

U.S. EXPORT CONTROL AND ECONOMIC SANCTIONS LAWS: WHAT EVERY COMPANY SHOULD KNOW

November 2006

M. Beth Peters, Esq.
Haley A. Boyette, Esq.
Hogan & Hartson LLP ^{1/}
Washington, D.C.

I. Introduction

One of the biggest challenges the United States faces in the post 9/11 era is preventing the proliferation of goods and technologies that can be used by terrorists to create weapons of mass destruction. The U.S. Government combats terrorism using export control and economic sanctions laws. These laws can affect both your international and domestic operations. It is imperative to have a basic understanding of these laws, not just to avoid severe civil and criminal penalties, but to keep your company's reputation intact—both in the United States and around the world.

Export control regulations restrict the export, reexport, import, and brokering of goods, services and technology. Generally speaking, there are three factors that influence the scope of restrictions: (1) the nature and use of the product; (2) the destination country; and (3) the identity of the specific end-user or end-users. Though these factors sound simple enough, there are a number of ways a company can inadvertently violate export restrictions, due to the expansive concept of “exporting.” For example, merely enabling a foreign customer to download software constitutes “exporting.” Furthermore, an item is “exported” even if it is only leaving the United States temporarily, regardless of whether it is sold for profit, going to a wholly-owned U.S. subsidiary in a foreign country, or merely being sent back to a foreign country from which it came.

Additionally, a transfer does not have to cross national borders to be an “export”. When a company grants a foreign person access to technology and software source code within the United States, an export is “deemed” to have occurred to that person's country of nationality and/or citizenship. ^{2/} Such transfers are known as “deemed exports.”

There primarily are three separate export licensing regimes. The first and most restrictive regime is the International Traffic in Arms Regulations (ITAR), which are administered by the U.S. State Department's Directorate of Defense Trade Controls (DDTC). ^{3/} Items within the DDTC's jurisdiction include “defense articles,” including “technical data” on the U.S. Munitions List, as well as “defense services.”

^{1/} M. Beth Peters is a partner and Haley A. Boyette is an associate with the law firm of Hogan & Hartson LLP. The authors would like to thank Tara Plochocki, a Summer Associate at Hogan & Hartson LLP, for her assistance.

^{2/} 15 CFR § 734.2(b)(2); 22 CFR §120.17.

^{3/} There are additional U.S. regulatory agencies that can have jurisdiction over export and import issues, such as the Food and Drug Administration and the Drug Enforcement Administration.

The second set of regulations is the Export Administration Regulations (EAR), promulgated by the U.S. Department of Commerce’s Bureau of Industry and Security (BIS). These regulations apply to purely commercial items as well as “dual-use” items (*i.e.*, items designed for civilian use, but that may also have military applications).

Lastly, the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury governs the enforcement of U.S. economic sanctions and embargoes. In addition to “blocking” the transfer of assets or items to certain countries, OFAC maintains a constantly expanding list of blocked individuals and entities, called Specially Designated Nationals (SDNs).

This paper describes these three U.S. regulatory regimes and offers general guidance that will help you and your company comply with these regulations.

II. The Export Administration Regulations

Nature of the Controls

BIS, pursuant to the EAR, controls the widest range of goods and technologies for export and imposes strict controls on those items that present foreign policy or national security concerns. ^{4/} These items include not only tangible goods, but related software and technology as well.

Everything from chemicals, toxins, viruses and bacteria, to paper clips and clothing are regulated for export under the EAR. However, most items subject to the jurisdiction of the EAR are freely exportable and do not require an export license from BIS.

Export classification under EAR is based on whether an item appears on the Commerce Control List (CCL). The CCL has ten categories, including:

- Category 0—Nuclear Materials, Facilities, and Equipment (and Misc. Items)
- Category 1—Materials, Chemicals, Microorganisms, and Toxins
- Category 2—Materials Processing
- Category 3—Electronics
- Category 4—Computers
- Category 5—Part 1 (Telecommunications) and Part 2 (Information Security)
- Category 6—Sensors and Lasers
- Category 7—Navigation and Avionics
- Category 8—Marine
- Category 9—Propulsion Systems, Space Vehicles and Related Equipment

Within each category there are five subcategories as follows:

- Subcategory A—Systems, Equipment and Components
- Subcategory B—Test, Inspection and Production Equipment
- Subcategory C—Materials

^{4/} DEPARTMENT OF COMMERCE, BUREAU OF INDUSTRY & SECURITY, DON’T LET THIS HAPPEN TO YOU!: ACTUAL INVESTIGATIONS OF EXPORT CONTROL AND ANTIBOYCOTT VIOLATIONS 3 (May 2006).

