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

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

Authors:
Bethany Banks, Sadiga Mehdiyeva

Contributors:
Giorgi Goguadze, Tamar Nadibaidze, Nikoloz Kipshidze

2025

About this Document

The views and opinions expressed in the document belong to the authors and do not necessarily reflect or represent the views of the Center of Strategy and Development (CSD)

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

Table of Contents

OVERVIEW

Over the course of the last decade, sanctions have increasingly become a tool used to target security threats, including both non-state groups and state actors. Non-compliance with sanctions regimes is now a signifcant risk for many private sector entities, particularly fnancial institutions, defense frms, transportation frms, and technology/electronics frms.

Over the past six months, sanctions enforcement related to advanced conventional weapons (ACW) components has **escalated, particularly in response to the activities of Russia, Iran, and North Korea.** These developments demonstrate the evolving nature of procurement networks and the increasingly strategic use of sanctions to disrupt ACW-related military cooperation among sanctioned states. The focus has expanded from purely targeting weapons systems to also disrupting access to critical dual-use components and technologies.

Russia . Sanctions against Russia remain sharply focused on its military-industrial base, especially following the 2022 invasion of Ukraine. Enforcement actions have increasingly targeted importers, producers, and third-country enablers supplying dual-use items such as microelectronics, engines, and precision manufacturing tools. The European Union (EU) and the United States have broadened controls to cover both sophisticated and lower-tech items that can support Russia's military. Despite efforts to accelerate domestic defense production, Russia continues to face major challenges including quality control issues and delays, with reports suggesting shortages of equipment.

Iran. Sanctions on Iran have primarily focused on its ballistic missile program and the proliferation of UAVs and missile systems to proxies and partners. Iranian manufacturers have been the subject of sanctions for their role in producing UAVs now categorized as advanced conventional weapons. Sanctions also aim to destabilize Iran's military-industrial complex by disrupting its access to missile and UAV components.

North Korea. North Korea remains one of the most heavily sanctioned states, subject to a comprehensive UN arms embargo that prohibits the export and import of all conventional arms, and restricts access to dual-use goods, technologies, and fnancial resources that could support its military programs. Over the past six months, renewed attention has been placed on North Korea's role in proliferating advanced conventional weapons, particularly through covert arms transfers and the development of ballistic and cruise missiles increasingly used in conventional warfare. Initial reporting from the Multilateral Sanctions Monitoring Team (MSMT) has confrmed the scale and scope of North Korea's ACW-related activity, reinforcing the need for vigilant compliance by private sector actors.

In 2024, two major **developments reshaped Azerbaijan's foreign policy landscape** in ways that may infuence its approach to sanctions enforcement. First, Azerbaijan formally reopened its embassy in Iran, signaling a diplomatic thaw after a period of heightened tensions. Second, in December 2024, an Azerbaijani passenger plane was downed, with Azerbaijan alleging that the aircraft was struck by a Russian air defense missile. This incident severely strained bilateral relations.

This manual will be focused on **providing operational awareness** of specifc 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. To navigate the evolving and complex landscape of ACW-related sanctions and export controls, organizations should implement dynamic compliance programs that incorporate regular risk assessments, staff training, and updated screening tools aligned with international best practices.

UNDERSTANDING OBLIGATIONS AND ACW

A range of bilateral and multilateral sanctions and export control regimes currently impose legal and operational obligations on private sector entities. Historically, these regimes have concentrated on restricting the proliferation of weapons of mass destruction (WMD), as seen in the extensive UN sanctions frameworks addressing North Korean proliferation fnance and, more recently, Iranian missile and nuclear activity. However, the global sanctions environment has evolved signifcantly as a result of Russia's military action in Ukraine, prompting the international community to broaden sanctions to encompass individuals, entities, and networks supporting the development, production, and procurement of advanced conventional weapons (ACW). In parallel, national export control laws have expanded to refect these shifts, creating layered and dynamic compliance obligations for frms engaged in sensitive sectors or operating across jurisdictions.

