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

2025

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

Center for Strategy and Development

ABOUT THIS MANUAL

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

For a full list of abbreviations used in the manual, please see Annex A.

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

Table of Contents

OVERVIEW

Since the mid-2010s, sanctions have become an increasingly prominent tool used to target security threats, including both non-state groups and state actors. Non-compliance with sanctions regimes is now a significant risk for many private sector entities, particularly financial institutions, defense contractors, transportation companies, and technology/electronics firms.

During the first half of 2025, sanctions enforcement related to advanced conventional weapon (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 growing tendency of using sanctions strategically to disrupt those networks. Indeed, the focus has expanded from purely targeting weapon systems to also disrupting access to critical dual-use components and technologies. The respective situations in relation to the three countries mentioned above are summarized below.

Russia: Sanctions against Russia remain sharply focused on degrading its military-industrial base, especially following the 2022 invasion of Ukraine. Enforcement actions have begun more and more to target 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 Russia making efforts to accelerate domestic defense production, it continues to face major challenges including quality control issues and delays.

Iran: Sanctions imposed on Iran have primarily focused on its ballistic missile program and the proliferation of unmanned aerial vehicles (UAVs) and missile systems to proxies and partners. Relatedly, Iranian manufacturers have been subjected to sanctions for their role in producing UAVs now categorized as ACWs. Sanctions have also aimed to destabilize Iran's military-industrial complex by disrupting its access to missile and UAV components.

North Korea: Still one of the most heavily sanctioned states in the world, North Korea remains under a comprehensive United Nations (UN) arms embargo that prohibits the export and import of all conventional weapons and restricts access to dual-use goods, technologies, and financial resources that could support its military programs. Over the past six months, the international community has placed renewed attention on North Korea's role in proliferating ACW components particularly through covert arms transfers and the development of ballistic and cruise missiles, the use of which is becoming more common in conventional warfare.

This manual focuses on **raising operational awareness** of specific ACW components and systems, as well as sanctions regimes seeking to restrict the ability of proliferating states to access the components and transactions required to manufacture and distribute ACWs.

UNDERSTANDING OBLIGATIONS AND ACWs

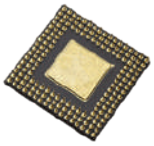
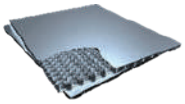
A range of bilateral and multilateral sanctions as well as export control regimes currently impose legal and operational obligations on private sector entities. Historically, these regimes have concentrated on restricting the proliferation of weapons of mass destruction (WMDs), as seen in the extensive UN sanctions frameworks addressing North Korean proliferation finance and, more recently, Iranian missile and nuclear activity. However, the global sanctions environment has evolved significantly 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 ACWs. In parallel, national export control laws have been expanded to reflect these shifts, creating layered compliance obligations for firms engaged in sensitive sectors or operating across jurisdictions. For Armenian firms in particular, the overlap among these regimes means that decisions about procurement, logistics, and trade partnerships must now account for heightened sanctions exposure and regulatory scrutiny.

ACWs and Their Components

ACWs comprise a diverse array of technologically sophisticated systems. While no single definition is universally accepted, ACWs 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. Elsewhere, emerging ACW categories include lethal autonomous weapon systems (LAWSs), such as UAVs, unmanned ground vehicles (UGVs), uncrewed surface vessels (USVs), and uncrewed underwater systems (UUSs). Ballistic and cruise missiles – though traditionally classified as delivery vehicles for WMDs – are increasingly deployed in conventional operations and thus considered part of the ACW landscape.

For most firms, one of the greatest compliance challenges will likely lie not in handling complete weapon 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 significant legal and sanctions risks and underscore the need for robust due diligence and end-use verification protocols.

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

Type of Component		Usage
Microelectronics/microchips		Communications equipment, unmanned aerial systems (UASs), precision long-range munitions
Semiconductors		Defense-related components (computers, sensors, switches, amplifiers)
Bearings		Tanks, aircraft, submarines, other military systems
Connectors, fasteners, transformers, casings, transistors, insulators		Basic components that constitute electronics systems in a conventional weapon system
Engines, vehicle parts		Tanks, armored combat vehicles (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. All three are present in Armenia, requiring diligence from firms operating there.