- Subcategory D—Software
- Subcategory E—Technology

If an item is not described in a particular entry on the CCL, it falls within the “basket” category known as EAR99. Items in this category are subject to minimal export controls and generally do not require the procurement of a license.

Whether or not a BIS export license is required will depend largely on the Export Classification Control Number (ECCN) assigned to a particular item or technology on the CCL. Each ECCN is a five-digit alphanumeric code corresponding to these categories and subcategories. For example, ECCN 1C351 (for Category 1, Materials, Chemicals, Microorganisms, and Toxins, and Subcategory C, Materials) covers “human and zoonotic pathogens and ‘toxins,’” including various viruses, bacteria and toxins such as the monkey pox virus, bacillus anthracis and salmonella typhi. Similarly, ECCN 1C992 covers certain vaccines, immunotoxins and medical kits.

The exportability of an item or technology will depend on its ECCN. Within each ECCN there is an explanation of the “reasons for control” of that item, which correspond to the EAR’s “country chart” which will identify which countries are available for export without a license under a particular ECCN.

Definition of “Export”

“Exports” include physical transfers or shipments of items, software or data. In addition, under the EAR, the “deemed export” rule covers the release of “technology” or software “source code” to a foreign national. [5/](#) Technology can mean both technical assistance, such as giving instructions concerning the regulated technology, as well as hard data in various forms, such as blueprints, models, manuals and diagrams. [6/](#) “Publicly available” information does not come under the purview of the export control rules. Examples include information generated as “fundamental research” at a university or information listed in certain patent applications. [7/](#)

The EAR also govern “reexports” of U.S. origin items, software and technology from one foreign country to another. U.S. export regulations “follow the good.”

Restricted Persons

The EAR also impose restrictions on transactions involving designated persons, entities and end uses that may require a license or are altogether prohibited. BIS designates restricted persons on the Denied Persons List, the Entity List and the Unverified List. The Denied Persons List concerns persons who have been denied export privileges due to unauthorized or illegal export conduct. The Unverified List applies to foreign persons who were parties to a transaction for which the Commerce Department could not conduct a pre-license check. The Entity List specifies restrictions on exporting to end users involved in proliferation activities, including entities in China, India, Pakistan, Russia, Israel and Syria.

[5/](#) 15 CFR § 734.2(b)(2)(ii).
[6/](#) 15 CFR Part 772.
[7/](#) 15 CFR § 734.3(b)(3).

Antiboycott Rules

The EAR contain regulations regarding “restrictive trade practices,” often referred to as the Anti-Boycott Regulations. These regulations prohibit participation of U.S. companies and their non-U.S. subsidiaries in boycotts not sanctioned by the U.S. government, such as the Arab League Boycott of Israel. The U.S. Treasury Department currently lists the following countries as “boycotting” countries: Kuwait, Lebanon, Libya, Qatar, Saudi Arabia, Syria, the United Arab Emirates and the Republic of Yemen.

Penalties

Both criminal and civil penalties for violation of the EAR may be imposed on individual persons or corporations. Criminal penalties for “knowing violations” can include a fine of \$50,000 or up to five times the value of the goods exported, whichever is greater, and/or imprisonment for up to five years. Penalties for other certain willful violations can include a fine of \$1,000,000 or up to five times the value of the goods exported, whichever is greater, and/or imprisonment for up to ten years. Civil penalties of up to \$50,000 per violation for corporations and/or individuals are possible, as well as administrative penalties such as suspension or denial of export privileges. Attendant negative publicity for violations is also a factor to consider.

III. The International Traffic in Arms Regulations

DDTC administers the ITAR, which govern the export of those items and services which are designed, developed or modified for a military purpose. Specifically, the ITAR control the transfer, export, temporary import and brokering of “Defense Articles,” “Defense Services,” and “Technical Data.”