ACW and components

Advanced conventional weapons comprise a diverse array of technologically sophisticated systems. While no single defnition is universally accepted, ACW are generally understood to include man-portable air-defense systems (MANPADS), anti-tank guided missiles (ATGMs), major weapons platforms such as tanks, aircraft, and missile systems, as well as supporting technologies including sensors, lasers, and precision-guided munitions. Emerging categories of ACW include lethal autonomous weapon systems (LAWS), such as unmanned aerial vehicles (UAVs), unmanned ground vehicles (UGVs), uncrewed surface vessels (USVs), and uncrewed underwater systems (UUSs). Ballistic and cruise missiles – though traditionally classifed as delivery vehicles for weapons of mass destruction – are increasingly deployed in conventional operations and are thus considered within the ACW landscape.

For most frms, the greater compliance challenge lies not in handling complete weapons systems, but in identifying and controlling the transfer of the components that make up ACWs. While certain items are clearly designed for military applications, many others are dual-use in nature. These dual-use components, particularly when embedded within broader procurement or shipping transactions, pose a signifcant detection risk and underscore the need for robust due diligence and end-use verifcation protocols.

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

Type of component	Usage
Microelectronics/microchips	Communications equipment, UAS, precision long-range munitions
Semi-conductors	Defense-related components (computers, sensors, switches, amplifers)
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

Procurement Networks

The network of actors involved in the proliferation of ACW components typically includes three categories: deliberate proliferators, complicit intermediaries, and unwitting participants.

Deliberate proliferators are state or non-state entities actively engaged in acquiring, developing, or distributing ACW-related materials and technologies. **Complicit intermediaries** knowingly facilitate these efforts, often by providing logistical, fnancial, or technical support to evade sanctions and export controls. **Unwitting participants** – such as manufacturers, freight forwarders, fnancial institutions, and other service providers – may inadvertently contribute to proliferation by failing to detect the true end use or end user of a transaction due to deceptive practices or inadequate compliance protocols.

Some intermediaries mislead the manufacturers of ACW components, making them unaware of the fnal destination of their merchandise. Another 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.

Vignette: On January 16, 2025, the Offce of Foreign Asset Control (OFAC) sanctioned Abdel Fattah Al-Burhan, the leader of the Sudanese Armed Forces (SAF), and others for actions that contributed to the escalation of confict in Sudan. Among those designated was Ahmad Abdalla, a dual Sudanese-Ukrainian national, who coordinated the acquisition of Iranian-made unmanned aerial vehicles (UAVs) through an Azerbaijani defense supplier. According to the U.S. Treasury, the UAVs were intended for use by the SAF in ongoing military operations, and the procurement involved multiple transshipment points and false end-user documentation to conceal their origin and destination. [1]

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 legacy or "classical" weapons systems - such as tanks, artillery, or other heavy military equipment - are comparatively easier to identify and interdict due to their distinct physical characteristics, logistical complexity, and visibility within international transportation channels. Many sanctioned states maintain existing stockpiles of such systems and may not require additional platforms in large numbers. However, these legacy systems are often outdated and

[1] https://home.treasury.gov/news/press-releases/jy2789

require signifcant upgrades to remain operationally effective. This creates a persistent demand for spare parts, advanced subsystems, and specialized technical expertise necessary for maintenance, modernization, and adaptation to contemporary battlefeld requirements. In many cases, these components and technologies form the foundation for reverse engineering efforts aimed at enabling domestic production, further complicating efforts to disrupt proliferation.

The 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.

