertise.

**Accomplices** are networks, companies, or individuals who knowingly and willingly act as intermediaries and/or facilitators in the weapons transshipment chain and assist the malicious actors in circumventing control and sanctions regimes.

**Unwitting actors** are subjects of the international trade markets (such as transportation, logistics, and export-import companies, banks, and other institutions), which are engaged in the system of weapons-related transshipment and/or associated financial transactions without their awareness.

The activity of intermediaries aims at misleading the manufacturers of critical elements suitable for integration into ACW systems, making them unaware of the final destination of their merchandise (see Vignette 2). Another tactical pattern – the use of convoluted supply chains and multiple transshipment hubs (such as Hong Kong, Dubai, and many others) – adds further complexity to the mission of tracing, identifying, and preventing the illegal proliferation of advanced conventional weapons.

- ◆ In March 2024, the Russian TV footage from the “Kurganmashzavod” factory (a part of Rostec, the prime Russian defence industrial holding) exposed several Japanese precision machinery units inside the workshop.<sup>2</sup> This particular enterprise is the only Russian facility producing and refurbishing BMP-2/3 infantry fighting vehicles. Since Japan is a party to the sanctions regime, the displayed equipment was apparently procured via a third party, without knowledge of the tools’ manufacturers and exporters.

## OBJECTS OF PROLIFERATION

The material objects of the ACW proliferation encompass the following categories:

- ▶ **Lethal weapon systems;**
- ▶ **Peripheral non-lethal equipment** (e.g., radar, electronic warfare, communication, night vision, guidance, and navigation systems) that enhances the performance of lethal weaponry systems after being embedded in them (such as Starlink satellite communication systems that enable precise weapons targeting);
- ▶ **Expendables** (i.e., munitions, spare parts, and replaceable components);
- ▶ **Dual-use technological items** that allow the conversion of legacy weapons to modern ones;
- ▶ **Hi-tech machine tools** used for domestic production of ACW or its parts (such as computer-controlled machinery and 3-D printers); and
- ▶ **Knowledge (expertise) and software** used in reverse engineering and the development of ACW by end-users.

Shipments of “classical” weapons (such as tanks or artillery) are easier to control, as they have a defined physical signature, require considerable logistical efforts, and are thus easier to detect. Moreover, the states of concern have enough such legacy weapon systems, so they probably do not need them too much. Nonetheless, those systems are obsolete, and require service, maintenance, and modernization up to standards. That condition creates a critical prerequisite for obtaining spare parts, sophisticated augmenting nodes, and qualified expertise, which are essential for converting the available weapons into more effective warfighting assets. Furthermore, the mentioned objects can be used to stage their reverse engineering and production in domestic conditions.

---

<sup>2</sup> Angelica Evans, Grace Mappes, Christina Harward, Riley Bailey, and George Barros, “Russian Offensive Campaign Assessment, March 7, 2024, Institute for the Study of War, [https://www.iswresearch.org/2024/03/russian-offensive-campaign-assessment\\_7.html](https://www.iswresearch.org/2024/03/russian-offensive-campaign-assessment_7.html)



◆ In autumn 2022, Russia started to receive Iran-made Shahid-136 kamikaze drones (a.k.a. loitering munitions). The initial delivery batches included assembly kits, accompanied by technicians and instructors. In less than a year, the Russian side was able to establish the assembly facility in its territory,<sup>3</sup> train personnel, increase the output of manufactured drones (who go by the new designation Geran-2), and modernize them by replacing the inertial guidance system with satellite navigation and enhancing their maneuverability and endurance.

The particular augmenting components, which are less detectable and traceable for their size, are a key concern from the standpoint of ACW proliferation. This category includes such items as computer chips, semiconductors, integral electronic micro-schemes, fuses, infrared or thermal cameras and other night-vision sensors, optic equipment, satellite navigation tools, and other similar matters.

◆ The newest Shahid-238 loitering munition, first publicly displayed by Iran in November 2023, was tested by Russia in Ukraine as early as February 2024. The examined debris indicate that this weapon integrates components produced in the following Western countries: Czechia (turbojet engine), Canada (antenna receiver), USA (satellite navigation and microprocessor chips by Texas Instruments), and Switzerland (microcontroller and inertial navigation block).<sup>4</sup> Those particular components were apparently procured by Iran from the free commercial market through third parties and then assembled domestically before their shipment to Russia.

## PATTERNS OF PROLIFERATION

Generally, the ACW proliferation is developing along the following tracks:

- ▶ **Direct peer-to-peer transfer.** That is the case with the overt arms deliveries to Russia from Iran and North Korea in their alliance settings. In fact, such an exchange represents a “cascade” of critical technology, i.e., a situation in which actors share with others their previously illegally acquired Western-made items.
- ▶ **Covert transfer.** This pattern relates primarily to the clandestine smuggling of dual-use technological articles disguised as authorized civil export-import commodities with phony final destination points.