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, financial, or technical support to evade sanctions and export controls. **Unwitting participants** – such as manufacturers, freight forwarders, financial 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.

Vignette: In April 2024, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) designated OJSC Keremet Bank, a financial institution based in the Kyrgyz Republic, for providing material support to a sanctioned Russian bank. OFAC stated that Keremet Bank had materially assisted, sponsored, or provided financial services to Rosbank, which was previously designated for operating or having operated in the financial services sector of the Russian Federation's economy. **This case highlights the risks that financial institutions in third countries may face when facilitating transactions involving sanctioned Russian entities.**

Objects Being Proliferated

ACW components, which on account of their size are less detectable and traceable than full systems, are a key concern from a proliferation standpoint. 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, and satellite navigation tools.

To counter such activity, companies and government agencies should **prioritize due diligence, licensing scrutiny, and end-use monitoring** for specific categories of augmenting components, including but not limited to:

- Microchips and semiconductors;
- Integrated circuits and fuses;
- Infrared sensors, thermal cameras, and night-vision technologies; and
- Advanced optics and satellite navigation systems.

These items are frequently embedded in dual-use goods and are often diverted under false pretexts. Focusing compliance resources and interdiction strategies on these specific components is essential in disrupting illicit ACW modernization and reverse-engineering efforts.

Shipments of legacy or "classical" weapon systems—such as tanks, artillery, or other heavy military equipment—are comparatively easy 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 require significant upgrades to regain operational effectiveness. This creates a persistent demand for spare parts, advanced subsystems, and specialized technical expertise necessary for maintenance, modernization, and adaptation to contemporary battlefield requirements. In many cases, these components and technologies together form the foundation for reverse-engineering efforts aimed at enabling domestic production, further complicating efforts to disrupt proliferation.

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 US and European companies. Analysis of missile debris from an attack on 2 January 2025 indicated that approximately 75% of the electronic components were tied to US-based firms. These findings underscore North Korea's reliance on foreign-sourced materials and components for its weapon programs, despite existing UN 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 intended end use from manufacturers. **This case highlights how covert procurement networks can exploit global supply chains despite sanctions.**

Patterns of Proliferation

Generally, ACW proliferation is developing along the following tracks:

- **Direct peer-to-peer transfer:** Overt state-to-state deliveries of weapons, components, or production technology (e.g. Iran and North Korea supplying Russia). Such exchanges create a cascade effect in which previously acquired Western-origin technology is redistributed among partners.
- **Covert transshipment:** Smuggling of dual-use items camouflaged as legitimate civilian trade, using falsified end user or destination data to obscure the identity of the true military recipient.
- **Domestic replication:** Integration of imported hardware, tooling, or know-how into a nation's own defense-industrial base through reverse engineering, re-manufacture, or incremental modernization.
- **Uncontrolled diffusion:** Secondary spread of ACW components from state actors to proxy forces or non-state groups, after which the materiel enters illicit arms markets and becomes difficult to trace.

The most likely practice involving Armenia is procurement of ACW components via transshipment hub. In this scenario, components such as microelectronics are exported legitimately to Armenia, only to then be re-exported to sanctioned end users. Microelectronic third-party distributors and wholesalers often operate through intermediary jurisdictions, complicating the ability of firms to identify (and avoid) counterparts associated with sanctioned end users.