Vignette: In November 2024, investigative reports from Reuters revealed that ballistic missiles manufactured by North Korea and used by Russia in Ukraine contained numerous components sourced from U.S. and European companies. Analysis of missile debris from a January 2 attack indicated that approximately 75% of the electronic components were tied to U.S.-based frms. These fndings underscore North Korea's reliance on foreign-sourced materials and components for its weapons programs, despite existing U.N. sanctions prohibiting such transfers. The components were covertly procured through a network of overseas agents and foreign companies, which repackaged and shipped them to North Korea while concealing the actual end-use from manufacturers. [2] [3]

Patterns of Proliferation

Generally, ACW proliferation is developing along the following tracks:

- **Direct peer-to-peer transfer.** This refers to overt arms shipments between allied states, such as deliveries from Iran and North Korea to Russia. Such exchanges represent 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 fnal destination points.
- **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 frms to identify and avoid frms associated with sanctioned end users.

[2] https://www.reuters.com/world/debris-north-korean-missile-ukraine-could-expose-procurement-networks-2024-02-22/?utm

[3] https://apnews.com/article/un-north-korea-ukraine-ballistic-missiles-e917b0eb55fd7489532c33d982731ff0

Vignette: In early 2025, the U.S. Department of the Treasury announced enforcement actions involving a transshipment scheme designed to obscure the Iranian origin of restricted goods. The case centered on the export of Iranian high-density polyethylene (HDPE), which is a dual-use material, through intermediaries in the UAE, which served as a transshipment hub to redirect goods to international markets. The operation used falsifed documentation and misdeclared origin information to evade detection. This example underscores the risks posed by seemingly legitimate commercial activity in intermediary jurisdictions and the importance of robust origin verifcation and counterparty due diligence in high-risk geographies. [4]

[4] https://ofac.treasury.gov/media/932841/download?inline

Azerbaijan's Legal and Regulatory Framework on ACW and Dual-Use Goods

Azerbaijan's approach to regulating advanced conventional weapons (ACW) components and dual-use goods is shaped by a combination of national laws and international standards. While Azerbaijan is not a party to all global sanctions or export control regimes, it has adopted domestic legislation that refects many of their core principles. These laws aim to prevent the proliferation of weapons of mass destruction (WMD), restrict access to sensitive goods and technologies, and enforce controls through permits, licenses, and institutional oversight.

National regulations defne categories of weapons and dual-use goods, establishing which may be circulated with special authorization and which are entirely prohibited from civilian use. Export control laws also impose licensing requirements on the import, export, and transit of goods that could be used in the development of ACW. Oversight responsibilities are distributed across several government bodies, depending on the classifcation of the goods involved.

In addition to controlling physical movement, Azerbaijan mandates internal compliance measures for companies and organizations engaged in the production or handling of controlled goods. These measures include notifying relevant authorities when such goods are modifed, retired, or otherwise removed from use.

Overall, Azerbaijan's legal and institutional framework integrates elements of sanctions enforcement, export control, and fnancial monitoring to address risks associated with the circulation and misuse of advanced weapons and dual-use items.

In Azerbaijan, sanctions related to the traffcking of illegal weapons and weapon components are primarily based on international conventions and agreements that Azerbaijan has ratifed or joined. As a result, national sanctions lists generally do not include individuals or institutions targeted by unilateral sanctions imposed by foreign countries.

Recently Azerbaijan amended its regulations on the cross-border transportation of currency to strengthen safeguards against illicit fnance and proliferation. The revised rules clearly defne when customs offcials may suspend transfers, including cases involving undeclared funds, suspected money laundering, or links to high-risk jurisdictions. Risk-based criteria include refusal to disclose the source or purpose of funds, submission of false documentation, and travel to or from sanctioned regions. These reforms are part of a broader National Action Plan to improve enforcement against terrorism fnancing and the proliferation of weapons of mass destruction. They are supported by new institutional guidance and practitioner tools aimed at enhancing transparency and oversight.

License and Permissions

Azerbaijani legislation specifcally 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 1. Legal categories of weapons and military equipment

Items classifed under the frst 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 classifed 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	I. 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 Infammable 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 2. The list of authorities responsible for granting permission on weapons and related goods with limited civilian circulation.

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 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.

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

01. Conducting inspections during the issuance of permits for goods subject to export control;

02. Supervising the utilization of goods during customs clearance, actual transportation, and fnal destination.

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, 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 3. List of institutions for monitoring the circulation and use of exemplary dual-purpose goods.