---

<sup>3</sup> David Albright, Sara Burkhard, and Victoria Cheng, “Drone Factory – No Show Day for Russia’s Drone Production,” Institute for Science and International Security, December 20, 2023, <https://isis-online.org/isis-reports/mobile/satellite-imagery-update-on-alabuga-shahed-136-drone-factory/>

<sup>4</sup> Povilas M., “New Shahed-238 Kamikaze Jet Drone Has Lots of Western Tech in It,” Technology.Org, February 12, 2024, <https://www.technology.org/2024/02/12/new-shahed-238-kamikaze-jet-drone-has-lots-of-western-tech-in-it/>

- **Domestic replication.** A way in which hardware and technological know-how (which is secured through two previous tracks) is integrated in the domestic defense industrial complex's production lines by means of reverse engineering, re-mastering, and additional modernization.
- **Uncontrolled migration.** A situation in which ACW items transferred by states to their particular proxy sub-state or non-state actors start to diffuse uncontrollably as the objects of arms trade.

The most likely case in the Caucasus is the procurement of ACW components through **third countries, known as transshipment hubs**. This poses a particular challenge because, often, microelectronics or other components are legitimately supplied to these organizations, and are then sent on to sanctioned end-users. Microelectronic third-party distributors and wholesalers often operate from intermediary jurisdictions, complicating the ability of firms to identify and avoid firms associated with sanctioned end users.

**Vignette 6:** In January 2024, the Russian military forces for the first time used in combat in Ukraine the North Korean KN-23/-24 intermediate-range ballistic missiles. An investigation by the Conflict Armament Research Group recovered and documented over 290 components of 50 unique types contained in those missiles.<sup>5</sup> Furthermore, the group has identified 26 enterprises established in eight national jurisdictions (China, Germany, Japan, the Netherlands, Singapore, Switzerland, Taiwan, and the USA). Seventy-five of the entire set of components were linked to U.S. companies. Three-thirds of the investigated items were manufactured between 2021 and 2023. This episode illustrates the scope and speed of trans-regional “cascading” of illegally acquired non-domestic technologies from a particular state to another one.



---



<sup>5</sup> “North Korean Missile Relies on Recent Electronic Components,” Ukraine Field Dispatch, Conflict Armament Research, February 2024, <https://storymaps.arcgis.com/stories/0814c6868bbd45a98b15693a31bd0e7f>



# ACW-Related Requirements in Azerbaijan

Azerbaijan's legislation emphasizes provisions, mechanisms, and requirements aimed at preventing the spread of weapons of mass destruction, though many requirements apply to dual use goods that are used in advanced conventional weapons. These measures significantly influence the development of national lists, incorporating sanctioned individuals and institutions identified by international organizations, alongside domestic judicial decisions.

According to the legal framework governing weapons in the country, they are classified into two main groups:

-  Items with limited civilian circulation, including military ammunition equipment, service weapons, civilian weapons, and drones. These items may be put into circulation through a special permit.
-  Items not allowed to be in civilian circulation, such as military equipment designed for combat purposes and prohibited weapons. These items do not participate in regular civilian circulation. Their handling and use are typically managed by specialized state agencies.

In national legislation, the legal regulation of weapon circulation, including advanced weapons, is managed through these legal instruments.