Vignette: In early 2025, the U.S. Department of the Treasury announced that enforcement actions would be taken on a transshipment scheme designed to obscure the Iranian origin of restricted goods. The case centered on exports of high-density polyethylene (HDPE), a dual-use material produced by Iran's Mehr Petrochemical Company, which were routed through the Jebel Ali Port in the United Arab Emirates to conceal their true origin. The network used falsified documentation listing "Middle East" or "Jebel Ali, UAE" as the country of origin, and directed shipping agents to omit Iranian port information from bills of lading. Payments totaling nearly $291 million were processed through U.S. correspondent banks using wire transfers that excluded any mention of Iran, allowing the scheme to bypass US sanctions controls. **This case highlights how intermediary jurisdictions can be exploited to mask the origin of restricted goods and underscores the importance of origin verification, end-use screening, and counterparty due diligence in high-risk supply chains.**

ACW-related Requirements in Armenia

Armenia's regulatory framework for dual-use goods and military items is governed by the 2010 Law on Export Control of Dual-Use Items and Technologies and Their Transit. While Armenia is not a member of any formal multilateral export control regimes (e.g. the Missile Technology Control Regime (MTCR) or the Nuclear Suppliers Group (NSG)), it voluntarily aligns with the Wassenaar Arrangement and the EU Dual-Use List. Export control decisions are made by interagency consensus, and oversight bodies include the Ministry of Economy, the Ministry of Defense, and the State Revenue Committee. **Firms in Armenia have been a particular focus of US enforcement authorities because of the country's reputation as a common transshipment hub.**

Examples of sanctioned entities in Armenia include:

Entity	Reason for Sanctions
TACO LLC	Shipped microelectronics to Russian defense entities (2023)
Medisar LLC	Added to the U.S. Entity List for procuring U.S.-origin goods for Russian military end users (2023)
Milur Electronics	Affiliated with sanctioned Russian company Milandr (2023)

Licensing and Permissions

Amendments to Armenia's export control enforcement framework have strengthened deterrence. Government Decree No. 808-N outlines the procedure for verifying compliance with export licensing and documentation requirements. As of 2024, the Ministry of Economy may initiate inspections to identify violations, with referral to law enforcement if evidence of criminal conduct is found. Parallel administrative measures are governed by Article 169.34 of the RA Code of Administrative Offenses, targeting unauthorized exports of listed dual-use and military goods to Eurasian Economic Union (EAEU) states by air. Violations are punishable by fines equivalent to 50% of the shipment's value (minimum 1 million AMD) and possible confiscation of goods. These measures provide layered enforcement options and close previously navigable loopholes in criminal and administrative legislation/frameworks.

Armenia maintains lists of both controlled and exempt goods to guide private sector compliance in adherence with the following classification.

Category	Description
Dual-use goods	Goods usable for both civilian and military purposes, subject to export control under Decree No. 1785-N.
Military goods	Items requiring permits under the authority of the Ministry of Defense, based on sensitivity and classification.
Exempt items	Items on the non-dual-use list as of December 2024, not requiring export licenses.

Control of Import, Export, and Transit Shipments

Reforms within the Customs Service of the State Revenue Committee have streamlined procedures related to dual-use and military goods. Previously, many goods not meeting the criteria for control still required expert review, resulting in delays and costs for importers (up to 60,000 AMD per assessment). In April 2024, a dedicated task force was created to conduct free, expedited screening for goods listed in the relevant nomenclatures. In the same year, between April 11 and May 31, the task force reviewed 1,035 applications covering 4,341 items, approving nearly 90% of submissions without requiring formal expert review. These changes saved businesses an estimated 15.9 million AMD and significantly reduced processing time.

Authority	Jurisdiction	Role
Ministry of Economy	Dual-use goods	Issues and oversees licenses for non-military controlled goods.
Ministry of Defense	Military goods	Adjudicates export control issues for defense-related items.
State Revenue Committee	Customs enforcement	Implements customs controls and screening procedures.

Many businesses rely on customs brokers to provide guidance on whether licenses are needed for exports or imports. In addition to government-published lists of controlled goods, a list of non-dual-use items (updated in 2024) helps exporters to determine when no licensing is required. Nonetheless, some business representatives expressed the need for additional training to recognize when goods fall under export control.

