Tip Sheet on Advanced Conventional Weapon (ACW) Components Sanctions Risk Identification and Compliance

Use this tip sheet to update your organization's practices to adhere to international best practices on sanctions and export control requirements, with a focus on transactions related to Advanced Conventional Weapon (ACW) components.

Why should you care? Sanctions are a critical international policy instrument used to influence the actions of states, organizations, and individuals that threaten global security and stability. For organizations, a lack of effective sanctions management can expose them to serious risks, including substantial financial penalties, restrictions on international trade, frozen assets, and loss of access to global financial systems. Non-compliance may also cause irreversible reputational harm and long-term disruption to operations and partnerships. Implementing a robust sanctions compliance framework is therefore essential to safeguard business integrity, ensure regulatory adherence, and maintain secure access to global markets.

ACW components: the electronic parts that make up weapons like missiles, military aircraft, bombs.

Dual-Use Goods: Components with military and civilian uses.

Sanctions: Blocking of assets or trade restrictions to achieve desired outcome.

Export Controls: Policies that limit or control the sale and shipment of certain dual-use goods.

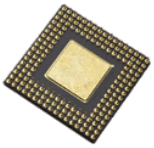
Update Your Risk Assessment: Existing risk assessments can and should be adapted to address sanctions targeting ACW. This can be achieved by identifying exposure to:

Geographic risk: Clients in proliferator or sanctioned countries

Product/Services risk: Clients, partners, or other relationships in risky sectors, including defense, shipping, freight forwarding, financial services, and electronics.

Other risks: Supply chains, mergers and acquisitions, shipment, and transactions.

Components:
Microelectronics/ microchips



Usage:
Communications equipment, unmanned aerial systems (UAS), long-range munitions

Components:
Semiconductors



Usage:
Defense-related components (computers, sensors, switches, amplifiers)

Components:
Engines, vehicle parts



Usage:
Tanks, armored combat vehicles (ACVs), aircraft

Components:
Bearings



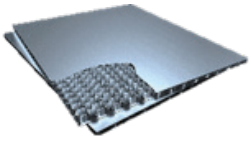
Usage:
Tanks, aircraft, submarines, other military systems

Components:
Connectors, transformers, casings, transistors



Usage:
Components for electronics systems in a conventional weapon system

Components:
Composite material



Usage:
Aircraft wings, missiles, drones

Conduct Due Diligence: Identifying ACW sanctions-related customers and transactions of concern is challenging - you have to have visibility on many data points, including origin, transit, and destination countries and people.

- 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.
- Repeated use of routing through high-risk transshipment hubs 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.
- Requests to alter documentation 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.
- Transactions involving shell companies or recently formed entities, particularly in jurisdictions known for limited regulatory oversight.
- 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
- 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.
- 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).
- Transactions involving individuals with prior export control violations, or firms engaged in large-volume purchases of electronic components (including EAR99 items)
- Shipments or payments previously linked to sanctioned jurisdictions that are later reassigned to alternate destinations.

Also known as **Know Your Customer**, your firm should carry out checks on potential customers, business partners, and goods. You can use public information such as early warning lists, red-flag checklists (like this one), and questionnaires, or paid services.

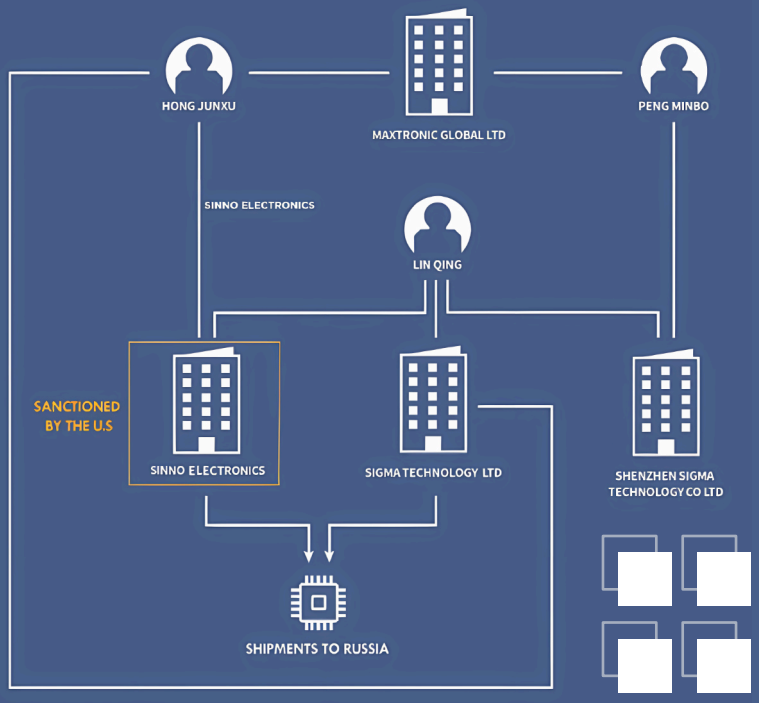
Screen Customers and Transactions:

Screen your **customers** at onboarding and at routine intervals. You can use automated list-based screening. Be aware of the limits to this approach - they can give a false sense of security. You can improve the effectiveness of screening by focusing on specific companies and areas of operation, taking stock of current threats, and investigating known networks.

Your firm should seek to identify specific **transactions** potentially related to ACW components. Financial institutions have access to significant amounts of data to use to identify these transactions, including export documents, trade financing documentation, payment transmittal orders, lines of credit, and wire transfers.

SIGMA TECHNOLOGY AND SINNO ELECTRONICS

An example of how various unsanctioned entities may in reality be involved in illicit transactions



Sources: US Bureau of Industry and Security; Hong Kong Companies Registry; Qichacha; Altana Trade Atlas; RUSI

Transactions of Concern

- Large dollar or volume purchases of items from wholesale electrical/industrial merchants, electrical parts and equipment providers, or electronic parts providers.
- Use of trade corridors known to serve as possible transshipment.
- Correspondent banking activities connected to proliferator country electronics resellers.
- Any business/services/products related to military or government work.
- 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 proliferator countries.
- The product's capabilities do not fit the buyer's line of business.
- Delivery dates are vague, or deliveries are planned for out of the way destinations.
- The shipping route is abnormal for the product and destination.
- The payment amount or method is out of the ordinary.
- The freight forwarding firm is listed as the product's final destination.
- The ordered product is incompatible with the technical level of the recipient country.

Control of Import, Export, and Transit Shipments in Armenia

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

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.

Update your Firm's Policies: After assessing your risk exposure, you will need to codify the outcomes of your assessment - and how you plan to address gaps - in your company policies. This includes:

- Determining the extent to which your firm will operate in proliferator country-related jurisdictions.
- Clarifying your policy on maintaining relationships with banks or businesses established in proliferator countries.
- Updating your firm's existing compliance manual or standard operating procedures to incorporate new and evolving sanctions requirements.
- Develop a training program to ensure all members of your organization understand the limitations that sanctions create and the ways in which risks can be identified.

Resources: For more information on sanctions and the latest sanctions lists, go to:

Office of Foreign Asset Control (OFAC) Sanctions List (sanctionssearch.ofac.treas.gov)

Bureau of Industry and Security (BIS) Entity List (bis.doc.gov/index.php/policyguidance/lists-of-parties-of-concern/entity-list)

Department of State CAATSA Sanctioned Entities List

European Union Sanctions Map (sanctionsmap.eu)

Sanctions Explorer by C4ADS (sanctionsexplorer.org)

Assessing an ACW Sanctions Compliance Program

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?