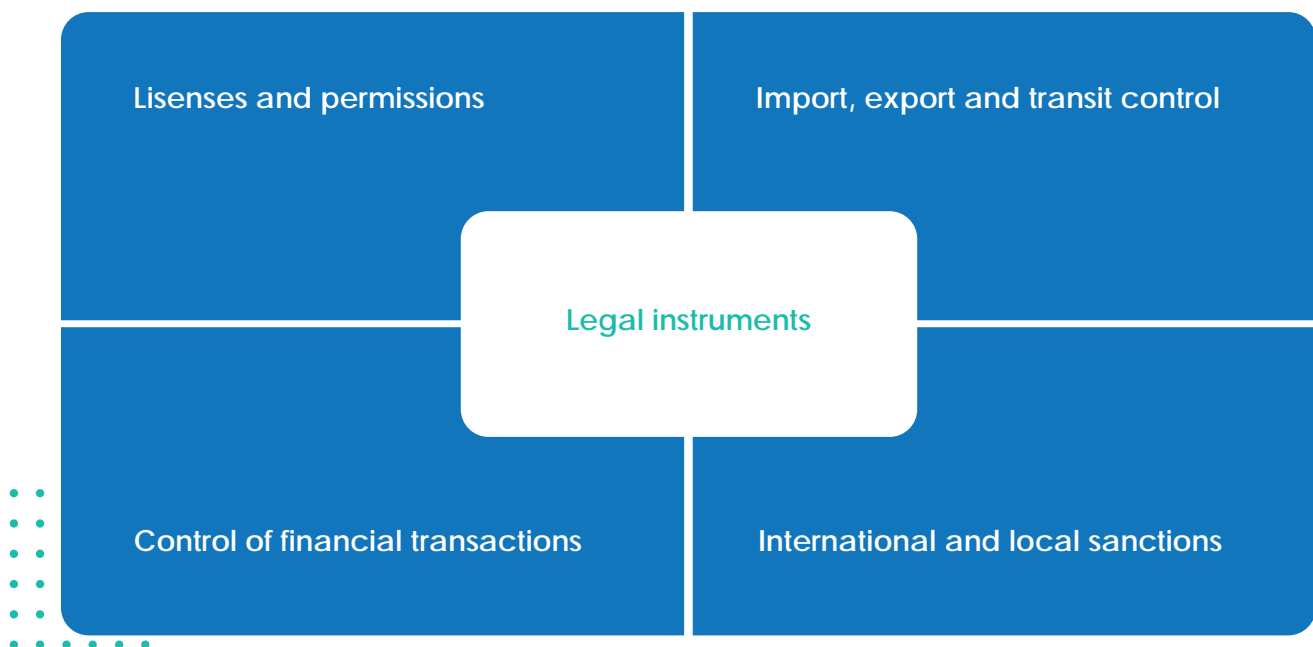


Figure 1. Key legal instruments to prevent illicit trafficking of Advanced Conventional Weapons

Permits and licenses are crucial legal tools for directly owning weapons and acquiring and distributing components needed for weapon production. For instance, individuals owning civilian or service weapons must obtain a special permit for items with restricted civilian circulation.<sup>6</sup> A similar type of permission is necessary for the circulation of dual-use goods, which can be broadly utilized in the development of advanced weapons. These dual-purpose goods are listed under export control according to national legislation requirements. Special permits are also mandatory for the export, re-export, import, re-import, and transit of all goods subject to export control.<sup>7</sup>

One of the most critical aspects of Advanced Conventional Weapons development involves dual-use goods. According to Azerbaijani legislation, items with dual purposes are subject to special customs scrutiny and [fall under the category of "goods subject to export control."](#) Consequently, [obtaining a special permit is mandatory for the circulation, export, and transit of dual-use goods.](#) These permits are categorized based on the parts and accessories directly utilized in weapon manufacturing. Depending on their classification, specific authorization types for the export and import of goods used in Advanced Conventional Weapons production are issued by the Cabinet of Ministers of the Azerbaijan Republic. The enforcement of these permits under specified conditions is overseen by various governmental bodies such as the Ministry of Defense, the Ministry of Defense Industry, the State Security Service, the Ministry of Energy, the Ministry of Internal Affairs, and the State Border, contingent upon the classification of the dual-use goods. Under this regulatory framework, the state has the authority to monitor not just the transportation of raw materials and dual-use goods suitable for weapon manufacturing, but also their final recipient and intended destination.

Also, organizations involved in the manufacturing of goods subject to export control or engaged in related activities are mandated to institute internal export control measures for these goods. Consequently, the organization's management is required to designate a specifically responsible individual to oversee such control. Furthermore, when these goods are either removed from the organization's operations or undergo upgrades, the organization must promptly notify the relevant state body responsible for export control.<sup>8</sup>

By overseeing financial transactions, the funding of illicit trade in advanced weapons and conducting such transactions in high-risk regions or with sanctioned entities and individuals can be deterred. This system, primarily built on anti-money laundering laws, mandates financial institutions and, sometimes, professionals like lawyers, auditors, and real estate agents, to carry out client due diligence processes.<sup>9</sup>

When it comes to sanctions in Azerbaijan, the sanctions enforced concerning the trafficking of illegal weapons and weapon components primarily derive from conventions and international agreements that the country has ratified or participated in. Consequently, national sanctions list typically do not encompass institutions and individuals subject to sanctions imposed by foreign countries on an individual basis.

---

<sup>6</sup> "On Licenses and Permits" Law, 15.03.2016, Annex 3, Clause 10

<sup>7</sup> "On Licenses and Permits" Law, 15.03.2016, Annex 3, Clause 9

<sup>8</sup> Export Control Regulations, 15.12.2005, CM Decision N230, art. 5

<sup>9</sup> Referencing the Law on Combating Money Laundering and Financing of Terrorism, Article 4



## OVERVIEW OF POLICY AND OBLIGATIONS

### License and Permissions

Azerbaijani legislation specifically regulates weapons, military equipment, and materials that can be utilized for military purposes. These are typically categorized into two distinct groups to ensure effective oversight and control. These categories are a) [goods with limited civilian circulation](#) and b) [goods barred from civilian circulation](#).