Border and Transit Considerations

Only two of Armenia's land borders—those with Georgia and Iran—are open for export and transit. Although Armenia is a member of the EAEU, it retains independent customs and border enforcement authority. Its other borders, with Turkey and Azerbaijan, are closed. Border posts, including at Zvartnots Airport and the Iranian land border, are equipped with US-supported detection infrastructure, especially for chemical, biological, radiological, and nuclear materials. Russian border control units were withdrawn from these checkpoints in 2024 and 2025, increasing Armenian responsibility for enforcement.

Export Licensing and Legal Foundations

The legal basis for Armenia's export control system is the Law on Export Control of Dual-Use Items and Technologies and Their Transit (Law No. 42-N, 2010). This law governs the circulation of dual-use items, including import, export, and intangible transfers, and defines the responsibilities of exporters, brokers, and state authorities. It requires legal and physical persons to obtain licenses and report activities involving goods that could be repurposed for weapons development. Armenia penalizes the unauthorized export of controlled items under its Criminal Code.

Government Decree No. 1785-N sets out the list of dual-use goods based on the EU Dual-Use Control List, while Decree No. 1308-N outlines the list of military goods, licensing procedures, and documentation required for the transit and trade of those items. Permits may come in the form of general, individual, or catch-all licenses, and the Interagency Licensing Committee—comprising multiple ministries—must approve applications unanimously. Any agency can veto an application based on security, end-use, or geopolitical risk considerations.

Financial Sector Enforcement and Controls

Armenia's banking sector conducts rigorous anti-money laundering (AML) and sanctions checks on all international transactions. Banks manually screen parties and intermediaries using tools like Accuity and public sanctions lists. Meanwhile, Armenia's Central Bank requires that the country's banks and financial organizations have internal compliance frameworks in place, and it also offers training for sanctions officers. In March 2024, most banks ceased cooperation with Russia's Mir payment system to avoid secondary sanctions risks. Armenia's banks report having comprehensive internal systems to detect and prevent transactions linked to sanctioned parties. These include manual screenings through databases such as Accuity, mandatory justifications for international wire transfers, and dedicated AML departments trained in sanctions compliance. Banks have also developed internal legal frameworks, such as sanctions compliance policies and internal checklists. Armenian institutions place an emphasis on having zero tolerance of sanctions breaches and report that compliance is considered a national concern.

Measure	Description/Example
Sanctions Screening	Manual checks against OFAC, EU, UN, and Bureau of Industry and Security (BIS) lists using databases like Accuity.
Transaction Vetting	Review of parties, intermediaries, goods/services, and just ification documents.
Internal Policies	Banks maintain a formal sanctions compliance policy and checklist.
Training	Annual or as-needed compliance training triggered by major sanctions updates.
System Restrictions	Blocked cooperation with Mir payment system to avoid secondary sanctions.

Interagency Export Control Process

Export and transit licenses for dual-use and military goods in Armenia require consensus from an interagency panel that includes the Ministries of Economy, Defense, Foreign Affairs, and Internal Affairs, as well as the National Security Service and the Customs Service. The panel has no formal public name and operates under national export control law. A license may be denied if any authorized agency raises an objection, something that according to consulted officials had occurred in several cases. Armenia has also faced restrictions from partner countries such as Russia, particularly when export applications involve technologies where ownership or development is shared.

International Engagement and Limitations

Although Armenia is not yet a member of the Wassenaar Arrangement, its national control lists align with Wassenaar standards, and it participates in Wassenaar's open sessions. Its full membership is pending the resolution of political issues with existing member states, including Turkey.

Controlling Intangible Assets from Armenia

Controlling the export of intangible assets from Armenia, such as information, intellectual property, and software, also poses challenges. Unlike dual-use physical goods, which customs authorities can detect and prevent from being illegally exported, intangible assets are often transferred virtually and difficult to monitor. According to current legislation, the transfer of such controlled intangible assets requires special licenses issued by authorized bodies. However, liability applies only if the exporter knew or should have known that the transferred information or products could be used not only for civilian purposes but also for military purposes, including the development of WMDs. This creates enforcement challenges and leaves room for evasion. For example, a programmer working with a foreign company may export software code or dual-use information without realizing its potential dual nature or risks. This issue has become particularly acute amid recent efforts to bypass economic sanctions.

