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

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

Why should you care? Sanctions against Russia, particularly by the U.S. and EU, increasingly impact firms, particularly financial institutions, in so-called transshipment hubs, or third-party locations that sanctions evaders use to obscure the origin or destination of funds or goods. Firms in Georgia face real reputational and business risks if they do not take steps to adhere to sanctions, even if Georgia is not a party to any sanctions again Russia.

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.

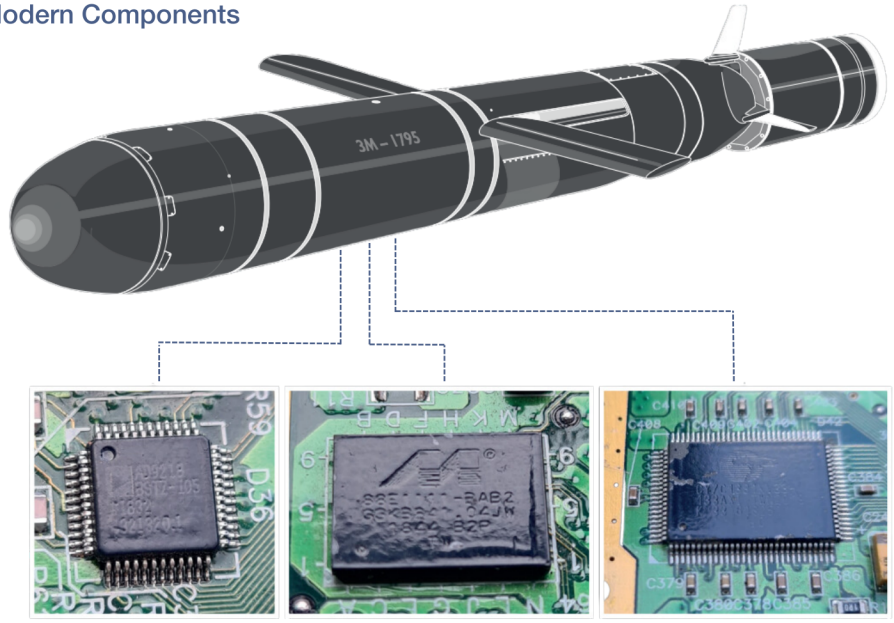
Export Controls: Policies that limit or control the sale and shipment of certain dual-use goods.

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 Russia or Belarus.
- **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.

Kalibr Cruise Missile Modern Components

Source: RUSI.



AD9218BSTZ-105
MSPS 3 V DUAL A/D CONVERTER

88E1111-BAB2
ULTRA GIGABIT ETHERNET TRANSCEIVER

CY7C1381KV33-133AXI
18MBIT PARALLEL STATIC RAM

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. 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 questionaries, or paid services.

Watch out for these behavioral red flags!

- Your firm is approached by a customer whose identity is not clear.
- The customer has little or no business background.
- The customer is involved in military business.
- The customer or their 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.
- The customer is unfamiliar with the product's performance characteristics but still wants it.
- The customer wants to pay in cash or cryptocurrency.
- The customer is evasive about whether the product is for domestic use or export.

Screen Customers and Transactions:

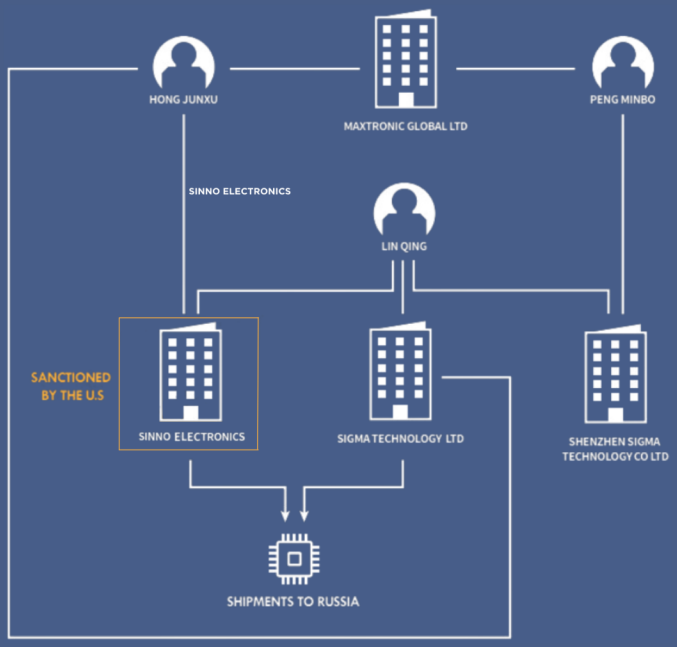
Screen your **customers** at onboarding and at routine intervals. You can use automated list-based screening. Be area of the limits to this approach - they can give a fall sense of security. You can improve the effectiveness of screening by focusing on specific companies and areas of operation, taking 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.
- Any business/services/products related to military or government work.
- Correspondent banking activities connected to Russian electronics resellers.
- Transactions involving payments being made from entities located in third-party countries not otherwise involved with the transactions and known to be a potential transshipment point for exports to Russia and Belarus.
- Delivery dates are vague, or deliveries are planned for out of the way destinations.
- The product's capabilities do not fit the buyer's line of business.
- The ordered product is incompatible with the technical level of the recipient country.
- The shipping route is abnormal for the product and destination.
- The freight forwarding firm is listed as the product's final destination.
- The payment amount or method is out of the ordinary.

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 Russia-related jurisdictions.
- Clarifying your policy on maintaining relationships with Russian banks or businesses.
- 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 to 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 (https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list)
- **Department of State** CAATSA list (www.state.gov/caatsa-section-231d-defense-and-intelligence-sectors-of-the-government-of-the-russian-federation)
- **European Union** Sanctions Map (www.sanctionsmap.eu)
- **Sanctions Explorer** by C4ADS (sanctionsexplorer.org)