Control of Financial Transactions

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

Per the requirements of this legislation, participants mandated to conduct inspection measures are categorized into two groups: a) fnancial institutions and b) non-fnancial 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 identifed 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 identifcation information and documents during fnancial transactions. Additionally, these zones may be subject to sanctions or similar measures by international organizations, states, or territories.

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).

Vignette: In February 2025, OFAC designated six entities in China and Hong Kong and two individuals in China and the UAE for their involvement in an Iranian UAV component procurement network. According to the U.S. Treasury, these parties supplied critical components to Pishtazan Kavosh Gostar Boshra and its subsidiary Narin Sepehr Mobin Isatis, which are under U.S. sanctions, to support Iran's drone and missile programs. The network used third-country suppliers and front companies to hide the origin of parts and evade export controls and sanctions. [5]

Application of International Sanctions

Azerbaijan has recently adopted dedicated legislation on the implementation of targeted fnancial sanctions. Under this framework, the Financial Monitoring Service regularly publishes a publicly accessible online list of individuals and entities subject to international sanctions enforced by Azerbaijan. These sanctions primarily fall under two main categories:

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

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

While the list of sanctions doesn't directly target ACW, it poses a signifcant barrier to illegal activities that may involve such weapons, including the transportation of dual-use goods. The

[5] https://www.reuters.com/world/us-targets-frms-china-hong-kong-over-alleged-role-iranian-drone-procurement-2025-02-26

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 ratifed.

In 2024–2025, Azerbaijan sought closer ties with emerging economies, including applying for BRICS membership. However, the government continues to align its national sanctions regime with UN Security Council resolutions and FATF recommendations, particularly in high-risk trade sectors such as dual-use goods, unmanned systems, and chemicals.

Extraterritorial Application of Sanctions

Defnition: 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 transaction includes U.S. persons, fnancial institutions, territory, or infrastructure, companies or individuals are subject to U.S. sanctions.

Even though Azerbaijan is not a party to all international sanctions regimes, U.S. enforcement authorities, particularly OFAC, can and do enforce U.S. sanctions against foreign companies and individuals. For example, 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 fnancial system and other penalties like fnes and/or restrictions. Azerbaijani companies should review this guidance to understand how U.S. sanctions and export control laws are applied to host non-U.S. persons accountable for violations, as well as how international companies can mitigate the risks of non-compliance.

National law Requirements by Sectors

Arms Procurement and Sales

Azerbaijan's defense production infrastructure and related confdentiality restrictions illustrate how national arms manufacturing, particularly of ACW components, can shape proliferation risks, infuence procurement networks, and create distinct compliance challenges. 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.[6] 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.

[6] Article 7.3 of the Statute

N	Manufacturing/research facility	Scope of operations
1.	“Iglim Science-Production Enterprise” LLC	■ Developing and preparing airfeld equipment for aviation operations; ■ Manufacturing tools and technological equipment for various purposes.
2.	Factory of Electronic Computing Machines LLC	■ Manufacturing electronic devices and gadgets; ■ Producing industrial and household appliances; ■ Crafting electromechanical and mechanical devices.
3.	"Avia-Agregate Plant LLC"	■ Manufacturing high-pressure balloons and cylindrical balloons; ■ Producing aircraft and kitchen equipment for civilian aviation; ■ Developing technological designs and tools.
4.	"Ganja Machine Building Plant" LLC	Manufacturing specialized and civilian products
5.	Tarter Electromechanics Plant	Manufacturing technical products
6.	Industrial Equipment Scientifc-Production Enterprise	Manufacturing fow meters, counters, dispensers, and alarms with a broad range of capabilities in fow and pressure, suitable for various liquids including aggressive substances.
7.	Radio assembly plant LLC	Manufacturing televisions, electronic cash registers, and electronic scales
8.	Shirvan Araz Plant LLC	■ Designing, enhancing, and manufacturing defense products; ■ Producing linear track equipment for multi-channel communication systems, alongside technical products and consumer goods
9.	Telemechanika Zavodu LLC	Manufacturing devices for the oil industry
10.	Sharur Radio Factory LLC	Manufacturing both defense and civilian products
11.	Azon Plant LLC	■ Manufacturing various types of microcircuits; ■ Producing mechanical parts for the oil industry; Manufacturing liquid nitrogen and oxygen.
12.	Dalga Scientifc-Production Enterprise	■ Designing and manufacturing marine navigation systems; ■ Developing and producing specialized navigation, communication, and information processing systems.