IMPLEMENTING AN EFFECTIVE AND COMPLIANT RESPONSE TO SANCTIONS

Any business that operates across multiple jurisdictions, in financial or banking services, or in certain sectors related to defense and equipment, 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 sector, to consider the risks posed by sanctions enforcement if they lack a sufficient compliance regime. Firms engaging in logistics, finance, and goods manufacturing 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 risks posed by their customers and specific transactions, as well as monitor and report illicit activity.

Firms producing high-specification goods and prone to being targeted by illicit procurement are often small and medium-sized enterprises (SMEs). Though many firms, particularly in the financial services and banking sector, likely have some form of compliance program in place, many lack the resources and understanding to assess risks and apply the appropriate risk-based approach to counter illicit ACW-related transactions.

ACW-specific Sanctions Compliance Programs in Armenia

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

- *Financial institutions:* According to the Bureau of Industry and Security/Financial Crimes Enforcement Network (FINCEN), firms of this type may be involved in providing financing, processing payments, issuing lines of credit, factoring accounts receivable by exporting, providing capital loans, and issuing or paying for insurance on the shipping and delivery of goods. **In Armenia, this includes commercial and electronic banks, credit card operators, and foreign exchange dealers.**
- *Electronics firms:* Exporters and resellers of electronics face particular challenges regarding compliance with sanctions and export control regimes, especially involving the sale of components that could be used in ACW production. Many electronics exporters sell at high volumes to a range of customers, and the majority of business likely comprises off-the-shelf components. A key part of preventing illicit sales is knowing and understanding the end user, which is difficult in this case as the customers are constantly changing. Compliance is easier for firms that specialize in particularly sensitive electronics, such as those earmarked for the defense sector, because they tend to have fewer repeat customers. **In Armenia, this type of firm includes importers and exporters of electronics and other technology.**
- *Transportation firms:* US 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 Armenia, firms of this type include air cargo companies, freight forwarders, railways, shipping lines, and road transport operators.**

- *Defense sector:* In some countries, organizations in the defense sector –state-owned or private – can be engaged in the import/export of military grade components. **In Armenia, this includes state agencies like the Ministry of Defense and the Military-Industrial Committee under the Ministry of High-Tech Industry, as well as manufacturers of imaging systems, Global Navigation Satellite System (GNSS) jamming equipment, and UAVs.**
- *IT companies, universities, and research centers:* Institutions that produce or share intangible goods, such as software, algorithms, source code, or technical research, face growing risks under export control regimes, especially when the outputs have potential dual-use applications. **In Armenia, this includes firms in the software development sector, academic institutions, and public or private research organizations.**

A basic sanctions compliance program typically contains a set of internal policies and procedures, usually outlined in a compliance manual. These policies tend to include[iv]:

- What types of sanctions pose a risk to the firm;
- Why it is important for the firm to comply with sanctions;
- What controls are in place to ensure compliance;
- What obligations individual employees have; and
- What the consequences are for non-compliance.

Tailoring Risk Assessments for ACWs

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 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 would be able to meet its sanctions-related obligations without a fulsome understanding of its exposure to risk.

Risk assessments can be used to identify, analyze, and understand sanctions risk, and then to mitigate that risk. They should have a broad scope and encompass:

- Customer risk;
- Product and service risk;
- Geographic risk (organization and customers);
- Transaction risk;
- Delivery risk;
- Risk from mergers and acquisitions;
- Supply chain risk;
- Risk from intermediaries; and
- Network and systems risk.

Many firms, particularly banks and financial institutions, will already have a robust system in place to identify risk associated with money laundering or terrorist financing, many of which can be adapted to address risks 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 the acquisition of WMDs and associated materials.

Existing risk assessments can and should be adapted to address sanctions targeting other weapons, including ACWs. This could be achieved by:

- Including an analysis of the firm's exposure to clients in the geographic area(s) 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; and
- Increasing the scope of risk assessments to include exposure to risk in supply chains and 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 have emerged, however, some clear best practices that firms (financial institutions and others) can implement to position themselves well to detect transactions and prove to enforcement authorities that their detection attempts are being made in good faith. Relatedly, a number of open-source tools are listed in Annex A to assist with this type of due diligence.