Registration

As an initial matter, persons engaged in manufacturing or exporting Defense Articles or Defense Services are required to register with DDTC. Persons must complete a registration statement and renew it every two years. In addition, registrants must notify DTC of any material changes to the information on the registration within five days of the event. DTC requires registrants to submit a notification of any change in ownership or control to a foreign person 60 days in advance.

Nature of the Items Controlled: Defense Articles

Exports of Defense Articles and Defense Services almost always require prior written authorization from the DDTC. The Defense Articles regulated by the ITAR are listed on the United States Munitions List (USML). ^{8/} The USML is divided into 21 categories, some of which cover goods, technology and software, as follows:

- Firearms, Close Assault Weapons and Combat Shotguns
- Guns and Armament

^{8/} 22 CFR § 121.

- Ammunitions/Ordnance
- Launch Vehicles, Guided Missiles, Ballistic Missiles, Rockets, Torpedoes, Bombs and Mines
- Explosives and Energetic Materials, Propellants, Incendiary Agents and Their Constituents
- Vessels of War and Special Naval Equipment
- Tanks and Military Vehicles
- Aircraft and Associated Equipment
- Military Training Equipment and Training
- Protective Personnel Equipment and Shelters
- Military Electronics
- Fire Control, Range Finder, Optical Guidance and Control Equipment
- Auxiliary Military Equipment
- Toxicological Agents Including Chemical Agents, Biological Agents and Associated Equipment
- Spacecraft Systems and Associated Equipment
- Nuclear Weapons, Design and Testing Related Items
- Classified Articles, Technical data and Defense Services Not Otherwise Enumerated
- Directed Energy Weapons
- Submersible Vessels, Oceanographic and Associated Equipment
- Miscellaneous Articles

The list covers the full range of military equipment and weapons. It also contains items that shield persons from harm. For example, the ITAR governs the export of chemical and biological agents as well as individual and collective protection against them. [9/](#) Protection is not limited to physical gear, but includes vaccines and medical countermeasures designed to protect against nerve agents, biological agents, and blistering agents. [10/](#) The regulations also may apply to specially designed parts, components and precursor products.

Not all items that fit into the USML are specifically enumerated. Category 21, “Miscellaneous Articles,” covers any article which has substantial military applicability and which has been specifically designed or modified for military purposes. [11/](#) If the export jurisdiction related to a particular item or technology is in question, DDTC will make a determination according to procedures set forth in the ITAR (called a Commodity Jurisdiction, or CJ, determination). [12/](#) It is important to note that mere intent to limit the use of an exported object to a civil purpose does not exempt an object from the restrictions imposed by the ITAR. In fact, the State Department has the authority to retain jurisdiction over predominantly

[9/](#) 22 CFR § 121.14(f)(4)-(5).

[10/](#) 22 CFR § 121.14(h). (“Medical countermeasures, to include pre- and post-treatments, vaccines, antidotes and medical diagnostics, specifically designed or modified for use with the chemical agents listed in paragraph (a) of this category and vaccines with the sole purpose of protecting against biological agents identified in paragraph (b) of this category. Examples include: barrier creams specifically designed to be applied to skin and personal equipment to protect against vesicant agents controlled in paragraph (a) of this category; atropine auto injectors specifically designed to counter nerve agent poisoning.”).

[11/](#) 22 CFR § 121.21(a).

[12/](#) 22 CFR § 120.4.

commercial items (such as commercial communications satellites) if they have significant potential military or intelligence-gathering utility. [13/](#)

Nature of the Items Controlled: Defense Services

The ITAR prohibit U.S. persons from providing assistance or training to a foreign person with respect to a Defense Article, anywhere in the world, with proper prior authorization. The regulations govern assistance or training involving the “design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles.” [14/](#) Under the ITAR definition, “assistance” can be a Defense Service even if all of the information is already in the public domain.