Figure 4. Selected production and research facilities under the Ministry of Defense Industry.

The export and import of weapons for defense purposes by the state are classifed as state secrets under specifc conditions and, by law, cannot be publicly disclosed. In addition to trade activities, the production and development of weaponry are also subject to the same confdentiality restrictions.

Shipping and logistics

In postal and courier services, a key focus of national legislation is the oversight of fnancial transactions. According to national regulations, postal services are permitted to conduct fnancial 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 fnancial operations as authorized by its license.

- Opening and maintaining postal accounts;
- Conducting money transfers;
- Opening correspondent accounts in fnancial 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

Several dual-use goods utilized by companies involved in transportation activities, along with materials applicable in the preparation of ACW and its components, such as explosives, fall under the category of dangerous goods. Special permits are mandated for handling these goods, including 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 specifc regulations governing the transportation of these goods via road, sea, air, and railways.

Financial Oversight and AML-Based Measures

While there is no specifc legislative or policy document in Azerbaijan that directly addresses fnancial transactions associated with Advanced Conventional Weapons (ACW) components, several legislative acts and regulatory mechanisms contain indirect measures aimed at preventing such activities.

These preventive measures are primarily governed by Anti-Money Laundering (AML) legislation, which imposes obligations on fnancial institutions to detect and deter money laundering and terrorist fnancing through standard and, where necessary, enhanced customer due diligence procedures. Individuals and entities from jurisdictions identifed as high-risk by the Financial Monitoring Service, along with their bank accounts and associated suppliers, are subject to heightened scrutiny, and institutions must implement internal controls to identify and prevent suspicious transactions.

Azerbaijan has shifted from relying solely on static legislative norms to adopting action plans, enabling more adaptive and targeted interventions that extend beyond banks to institutions such as the Prosecutor General's Offce, the Supreme Court, and the Bar Association. The National Action Plan for Combating the Legalization of Criminally Acquired Property and the Financing of Terrorism for 2023–2025, approved by Presidential Decree No. 3770 on 28 February 2023, refects this comprehensive approach. Implementation began in 2024 and includes risk assessments, methodologies for identifying shell companies and benefcial owners, capacity building for supervisory bodies, and measures to enhance judicial and prosecutorial effectiveness, with reforms planned through 2025 to create a clear framework for combating the fnancing of illegal trade.

In sum, Azerbaijan maintains a multi-tiered system of legal, technical, and institutional controls to regulate dual-use goods and advanced conventional weapons. Entities operating in high-risk sectors should ensure compliance with national and international export controls, regularly consult the FATF and Azerbaijani Financial Monitoring Service sanctions lists, and implement robust internal control systems.

IMPLEMENTING AN EFFECTIVE AND COMPLIANT RESPONSE TO SANCTIONS

Any business that operates across multiple jurisdictions, in fnancial 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 the risk posed by sanctions enforcement if they lack a suffcient compliance regime. Some types of frms, such as logistics, fnance and goods manufacturers, are more vulnerable than others. Because proliferating states rely on access to the formal fnancial system to raise and gain access to funds, conduct payments, and facilitate illicit activities, it is contingent on private sector frms to assess the risk posed by their customers and specifc transactions, as well as monitor and report illicit activity. Firms that produce high-specifcation goods and that are prone to being targeted by illicit procurement are often small and medium-sized enterprises. Though many frms, particularly in the fnancial services and banking sector, likely have some form of compliance program in place, many frms lack the resources and understanding to assess risks and apply the appropriate risk-based approach to countering illicit transactions associated with ACW.