N	I.Goods with limited civilian circulation	II.Goods barred from civilian circulation
1.	Equipment for military weapons and ammunition	Combat military equipment
2.	Equipment for use of combat military equipment	Weapons and ammunition prohibited by law
3.	Service and civil arms	---
4.	Explosive materials and devices	---
5.	Remotely controlled drones	---

*Figure 2. Legal categories of weapons and military equipment*

Items classified under the first category are only permitted for civilian circulation upon the issuance of special permits. Conversely, the legislation of Azerbaijan does not provide for ordinary circulation or circulation with permission for items classified under the second category. Weapons falling within this category are subject to rigorous state control measures.

The purchase, sale, transportation, and other operations involving tools permitted for civilian circulation but capable of being used in the preparation of Advanced Conventional Weapons (ACW) are prohibited without obtaining a [special permit from the relevant state authorities](#).

N	Weapons and related goods	Authorities granting permission
1.	Equipment for the production of military weapons and ammunition	Ministry of Defence Industry
2.	Equipment for the production of combat military equipment	Ministry of Defence Industry
3.	Explosives materials and devices Inflammable substances and pyrotechnic products	Ministry of Emergency Situations
4.	Remotely controlled drones	Ministry of Digital Development and Transport
5.	Service and civil arms	Ministry of Internal Affairs

Figure 3. The list of authorities responsible for granting permission on weapons and related goods with limited civilian circulation.

The oversight of items capable of being used in the preparation of Advanced Conventional Weapons (ACW) is conducted by the authorities responsible for issuing the special permits. Inspections under this control framework occur annually and follow a predetermined schedule. The specific objects inspected by the supervisory authority are determined based on the level of risk associated with them.

In addition to regulating items categorized as weapons and goods intended for weapons purposes, Azerbaijani legislation also addresses dual-use goods under a distinct regulatory framework. This regulation primarily takes the form of permits for the export, re-export, import, re-import, and transit of dual-use goods.

### Control of import, export and transit shipments

In Azerbaijani legislation, the category of dual-use goods, which have the potential to be utilized in the preparation of Advanced Conventional Weapons (ACW), is subject to **special customs control**. These goods are encompassed within an extensive list and are closely monitored under the "export control" regime. The term "dual-use goods" refers to items used for civilian purposes but also capable of being employed in the development and preparation of weapons of mass destruction and their delivery systems, as well as other types of weapons, military equipment, and ammunition.

The provisions of this legislation extend beyond dual-use goods and instances facilitating the proliferation of other weapons. They also encompass scenarios where export operations and contracts pose a threat to **Azerbaijan's national security and interests**. Consequently, this broadens the application of the law and introduces a degree of ambiguity.

The control of operations involving dual-use goods in accordance with legislative requirements can be delineated into two stages:

1. Conducting inspections during the issuance of permits for goods subject to export control;
2. Supervising the utilization of goods during customs clearance, actual transportation, and final destination.

Government agencies that allow the circulation of dual use goods and agencies that control the subsequent actual movement and use of these goods operate in a related manner. Legislation has placed the control of dual use goods on **both groups of institutions**. Thus, the permitting agency monitors compliance with permit conditions, while the controlling agency monitors in other areas.

Category	Goods under export control	Permit granting authority	Controlling agency
6 6A	Receivers (sensors) and lasers: acoustics, optics, location systems, laser equipment	on export, import, re-export, re-import, transit: for military purposes - the Cabinet of Ministers of the Republic of Azerbaijan - on the basis of the opinions of relevant authorities	as relevant: Ministry of Defense of the Republic of Azerbaijan, Ministry of Defense Industry (as relevant), State Security Service, State Border Service
ML7	Toxic substances, tear gas, military reagents, precursors for the preparation of toxic substances	on export, import, re-export, re-import, transit: for military purposes - the Cabinet of Ministers of the Republic of Azerbaijan - on the basis of the opinions of relevant authorities	as relevant: Ministry of Defense of the Republic of Azerbaijan, Ministry of Defense Industry (as relevant), State Security Service, Ministry of Internal Affairs, State Border Service
ML8	"Additives" (substances used to improve the parameters of explosives) and precursors	on export, import, re-export, re-import: based on the opinions of the Ministry of Energy of the Republic of Azerbaijan, the Ministry of Defense Industry (relevant) - the Ministry of Health, the Ministry of Ecology and Natural Resources; in transit: Based on the opinions of the Ministry of Digital Development and Transport, Ministry of Health, Ministry of Ecology and Natural Resources	Ministry of Energy, Ministry of Defense Industry of the Republic of Azerbaijan (as applicable)  Ministry of Digital Development and Transport of the Republic of Azerbaijan
PL5002; PL5006; ML5; ML6; PL5031	Fire-controlling military devices, telescopic sights, ground vehicles for military purposes	on export, import, re-export, re-import transit: Based on the opinions of the Cabinet of Ministers of the Republic of Azerbaijan-relevant State bodies	as relevant: Ministry of Defense of the Republic of Azerbaijan, Ministry of Defense Industry (as relevant), State Security Service, Ministry of Internal Affairs, State Border Service, Security Service of the President of the Republic of Azerbaijan

Figure 4. List of institutions for monitoring the circulation and use of exemplary dual-purpose goods.