Nature of the Items Controlled: Technical Data

The ITAR govern the export of Technical Data, which technically is defined as a subset of “Defense Articles.” Technical Data includes information, presented in any form, that is required for design, development, production, manufacture, assembly, operation, repair, testing maintenance or modification of Defense Articles. [15/](#) Technical Data can be “deemed” to be exported under the ITAR when transferred to foreign nationals, including to foreign national employees of embassies located in the United States. [16/](#) Technical Data excludes information in the public domain, marketing information, fundamental research at universities and basic mathematical, scientific or engineering principles commonly taught in schools and universities. [17/](#)

Penalties

Severe criminal and civil penalties for violation of the ITAR may be imposed on individual persons or corporations. For example, civil penalties of up to \$500,000 per violation are possible. The punishment can include imprisonment, monetary fines, or a suspension or denial of exporting privileges.

IV. U.S. Economic Sanctions Programs & the Office of Foreign Assets Control

The United States maintains comprehensive economic sanctions programs as well as more limited sanctions regimes. The U.S. Treasury Department’s Office of Foreign Assets Control (OFAC) administers and enforces both types of sanctions programs. [18/](#) The sanctions

[13/](#) 22 CFR § 120.3(b).

[14/](#) 22 CFR § 120.9(a)(1).

[15/](#) 22 CFR § 120.10(a)(1).

[16/](#) 22 CFR §120.16.

[17/](#) 22 CFR §120.10(a)(5); §120.11.

[18/](#) More information about OFAC and U.S. sanctions programs is available at <http://www.treas.gov/offices/enforcement/ofac/index.shtml>.

laws and regulations proscribe certain transactions with specific countries, entities and individuals. [19/](#)

Scope: Countries and Designated Persons

The U.S. Government currently maintains comprehensive economic sanctions against four countries: Cuba, Iran, Sudan and Syria. More limited economic sanctions are currently in effect against: Burma (Myanmar), Iraq, Liberia, Belarus and North Korea. In addition, the U.S. Government has imposed economic sanctions against certain senior members of the Governments of Zimbabwe and the Democratic Republic of Congo, and certain entities owned or controlled by them, as well as against certain persons who are contributing to the conflict in the Ivory Coast (Côte D'Ivoire). These sanctions are not territorial in nature (i.e., they do not apply to Zimbabwe or the Ivory Coast as a whole or to their governments as a whole), and they only target designated persons and entities in their individual capacity.

The U.S. sanctions programs also prohibit transactions with persons and entities designated as terrorists, sponsors of terrorist activity and terrorist organizations, narcotics traffickers and kingpins, agents of sanctioned country governments, and proliferators of weapons of mass destruction. These persons and entities are designated by the U.S. Government as Specially Designated Nationals or Blocked Persons (SDNs) and are included on the SDN list, which is maintained by OFAC. [20/](#) The SDN list currently contains more than 6,000 entries, including the names of individuals and entities, as well as other known information (e.g., aliases, date of birth, last known residential or business address, passport number etc.). OFAC regularly updates the SDN list due to frequent additions of newly designated persons and entities (occasionally, certain entries are removed from the SDN list).

Restrictions

Under the comprehensive U.S. sanctions programs, a “U.S. person” generally may not, without a license or authorization from the U.S. Government [21/](#), engage in any of the following:

- Export or import, directly or indirectly, goods, services or technology to and from, a sanctioned country;
- Enter into a contract involving, or otherwise provide services to, a sanctioned country, including an entity or individual located in a sanctioned country;
- Engage in any transaction with persons and entities designated as SDNs;
- Approve or facilitate any of the above activities; and
- Evade provisions of the sanctions regulations.

[19/](#) OFAC regulations governing U.S. economic sanctions programs are found at 31 C.F.R. Parts 500-598.

[20/](#) The SDN list is available at <http://www.treas.gov/offices/enforcement/ofac/sdn/t11sdn.pdf>.

[21/](#) There are comprehensive OFAC sanctions against Cuba, Iran, and Sudan; while the OFAC sanctions against Syria currently are narrow, the U.S. export controls are extremely broad. For most sanctions programs, authorization to conduct a transaction is obtained from OFAC; for certain transactions, U.S. persons must file requests for authorization with the Commerce Department’s Bureau of Industry and Security (BIS).

The prohibitions on exportation and importation of services generally are very broad and apply to services provided or received, directly or indirectly, to or from a sanctioned country or an SDN.