ACW-specifc Sanctions Compliance Programs in Azerbaijan

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

- Financial institutions: According to the U.S. Department of Commerce's Bureau of Industry and Security (BIS) and the U.S. Department of Treasury's Financial Crimes Enforcement Networks (FinCEN), these types of frms may be involved in providing fnancing, processing payments, issuing lines of credit, providing capital loans, and issuing or paying insurance on shipping and delivery of goods. **In Azerbaijan, this includes commercial and electronic banks, credit card operators, and foreign exchange dealers.**
- Electronics frms: 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 diffcult with so many changing customers. Compliance is easier for frms 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 frm includes importers and exporters of electronics and other technology.**
- Transportation frms: U.S. sanctions and export control enforcement has increasingly focused on supply chain risks, targeting frms 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 frms include air cargo companies, freight forwarders, railways, shipping 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.

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 [7]:

- What sanctions are a risk to the frm in question
- Why it is important the frm comply with sanctions
- What controls exist to ensure the frm'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 frms, but it is unlikely that a frm can meet its sanctions-related obligations without a fulsome understanding of its exposure to risk.

Risk assessments are a product that identifes, 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 frms, particularly banks and fnancial institutions, will already have a robust system in place to identity risk associated with money laundering (AML) or terrorist fnancing (CTF), many of which can be adapted to address risk related to ACW and sanctions. Some frms may also have risk assessments related to proliferation fnance, a subset of fnancial 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 frm'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, fnancial services, and electronics.

[7] Zia Ullah and Victoria Turner, "Principled Guide to Sanctions Compliance Programmes," Global Investigations Review, July 8, 2022, https://globalinvestigationsreview.com/guide/the-guide-sanctions/third-edition/article/principled-guide-sanctions-compliance-programmes

- 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 frms, both fnancial institutions and others, can implement that will put a frm in a good position to detect transactions and prove to enforcement authorities that they 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 frm'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-fag 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 complicated networks associated with ACW components, due diligence may need to extend beyond immediate customers to also consider your clients' clients. [8] Increasingly, sanctions enforcement agencies also expect frms 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 identifers to ensuring goods requested are appropriate for the stated end uses.

Customs offcials have developed a useful list of **behavioral red fags for customer interactions** in proliferation fnance that can be applied to screening of customers with risk associated with ACW transactions. Red fags can include:

- Your frm 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. [9]

[8] 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

[9] "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-fags

List-Based Screening: Conducting sanctions screening is the major way fnancial services frms can ensure they are 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 fnancial frms, and lists are often updated infrequently. They can also give a fall sense of security.

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

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

Training: A routine training program should also be part of a compliance program, to ensure all members of an organization understand the limitations that sanctions create and the ways in which risks can be identifed. [10]

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 specifc clients ties to those networks – to reveal a possible connection with the frm.

Identifying ACW Transactions of Concern

Identifying transactions or goods/services that would expose a frm 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, [11] there are specifc transactions fnancial institutions may have access to that would alert them to potentially suspicious activities related to ACW components:

- Customers' end-use certifcates, export documents, or other more extensive documentation associated with letters of credit-based trade fnancing.
- 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 fnancial institution or handled as part of a correspondent banking transaction.

[10] 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

[11] "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.fncen.gov/sites/default/fles/2022-06/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf

Government offcials have created **"red fag indicators"** to help exporters identify behavior or transactions of concern. A full list of the red fags is included in Annex C. Some specifc red fags 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. [12]
- 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 frms that also have offces in sanctioned end users.
- Transactions identifed through correspondent banking activities connected to frms that resell electronics and other similar items to sanctioned frms.
- 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 ft 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 frm is listed as the product's fnal destination.
- Packaging is inconsistent with the stated method of shipment or destination. [13]

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.