None of the practices outlined below should be deployed in isolation: due diligence and risk assessment requirements must align with screening tools 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 complicated networks associated with ACW components, due diligence may need to extend beyond immediate customers to also consider the firm's clients' clients. Increasingly, sanctions enforcement agencies also expect firms to know about compliance risks posed by their suppliers and ensure that processes mitigate the risks. 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 in various countries have developed standard **behavioral red flags for customer interactions** in proliferation finance that can be applied to the screening of customers posing risks associated with ACW transactions. Red flags may include situations where:

- The firm is approached by a customer whose identity is not clear;
- The customer has little or no business background;
- The customer is usually involved in military-related business;
- The customer or their address matches or resembles one listed on a sanctions list;
- The customer is reluctant to offer information about the end use of the goods;
- The customer requests shipping or labelling that is inconsistent with standard practices;
- The customer is unfamiliar with the product's performance characteristics but still insists on purchasing it;
- The customer declines routine installation, training, or maintenance services; and
- When questioned, the customer is evasive or unclear about whether the product is intended for domestic use, export, or re-export.[vi]

List-based Screening: Conducting sanctions screening is the main way through which a financial services firm can ensure it is not engaging in transactions that are subject to a sanctions regime. List-based screening is often automated and can be useful in quickly 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, while they can also give a false sense of security.

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

Internal Policies: Firms should also clarify their policy on maintaining relationships with certain banks or businesses and determine the extent to which they operate in high-risk jurisdictions.

Training: Routine training should also be part of a compliance program to ensure all members of an organization understand the limitations created by sanctions and the ways in which risks can be identified.[vii]

Existing best practices can and should be adapted to address sanctions targeting other weapons as well, including ACWs. This could be accomplished by:

- Including questions relevant to sanctions and conventional weapons/components in the due diligence process – whether during onboarding or over the course of the client relationship;
- Ensuring that clients, particularly those involved in the manufacture and trade of defense-related items, have comprehensive due diligence procedures in place, with a clear idea of their trading partners and the potential end use of their products; and
- Investigating weapons and components networks – and any specific client ties to those networks – to identify any possible connection with the firm.

Identifying ACW-related 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 ACWs and their components.

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

- Customers' end-use certificates, export documents, or other supporting documentation associated with letters of credit-based trade financing;
- Information about other parties to a transaction, as contained in payment transmittal orders handled by intermediary institutions;
- Letters of credit received by exporters receive from their customers (importers);
- Lines of credit extended to exporters to facilitate the transaction; and
- Wire transfer payments from importers, as received by the exporter's financial institution or processed through correspondent banking transaction.

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

- Large-dollar or high-volume purchases of items from wholesale electrical/industrial merchants, or suppliers of electrical parts and equipment;
- A customer transports commodities of concern using trade corridors known for transshipment to sanctioned end users;
- The nature of a customer's underlying business/services/products relates to military or government work;
- US-based merchants involved in importing/exporting electronic equipment use business checking or foreign exchange accounts to transact with third-country-based electronics or aerospace firms that have offices in sanctioned jurisdictions;
- Transactions identified through correspondent banking involving firms that resell electronics and other similar goods to sanctioned entities;
- Payments originate from entities located in third-party countries and are not otherwise connected to the transaction and known to be a potential transshipment point for exports to sanctioned end users;[ix]
- Delivery dates are vague or involve unusual destinations;
- The product's capabilities do not match the buyer's stated business activity (e.g. sophisticated computers ordered by a small bakery);
- The ordered product is incompatible with the technical level of the recipient country (e.g. a semiconductor manufacturing equipment shipped to a country without an electronics industry);
- The shipping route is unusual for the product and destination;
- The freight forwarding firm is listed as the product's final destination; and
- Packaging is inconsistent with the stated method of shipment or destination.[x]