It's important to note that the information gathered during the authorization process is typically utilized during the subsequent control procedures. This information encompasses details regarding the customer and the end user involved in the transaction.

### Control of Financial Transactions

In addition to direct legal measures aimed at preventing the illicit circulation of weapons and weapon parts, Azerbaijani legislation also incorporates financial instruments for this purpose. The [primary legal instrument](#) in this regard is legislation targeting the combating of money laundering and the financing of terrorism. Accordingly, entities categorized within the special risk group are required to conduct specific inspection measures concerning clients and financial sources during the execution of various financial transactions, as well as the provision of legal, tax, audit, and real estate services, in accordance with the requirements of this legislation.

As per the requirements of this legislation, participants mandated to conduct inspection measures are categorized into two groups: a) financial institutions and b) non-financial institutions. Financial institutions, including banks, insurers, investment funds, and others, are subject to stricter regulations governing their activities. Alongside measures for identifying and verifying potential customers, Azerbaijani legislation introduces the [concept of "high-risk zones"](#) as a means of preventing illegal economic activities.

In this legislation, "high-risk zones" are identified as areas lacking adequate measures to combat illicit activities, supporting armed separatism, extremism, mercenary and terrorist actions, and where there is no requirement for disclosing identification information and documents during financial transactions. Additionally, these zones may be subject to sanctions or similar measures by international organizations, states, or territories. The list of such areas is established based on reports submitted by international organizations.

Furthermore, the Azerbaijani government reserves the authority to impose restrictions and special requirements within high-risk zones, based on recommendations from the Financial Action Task Force (FATF).

### Application of International Sanctions

Azerbaijan has recently implemented dedicated legislation on targeted financial sanctions. In accordance with this legislation, the Financial Monitoring Service periodically publishes a publicly accessible online list of companies and individuals subject to international sanctions applied by Azerbaijan at the national level. These sanctions primarily focus on two main directions:



Sanctions arising from international agreements to which Azerbaijan is a party, as well as those determined based on specific decisions of the UN Security Council;





Sanctions applied to individuals and institutions deemed necessary to be sanctioned within the framework of combating terrorism and terrorist financing, as decreed by the courts of the Republic of Azerbaijan.

While the list of sanctions doesn't directly target Advanced Conventional Weapons (ACW), it poses a significant barrier to illegal activities that may involve such weapons, including the transportation of dual-use goods. The Financial Monitoring Service publicly discloses the names of [sanctioned individuals and companies online](#). Additionally, the online resource provides a list of high-risk zones based on statements provided by the Financial Action Task Force (FATF). For instance, the latest list, updated on February 24, 2024, includes the [Democratic People's Republic of Korea, Iran, and Myanmar among the high-risk areas](#). The periodic publication of this list of risky jurisdictions aids business entities in conducting their economic activities with greater caution, safeguarding them from potential inclusion in future international sanctions lists.

Azerbaijan primarily acknowledges and enforces sanctions imposed by international organizations as part of its commitments under the international agreements it has ratified.

### Extraterritorial Application of Sanctions

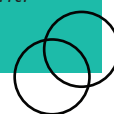
Definition: Extraterritoriality refers to the enforcement of domestic laws, even when the activity took place in another country. Typically, U.S. sanctions can be enforced extraterritorially – meaning if the transactions includes U.S. persons, financial institutions, territory, or infrastructure, companies or individuals are subject to U.S. sanctions.

Azerbaijan Context: Even though Azerbaijan is not a part to all international sanctions regimes focused, U.S. enforcement authorities, particularly OFAC, can and do enforce U.S. sanctions against foreign companies and individuals. If an Azerbaijani company ships machine tool parts to Russia's defense industrial sector, that Azerbaijani company is putting itself at risk of secondary sanctions by OFAC. The penalties for that transaction are severe – that could mean getting blocked from the U.S. and European financial system and other penalties like fines and/or restrictions. Azerbaijani companies should review [this guidance](#) to understand how U.S. sanctions and export control laws are applies to host non-U.S. persons accountable for violations, as well as how international companies can mitigate the risks of non-compliance.

