How to Avoid Dealing with Unauthorized Persons, Entities, and Countries

December 2018

Licensing and other export certification requirements for exporting a military-related product (or service), are dependent upon the item's technical characteristics, the destination, the end-user, and the end-use. You, as the exporter, must determine whether your export requires a license. An export license may be required based on the country, company, or individual that you are doing business with or who ends up with the product or service.

To avoid dealing with unauthorized persons, entities, and countries, complete the following steps:

1. Check the Consolidated Screening List to see if trade with your business partner or end-user is allowed but requires a license, is restricted, or is prohibited.

The Consolidated Screening List (CSL) is a list of parties for which the U.S. Government maintains restrictions on certain exports, reexports, or transfers of items. The CSL consolidates export screening lists from the Departments of Commerce, State and the Treasury and may be used as an aid to industry in conducting electronic screens of potential parties to regulated transactions.

The following agencies publish separate lists that are all included in the CSL. These lists identify persons, businesses, organizations, and other groups to which trade is restricted or prohibited. See Appendix 1 for the complete set of lists included in the CSL.

- The Office of Foreign Assets Control (OFAC) of the Department of the Treasury administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals.
- The Bureau of Industry and Security (BIS) of the Department of Commerce protects the security of the United States, which includes its national security, economic security, cyber security, and homeland security.
- The Bureau of International Security and Non-proliferation (ISN) of the Department of State prevents the spread of weapons of mass destruction, delivery systems, and advanced conventional weapons capabilities and rolling back such proliferation where it has already taken root.
- The Directorate of Defense Trade Controls (DDTC) of the Department of State ensures commercial exports of defense articles and defense services are consistent with U.S. national security and foreign policy objectives.

2. Do your due diligence in researching your business partner, having compliance programs in place, and being alert to suspicious activity.

The BIS, the Defense Security Cooperation Agency (DSCA), and other agencies perform end-use checks, end-use monitoring, and physical verifications around the world with the foreign party of international transactions to determine if the party is a reliable recipient of U.S. goods and that items are or will be used in accordance with U.S. trade laws and regulations.

It is recommended by the BIS that U.S. businesses engaged in international defense or military-related transactions carry out the following compliance measures:

- Attend compliance training and seminars.

Compliance training and seminars are a good way for company leadership to familiarize themselves with the complexities of end-use monitoring and how to avoid dealing with unauthorized persons, entities, and countries. Trainings provide the foundation for effective export compliance.

- Implement compliance programs.

Good compliance programs ensure that businesses have all the necessary steps and contingency plans in place to ensure company compliance with all U.S. export laws and regulations. Important elements of a compliance program include management commitment, continuous risk assessment, formal written guidelines, pre and post export compliance security and screening, adherence to recordkeeping requirements, internal and externs compliance monitoring and periodic audits, program for handling compliance problems, and completing appropriate corrective actions. For more information see the Export Compliance Guidelines posted by the BIS.

- Be alert to suspicious inquiries.

Consider any abnormal circumstances in a transaction that indicate that the export may be destined for an inappropriate end-use, end-user, or destination. Such circumstances are referred to as "Red Flags." Included among examples of red flags are orders for items which are inconsistent with the needs of the purchaser, a customer's declining installation and testing when included in the sales price or when normally requested, or requests for equipment configurations which are incompatible with the stated destination (e.g. 120 volts in a country with a standard of 220 volts). See the Red Flags List published by the BIS, which is not all-inclusive, but is intended to illustrate the types of circumstances that should cause reasonable suspicion that a transaction will violate U.S. trade laws and regulations.

- Research your customer.

When researching your business partner or customer, there are several things you can do to ensure they are a reliable end-user and partner and will not violate any U.S. trade policies. First, you can use the CSL to screen your customers. Request an end-user certificate and visit the their public website, if available. Review other social media sources and request business registration. Provide license and regulatory conditions in writing and obtain written confirmation. Conduct a visit to the company, in person or virtually, and make sure there aren't any other red flags.

- Voluntarily disclose any violations you think may have or will occur.