Illicit transactions may also be facilitated by **intentionally misidentifying controlled items** as "Export Administration Regulations 99 (EAR99)" items, which generally include consumer goods that do not require a license for export/transfer. Items could also reach sanctioned end users courtesy of the deliberate concealment of 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 in place **robust sanctions compliance programs tailored to identify transactions related to ACW components.**
- A firm is unlikely to meet its sanctions-related obligations without a thorough understanding of its exposure to risk, which should be outlined in a **risk assessment** document.
- Financial institutions and exporters should be aware of specific **transactions and red flag indicators**, and incorporate them into their sanctions compliance programs.
- There are various **best practices for sanctions compliance programs** – including due diligence, screening, internal policies, and training – that firms can tailor to address 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 Countering America's Adversaries Through Sanctions Act 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 pursuant to the Sanctions Act.

European Union: The EU maintains a list of sanctioned individuals and entities, which is constantly reviewed and 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 sensitive items.

List of Abbreviations used in the document.

Abbreviations	Definition
ACW	Advanced Conventional Weapons
AML	Anti-Money Laundering
ATGMs	Anti-Tank Guided Missiles
BIS	Bureau of Industry and Security
CAATSA	Countering America's Adversaries Through Sanctions Act
EAEU	Eurasian Economic Union
EAR	Export Administration Regulations
EU	European Union
FINCEN	Financial Crimes Enforcement Network
HDPE	High-Density Polyethylene
IT	Information Technology
LAWSs	Lethal Autonomous Weapon Systems
MANPADS	Man-Portable Air Defense Systems
MTCR	Missile Technology Control Regime
NSG	Nuclear Suppliers Group
OFAC	Office of Foreign Assets Control
SDN	Specially Designated Nationals
SMEs	Small and Medium-sized Enterprises
UAV	Unmanned Aerial Vehicle
UGVs	Unmanned Ground Vehicles
UK	United Kingdom
UN	United Nations
US	United States
USVs	Uncrewed Surface Vessels
UUSs	Uncrewed Underwater Systems
WMDs	Weapons of Mass Destruction

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

- 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 do not align with the given entity's usual trade flows or customer base.
- Email domains that are generic or do not match the company's claimed identity (e.g. free webmail services instead of company-specific domains), particularly in initial procurement enquiries or communications.
- Requests to alter documentation (e.g., invoices, bills of lading, or 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 involve firms 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, the use of atypical or indirect shipping routes inconsistent with commercial norms, or freight forwarding firms being listed as final consignees for sensitive goods.
- Last-minute modifications to payment structures, routing, or counterparties—particularly when involving sanctioned jurisdictions or high-risk actors.
- Entities sharing physical locations, ownership structures, or control with firms on the BIS Entity List or OFAC SDN List, or state-owned enterprises from sanctioned jurisdictions (or whose listed addresses are residential, unverifiable, or non-commercial in nature).
- Transactions involving individuals with prior export control violations, or firms 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 as well as those operating under generic names or in "special purpose projects," or entities with minimal or no public-facing presence (e.g. no website or business registration data).

ANNEX C: Template for Assessing ACW Sanctions Compliance Programs[xii]

I. SENIOR MANAGEMENT COMMITMENT

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

II. RISK ASSESSMENT

- ☐ Has your firm conducted a documented risk assessment specific 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 of 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 being 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 a written sanctions compliance program 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 for routinely testing and auditing the effectiveness of your sanctions controls?
- ☐ Are findings from audits used to update internal controls and training?

V. TRAINING

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

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

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

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

[iv] 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

[v] 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

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

[vii] Alexey Eremenko 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

[viii] "FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts," FinCEN & BIS Join Alert, June 28, 2022, https://www.fincen.gov/sites/default/files/2022-06/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf

[ix] "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 Joint Alert, June 28, 2022, https://www.fincen.gov/sites/default/files/2022-06/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf

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

[xi] "FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts," FinCEN & BIS Join Alert, June 28, 2022, https://www.fincen.gov/sites/default/files/2022-06/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf

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