*Case Study: In March 2024, the U.S. released a notice on Obligations of foreign-based persons to comply with U.S. sanctions and export control laws that included the below case study:*



*In December 2023, DOJ unsealed an indictment charging one Iran-based person and an individual based in China and Hong Kong for conspiring to illegally purchase and export from the United States to Iran dual-use microelectronics commonly used in UAV production.<sup>25</sup> To obtain the products, the defendants allegedly caused Canadian and French companies to place orders with U.S. manufacturers, causing the items to be shipped first to either Canada and France and then to Hong Kong and China, where they were reexported to Iranian end users. <sup>26</sup> The defendants allegedly provided false and misleading information about the ultimate end use and true identities of the end users to the U.S. manufacturers.*



## Arms Production, Volume, Procurement, Sales, and International Trade

The Ministry of Defense Industry in Azerbaijan is the primary institution responsible for overseeing the production and distribution of weapons within the country. It plays a crucial role in preparing the State Defense Order Program, which addresses the nation's essential requirements for defense and weapon supply.<sup>10</sup> The Ministry of Defense Industry in Azerbaijan operates a total of 23 production and research facilities with diverse purposes. These facilities are involved in manufacturing electronic products, and some also produce equipment that serves as components for weapons or military applications.

N	Manufacturing/research facility	Scope of operations
1	"Iglim Science-Production Enterprise" LLC	<ul style="list-style-type: none"> <li>▶ Developing and preparing airfield equipment for aviation operations;</li> <li>▶ Manufacturing tools and technological equipment for various purposes.</li> </ul>
2	Factory of Electronic Computing Machines LLC	<ul style="list-style-type: none"> <li>▶ Manufacturing electronic devices and gadgets;</li> <li>▶ Producing industrial and household appliances;</li> <li>▶ Crafting electromechanical and mechanical devices.</li> </ul>
3	"Avia-Agregate Plant LLC"	<ul style="list-style-type: none"> <li>▶ Manufacturing high-pressure balloons and cylindrical balloons;</li> <li>▶ Producing aircraft and kitchen equipment for civilian aviation;</li> <li>▶ Developing technological designs and tools.</li> </ul>
4	"Ganja Machine Building Plant" LLC	Manufacturing specialized and civilian products
5	Tarter Electromechanics Plant	Manufacturing technical products
6	Industrial Equipment Scientific-Production Enterprise	Manufacturing flow meters, counters, dispensers, and alarms with a broad range of capabilities in flow and pressure, suitable for various liquids including aggressive substances.
7	Radio assembly plant LLC	Manufacturing televisions, electronic cash registers, and electronic scales
8	Radio assembly plant LLC	<ul style="list-style-type: none"> <li>▶ Designing, enhancing, and manufacturing defense products;</li> <li>▶ Producing linear track equipment for multi-channel communication systems, alongside technical products and consumer goods.</li> </ul>

<sup>10</sup> Article 7.3 of the Statute

9	Telemechanika Factory LLC	Manufacturing devices for the oil industry
10	Sharur Radio Factory LLC	Manufacturing both defense and civilian products
11	Azon Plant LLC	<ul style="list-style-type: none"> <li>▶ Manufacturing various types of microcircuits;</li> <li>▶ Producing mechanical parts for the oil industry; Manufacturing liquid nitrogen and oxygen.</li> </ul>
12	Dalga Scientific-Production Enterprise	<ul style="list-style-type: none"> <li>▶ Designing and manufacturing marine navigation systems;</li> <li>▶ Developing and producing specialized navigation, communication, and information processing systems.</li> </ul>

Figure 5. Selected production and research facilities under the Ministry of Defense Industry.

The export and import of weapons to foreign countries for defense purposes by the state are classified as state secrets under specific conditions and are not permitted to be publicly disclosed.

### Shipping and logistics

In postal and courier services, a key focus of national legislation is the oversight of financial transactions. According to national regulations, postal services are permitted to conduct financial transactions provided they obtain a [special license from the Central Bank](#). The terms of this license directly dictate the main limitations imposed on such activities. The postal service conducts the following financial operations as authorized by its license.

- ▶▶ Opening and maintaining postal accounts;
- ▶▶ Conducting money transfers;
- ▶▶ Opening correspondent accounts in financial institutions, including the Central Bank of the Republic of Azerbaijan;
- ▶▶ Accepting postal deposits;
- ▶▶ Providing payment services, organizing payment systems, issuing postal checks;
- ▶▶ Conducting currency exchange operations based at the customers' orders and funds;
- ▶▶ Collection of cash and other valuables. (Law on Post 29.06.2004, N714-IIQ, article 13-1)

Post offices engaged in financial transactions must adhere to the requirements outlined in anti-money laundering (AML) and targeted financial sanctions legislation. Non-compliance with these requirements may lead to restrictions on the activities of the postal service, revocation of the license, and individual penalties applied to post office officials. Sending all military items, weapons, and weapon parts to and from Azerbaijan via postal services is **strictly prohibited**. Similarly, transporting these items through the territory of Azerbaijan in transit via postal services is also prohibited.