Create internal and external reporting procedures for suspected violations of noncompliance. If a violation does occur, it is important to have all the necessary steps in place to report it to the appropriate authority as quickly as possible. Voluntary disclosures and transparency are important

in reporting a violation. You can also report suspicious inquiries if you believe you have been approached by a shady buyer or suspicious entity.

- Comply with foreign import and export controls.

  Understand foreign export control practices and what foreign countries are doing to ensure end-use compliance. This will help you and your company cooperate with all parties involved in the defense trade transactions, including any foreign organizations. Additionally, foreign government agencies most likely have more information about individuals and entities than you do, consulting with them when researching your business partner is a good idea.

3. Once you have verified you are dealing with an authorized international partner and have received the necessary licensing (if required), use the Destination Control Statement on all trade documents.

The Destination Controls Statement (DCS) is required for all exports from the U.S. of items on the U.S. Munitions List controlled by the International Traffic in Arms Regulations. It is also required for items on the Commerce Control List controlled by the Export Administration Regulations. At a minimum, the DCS must state:

"These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user (s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any other person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations."

The DCS must be entered on the invoice and on the bill of lading, air waybill, or other export control document that is included with the shipment from origin to destination.

Defense Industry Maine and the Maine International Trade Center are here to help you on your defense trade endeavors! We can research defense markets, help you navigate ITAR and EAR compliance, assist you in researching foreign trade partners that you would like to verify as an authorized person, and put you in touch with the right people to help your Maine company succeed. Contact us today for more information!

Note: The sale of defense products, technical data, software and services in defense industry transactions is regulated under the International Traffic In Arms Regulations ("ITAR"), the Export Administration Regulations ("EAR"), the U.S. sanctions laws, the Foreign Corrupt Practices Act and other laws. Companies engaged in this activity may be subject to export licensing, registration, recordkeeping and other legal requirements. MITC is not providing legal advice to your company regarding compliance under these laws and we strongly recommend that you obtain legal counsel to advise you on these issues.

Appendix 1: Separate Lists Included in the Consolidated Screening List

The OFAC posts the following lists:

- Specially Designated Nationals List – Parties who may be prohibited from export transactions based on OFAC's regulations.
- Foreign Sanctions Evaders List – Foreign individuals and entities determined to have violated, attempted to violate, conspired to violate, or caused a violation of U.S. sanctions on Syria or Iran, as well as foreign persons who have facilitated deceptive transactions for or on behalf of persons subject to U.S. Sanctions.
- Sectoral Sanctions Identifications (SSI) List – Individuals operating in sectors of the Russian economy with whom U.S. persons are prohibited from transacting in, providing financing for, or dealing in debt with a maturity of longer than 90 days.
- Palestinian Legislative Council (PLC) List – Individuals of the PLC who were elected on the party slate of Hamas, or any other Foreign Terrorist Organization (FTO), Specially Designed Terrorist (SDT), or Specially Designated Global Terrorist (SDGT).
- The List of Foreign Financial Institutions – Includes the names of foreign financial Institutions that are subject to sanctions, certain prohibitions, or strict conditions before a U.S. company may do business with them.

The BIS posts the following lists:

- Denied Persons List – Individuals and entities that have been denied export privileges. Any dealings with a party on this list that would violate the terms of its denial order are prohibited.
- Unverified List – End-users who BIS has been unable to verify in prior transactions. The presence of a party on this list in a transaction is a "Red Flag" that should be resolved before proceeding with the transaction.
- Entity List – Parties whose presence in a transaction can trigger a license requirement supplemental to those elsewhere in the Export Administration Regulations (EAR). The list specifies the license requirements and policy that apply to each listed party.

The ISN posts the following list:

- Nonproliferation Sanctions – Parties that have been sanctioned under various statutes. The linked webpage is updated as appropriate, but the Federal Register is the only official and complete listing of nonproliferation sanctions determinations.

The DDTC posts the following list:

- AECA Debarred List – Entities and individuals prohibited from participating directly or indirectly in the export of defense articles, including technical data and defense services.