[12] "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.fncen.gov/sites/default/fles/2022-06/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf

[13] "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-fags

Key Takeaways

- Private sector frms – particularly in the fnancial 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 frm 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 **specifc transactions and red fag indicators** that fnancial 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 frms 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 specifc license requirements for the export, reexport and/or transfer (in-country) of specifed 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.
- Offce 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: [14]

- Customer declines to provide end-use or end-user information, or provides vague, incomplete, or inconsistent details regarding the purpose or destination of the goods or services.
- Transactions involving shell companies or recently formed entities, especially those with opaque ownership structures or lacking a clear operational history, particularly in jurisdictions known for limited regulatory oversight.
- Repeated use of routing through high-risk transshipment hubs, such as Hong Kong, the UAE, Turkey, or Central Asian countries , especially when these jurisdictions are not aligned with usual trade fows or customer base.
- Use of email domains that are generic or mismatched with the company's claimed identity (e.g., free webmail services instead of company-specifc domains), particularly in initial procurement inquiries or communications.
- Requests to alter documentation (e.g., invoices, bills of lading, country of origin labels) in a way that could conceal the actual nature or origin of goods or their intended end user.
- Correspondent banking transactions involving frms that are petroleum-related, electronics resellers, or share ownership, addresses, or control with sanctioned or state-owned entities.
- Shipments or payments previously linked to sanctioned jurisdictions that are later reassigned to alternate destinations; use of atypical or indirect shipping routes inconsistent with commercial norms; or freight forwarding frms listed as fnal consignees for sensitive goods.
- Last-minute modifcations to payment structures, routing, or counterparties—particularly when involving sanctioned jurisdictions or high-risk actors.
- Entities sharing physical locations, ownership structures, or control with frms on the BIS Entity List, OFAC SDN List, or state-owned enterprises from sanctioned jurisdictions; or whose listed addresses are residential, unverifable, or non-commercial in nature.
- Transactions involving individuals with prior export control violations, or frms engaged in large-volume purchases of electronic components (including EAR99 items), particularly when paired with payments to shipping companies or routed through high-risk jurisdictions.
- Customers involved in defense-related, dual-use, or government-linked sectors; those operating under generic names or in "special purpose projects"; or entities with minimal or no public-facing presence (e.g., absent websites or business registration data).

[14] "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.fncen.gov/sites/default/fles/2022-06/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf

ANNEX C: Template for Assessing ACW Sanctions Compliance Program [15]

I. Senior Management Commitment

- ☐ Has senior management formally approved the sanctions compliance program (SCP), and is there clear documentation of their support?
- ☐ Does your frm designate a sanctions compliance offcer with adequate authority and resources?
- ☐ Is there a "culture of compliance" at your frm?

II. Risk Assessment

- ☐ Has your frm conducted a documented risk assessment specifc to sanctions exposure, including risks related to ACW components and end-users?
- ☐ Do you conduct due diligence to verify the identity and background of customers, suppliers, and other 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 frm 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 frm know the receiving country?
  - ☐ Is the receiving country sanctioned?
  - ☐ Is the country a known facilitator for a sanctioned end user?
- ☐ Does your frm know the end-use and end-user?
  - ☐ Have you confrmed 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 benefciary are subject to sanctions?
- ☐ Does your frm 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 frm have a written SCP that includes procedures for onboarding, screening, recordkeeping, escalation, and reporting?
- ☐ Are internal controls clearly communicated and integrated across business units?

IV. Testing and Auditing

- ☐ Is there a process to routinely test and audit the effectiveness of your sanctions controls?

  Are fndings from audits used to update internal controls and training?

V. Training

- ☐ Does your frm provide regular, role-specifc training on sanctions compliance, tailored to staff functions and risk exposure?

[15] Sources for Checklist include: LexisNexis Sanctions Risk Checklist, https://www.lexisnexis.com/community/cfs-fle/__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/fles/126/framework_ofac_cc.pdf