Several dual-use goods utilized by companies involved in transportation activities, along with materials applicable in the preparation of Advanced Conventional Weapons (ACW) and its components, such as explosives, fall under the category of dangerous goods. Special permits are mandated for such activities, encompassing the collection, storage, and direct transportation of these goods. These permits facilitate control over the volume, environmental impact, movement, and transit of dangerous goods. Additionally, legislation has instituted specific regulations governing the transportation of these goods via road, sea, air, and railways.

### **Financial Institutions**

While there isn't a specific legislative or political document directly addressing the illegal circulation of Advanced Conventional Weapons (ACW) within financial transactions in Azerbaijan, certain legislative acts and mechanisms indirectly include measures to prevent such illegal activities. Generally, legislation aimed at preventing financial institutions from participating in the illegal circulation of ACW and weapon parts, as well as preventing the diversion of financial resources in this direction, can be categorized into two main directions:

#### ***Preventive measures.***

Preventive measures are primarily governed by **Anti-Money Laundering (AML)** legislation, which imposes various requirements on financial institutions to deter money laundering and terrorist financing. These requirements encompass standard and, in certain instances, enhanced customer due diligence procedures. For instance, individuals from territories identified as high-risk zones by the financial monitoring authority, as well as companies registered in these zones, along with their bank accounts and suppliers, are subjected to heightened customer due diligence procedures. As a preventive measure, financial institutions are required to establish an **internal control system** aimed at preventing suspicious financial transactions.

#### ***Sanctions lists.***

As mandated by national legislation, Azerbaijan publishes a list of individuals and institutions subjected to targeted financial sanctions to comply with its international obligations. The lists cover Azerbaijan's obligations in the following areas:

- ▶ Combating terrorism and terrorist financing;
- ▶ Combating the proliferation and proliferation financing of weapons of mass destruction;
- ▶ Individuals and institutions identified by the local executive authority for sanctions in accordance with resolutions of the UN Security Council.

It's important to note that the scope of combating the proliferation and financing of weapons of mass destruction extends beyond the direct production of nuclear, chemical, and biological weapons. It also encompasses their means of delivery, remotely operated combat vehicles, and dual-use goods. Considering the significant role played by remotely operated weapons and dual-use goods in the development of Advanced Conventional Weapons (ACW), it can be inferred that targeted financial sanctions help mitigate the illicit circulation of ACW weapons, at least to some extent.

The mechanism of targeted financial sanctions involves actions such as freezing assets and prohibiting the provision of economic resources or financial services to individuals and entities listed in the sanctions. The database of sanctioned persons in the Republic of Azerbaijan is publicly published on the page <https://www.fiu.az/en>



# 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 take seriously the risk posed by non-compliance with sanctions or export control regimes. The rapid expansion of enforcement mechanisms now forces all businesses, regardless of sectors, to consider risk posed by sanctions enforcement if they lack a sufficient compliance regime. Some types of firms, such as logistics, finance and goods manufacturers, are more vulnerable than others. Because proliferating states rely 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 activity. Firms that produce high-specification goods and that are prone to being targeted by illicit procurement are often small and medium-sized enterprises. Though many firms, particularly in the financial services and banking sector, likely 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 AZERBAIJAN

There are multiple types of firms that need to have in place effective sanctions compliance programs, including:

- ▶ **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 an exporting, providing capital loans, and issuing or paying insuring on shipping and delivery of goods. **In Azerbaijan, this includes commercial and electronic banks, credit card operators, and foreign exchange dealers.**
- ▶ **Electronics firms:** Electronics exporters and resellers face particular challenges with 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 the majority of business likely comprises off-the-shelf components. A key part of preventing illicit sales is understanding the end user, which is difficult with so many changing customers. Compliance is easier for firms that specialize in particularly sensitive electronics, such as those for the defense sector, because they tend to have more limited, repeat customers. **In Azerbaijan, this type of firm includes importers and exporters of electronics and other technology.**

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

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 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:

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

## TAILORING RISK ASSESSMENTS TO ACW

A risk assessment allows organizations to set priorities and processes in order to understand exposure to ACW and sanctions related risk, and 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 a risk assessment will be applicable to all types of firms, but it is unlikely that a firm can meet its sanctions-related obligations without a fulsome understanding of its exposure to risk.

Risk assessments are a product that identifies, analyzes, and understands sanctions risk, with a view to mitigating that risk. Risk assessments should have a broad scope and should include assessment of:

- ▶ customer risk;
- ▶ product and services risk;
- ▶ geography (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 risk associated with money laundering (AML) or terrorist financing (CTF), many of which can be adapted to address risk related to ACW and sanctions. Some firms may also have risk assessments related to proliferation finance, a subset of financial crime focused on violations of UN Security Council resolutions aimed at countering acquisition of weapons of mass destruction and associated materials.