U.S. persons also must “block” (freeze) property and property interests of SDNs, and certain sanctioned country governments, that are within the possession or control of a U.S. person. [22/](#) This includes funds received from or held on behalf of, or a contract involving, an SDN. For example, a U.S. person who receives a payment from an SDN must place such funds into a blocked, interest-bearing account at a U.S. financial institution. In addition, the receipt of such blocked property must be reported to OFAC. Similarly, if a U.S. person has an existing contract with a person who subsequently becomes an SDN, the U.S. person must “block” such contract on its books, preventing any further activity or performance under the contract, and must file a blocked property report with OFAC.

In addition, the comprehensive U.S. sanctions programs have broad prohibitions on approval and facilitation by U.S. persons. For example, U.S. persons are prohibited from participating in, approving or facilitating, aiding or otherwise supporting activities by foreign persons involving a sanctioned country where such actions would constitute violations of the sanctions if engaged in by a U.S. person. Similarly, OFAC interprets the facilitation provision to prohibit a U.S. person from altering its operating policies or procedures, or those of a foreign affiliate, in order to permit a foreign affiliate to engage in transactions involving a sanctioned country that previously required the approval or participation of the U.S. person. Moreover, OFAC regulations prohibit U.S. persons from engaging in any transaction that evades or avoids, or has the purpose of evading or avoiding, the restrictions imposed by U.S. sanctions programs.

Penalties

Significant criminal and civil penalties for violating economic sanctions include monetary fines and imprisonment, and may be imposed on individuals, as well as organizations. Violations also can result in adverse publicity and reputational harm. [23/](#)

[22/](#) Not all of the country-specific sanctions programs have “blocking” provisions (for example, the current U.S. sanctions against Iran do not block the property of the Government of Iran). The broadest restrictions are in the Cuba sanctions program. The terms property and property interests are defined broadly to include all forms of financial interests, whether tangible or intangible, such as bank deposits, savings accounts, real property, leases, letters of credit, money, securities, as well as contracts of any nature. *See generally* 31 C.F.R. §§ 515.311, 538.310.

[23/](#) For most sanctions programs, civil penalties now include a fine of up to \$50,000 per violation (for the Cuban sanctions, the fine is up to \$65,000 per violation; for violations of the Narcotics Kingpin Act sanctions, the fine is up to \$1.075 million). Until recently, the civil penalty amount was limited to \$11,000 per violation. The USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177 (H.R. 3199), which was signed into law on March 9, 2006, amended the International Emergency Economic Powers Act (IEEPA) by increasing the maximum amount of a civil penalty from \$11,000 to \$50,000. Also, the criminal penalty for willful violations by individuals has been increased from 10 to 20 years imprisonment.

V. Compliance Programs

Though it takes a great deal of prudence to comply with the three major export control regimes, you can decrease the chances of inadvertently committing a violation by taking several steps.

- Implement a written statement of management commitment to compliance with export controls and economic sanctions laws.
- Classify your products, software and technology and create an export classification matrix.
- Develop export compliance policies and procedures.
- When dealing with a new product or design, be conscious of the fact that it might be regulated, regardless of how benign the object or technology seems to be.
- Screen all parties that interact with your company, including suppliers, customers, potential hires, employees, distributors, researchers, and any other third party.
- Look for red flags in your commercial dealings. If you receive an order from a company in an industry that generally would not need your product, conduct further investigation before completing a transaction.
- Review transactions involving products, software, raw materials and technical data for export compliance.
 - What is the item or technical data to be exported?
 - Is it subject to the EAR or ITAR?
 - Who are all of the parties in the transaction?
 - Are any parties on any U.S. Government restricted party lists?
 - Does the transaction involve a country subject to sanctions or an embargo?
 - Are there any red flags?
 - Are there any boycott requests?
 - Do I require an export authorization?
- Assign export compliance personnel and responsible officials.
- Develop an export compliance instruction manual and maintain an export compliance intranet site.
- Conduct compliance training.
- Establish an internal export compliance audit function.

Having a compliance program is recommended under U.S. sentencing guidelines and is a strong mitigating factor in any enforcement action. The program should be tailored to the company's assessment of its trade control compliance risks and address in detail those priority risk areas.