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.
- 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 SANCTIONS AND EXPORT CONTROL REGIMES

Developing a compliance program that can detect illicit transactions associated with ACW can be challenging, due to the multi-tier visibility of goods and transactions required, including in origin, transit, and destination countries. There are, however, some clear best practices that firms, both financial institutions and others, can implement that will put a firm in a good position to detect transactions and prove to enforcement authorities that that are attempting to 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 in order for this system to be effective. Ultimately, a firm's risk assessment should inform how a screening solution is utilized and what is screened and when.



**Due Diligence (Know Your Customer/Supplier):** Firms should ensure due-diligence checks are carried out on potential customers, business partners, and goods utilizing public information such as early warning lists, red-flag checklists, and questionnaires. A basic requirement for a sanctions compliance program is to be clear on the ownership and control structure of the organization. To detect the complicate networks associated with ACW components, due diligence may need to extend beyond immediate customers to also consider your clients' clients. Increasingly, sanctions enforcement agencies also expect firms to know about compliance risks posed by their suppliers and ensure that processes 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 uses.

Customs officials have developed a useful list of **behavioral red flags for customer interactions** in proliferation finance that can be applied to screening of customers with risk associated with ACW transactions. Red flags can 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 his address is similar to one of the parties listed in 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.

**List-Based Screening:** Conducting sanctions screening is the major way financial services firms can ensure it is not engaging in transactions that are subject to a sanctions regime. List-based screening can often be automated and can be useful in identifying suspicious transactions. However, there are limits to this approach. Few of these lists are designed for exporters rather than financial firms, and lists are often updated infrequently. They can also give a fall 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, investigating known networks.

**Internal policies:** Firms should also clarify policy on maintaining relationships with certain banks or businesses and determine extent to which organization operates in high-risk jurisdictions.

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

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

- Including questions relevant to sanctions and conventional weapons/components in their due diligence process – whether at the on-boarding stage or over the course of the client relationship.
- Ensuring that the due diligence procedures of their clients, particularly those involved in the manufacturing and trade of defense or related items, is comprehensive, ensuring the client has a clear idea of who they are trading with and the potential end-use of their products.
- Investigating weapons and components networks – and specific clients ties to those networks – to reveal and possible connection with the firm.

## IDENTIFYING ACW TRANSACTIONS OF CONCERN

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

According to BIS/FINCEN , 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 its customer (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 sanctioned end users.
- ▶ 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 sanctioned end users.
- ▶ Transactions identified through correspondent banking activities connected to firms that resell electronics and other similar items to sanctioned firms.
- ▶ 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 sanctioned end users.
- ▶ Delivery dates are vague, or deliveries are planned for out of the way destinations.
- ▶ The product’s capabilities do not fit the buyer’s line of business (for example, an order for sophisticated computers for a small bakery).
- ▶ The ordered product is incompatible with the technical level of the country it is being shipped to (for example, semi-conductor 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.

Illicit transactions may also occur by intentionally misidentifying controlled items as “EAR99” items, which generally includes consumer goods that don’t 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 a fulsome understanding of its exposure to risk, which should be outlined in a **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.



## ANNEX A: RESOURCES FOR ADDITIONAL SUPPORT

---

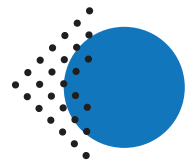
- ◆ **OFAC List of Specially Designated Nationals and Blocked Persons (SDN List):** OFAC publishes lists of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries.
- ◆ **Bureau of Industry and Security (BIS) at U.S. Department of Commerce Entity List:** The 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, kept under constant review and is subject to periodic renewals 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.



## ANNEX B: ADDITIONAL TRANSACTIONAL AND BEHAVIORAL RED FLAGS:

- ◆ A customer transports commodities of concern and uses trade corridors known to serve as possible transshipment points for exports to a sanctioned end user.
- ◆ The nature of a customer’s underlying business (specifically military or government-related work), type of service(s) or product(s) offered.
- ◆ Transactions involving entities with little to no web presence.
- ◆ Transactions involving a change in shipments or payments that were previously scheduled to go to a sanctioned end user, or a company located in a sanctioned end user, but that 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 a sanctioned end user.
- ◆ Last-minute changes to transactions associated with an originator or beneficiary located in a sanctioned end user.
- ◆ 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 transshipment hubs.
- ◆ Transactions associated with atypical shipping routes for a product and destination.
- ◆ Transactions involving entities whose website or business registration states the entities work on “special purpose projects.”
- ◆ Transactions involving companies that are physically co-located with 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.

- ◆ 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 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 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 a sanctioned end users.
- ◆ Transactions identified through correspondent banking activities connected to petroleum-related firms or firms that resell electronics and other similar items to a sanctioned firms.



# ANNEX C: Template for Assessing ACW Sanctions Compliance Program

## 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?
- 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 sanctioned?
  - Is the country a known facilitator for a sanctioned end user?
- 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?



- 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?



