Q. Do defense export controls apply to me?

A. Follow this checklist to determine whether you are subject to ITAR

- Find out if what you want to export (hardware, technical data, and/or defense services) is covered in the U.S. Munitions List (USML), found in Part 121 of the ITAR.
- Not sure if your desired export is covered by the USML? File a Commodity Jurisdiction request.
- If what you want to export is on the USML, you must be registered with DDTC.
- After you are registered, you may apply for an export license. D-Trade is the preferred way of licensing.
- Have basic questions you need answered? Call the DDTC Response Team.

Q. What items are covered on the U.S. Munitions List (USML)?

A. The U.S. Munitions List contains twenty-one categories of products and services. These categories are designed to protect military critical technology, but it should be noted that many of the items on the list are considered dual use and may be commercial in nature as well. Listed categories are:

Category I-Firearms

Category II-Artillery Projectors

Category III-Ammunition

Category IV-Launch Vehicles, Guided Missiles, Ballistic Missiles, Rockets, Torpedoes, Bombs and Mines

Category V-Explosives, Propellants, Incendiary Agents, and Their Constituents

Category VI-Vessels of War and Special Naval Equipment

Category VII-Tanks and Military Vehicles

Category VIII-Aircraft, [Spacecraft] and Associated Equipment

Category IX-Military Training Equipment

Category X-Protective Personnel Equipment

Category XI-Military [and Space] Electronics

Category XII-Fire Control, Range Finder, Optical and Guidance and Control Equipment

Category XIII-Auxiliary Military Equipment

Category XIV-Toxicological Agents and Equipment and Radiological Equipment

Category XV-Spacecraft Systems and Associated Equipment

Category XVI-Nuclear Weapons Design and Test Equipment

Category XVII-Classified Articles, Technical Data and Defense Services Not Otherwise Enumerated

Category XVIII-[Reserved]

Category XIX-[Reserved]

Category XX-Submersible Vessels, Oceanographic and Associated Equipment

Category XXI-Miscellaneous Articles

Q. Am I subject to the Export Administration Regulations?

A. See http://www.export.gov and Am I Subject to the EAR?

Export.gov brings together resources from across the U.S. Government to assist American businesses in planning their international sales strategies and succeed in today's global marketplace.

If you need assistance to determine whether the item you want to export requires a license, you should:

- Check the BIS Website http://www.bis.doc.gov, or
- Call one of our export counselors at 202-482-4811 (Washington, DC) or 949-660-0144 (California) for counseling assistance.

Please note that, whether you are the exporter, freight forwarder, consignee, or other party to the transaction, you must address any red flags that arise. Taking part in an export transaction where a license is required but not obtained may subject you to criminal and/or administrative liability.

Q. Are there penalties for failing to comply with ITAR/EAR?

A. ITAR: Sanctions for violations of ITAR include severe criminal and civil penalties. Penalties can include imprisonment of up to ten years and fines of up to $1,000,000 per violation. Criminal sanctions can be imposed on the company defendants as well as officers, directors and employees in their personal capacities. Civil penalties may include debarment which precludes companies selling products and services to the federal government – a costly sanction for a government contracting firm. Additional penalties may include denial of export privileges and seizure of goods being transferred in violation of ITAR.

EAR: Violations of the Export Administration Act may be subject to both criminal and administrative penalties. When the EAA is in effect, criminal penalties can reach 20 years imprisonment and $1 million per violation. Administrative monetary penalties can reach $11,000 per violation, and $120,000 per violation in cases involving items controlled for national security reasons. When the EAA is in lapse, the criminal and administrative penalties are set forth in the International Emergency Economic Powers Act (IEEPA).

On October 16, 2007, President Bush signed into law the International Emergency Economic Powers (IEEPA) Enhancement Act, Public Law No. 110-96, amending IEEPA section 206. The Act enhances criminal and administrative penalties that can be imposed under IEEPA and also amends IEEPA to clarify that civil penalties may be assessed for certain unlawful acts. Criminal penalties can reach $1,000,000 and 20 years imprisonment per violation and the administrative penalties can reach the greater of

$250,000 per violation or twice the amount of the transaction that is the basis of the violation. See Endnote below.

Violators may also be subject to denial of their export privileges. A denial of export privileges prohibits a person from participating in any way in any transaction subject to the EAR. Furthermore, it is unlawful for other businesses and individuals to participate in any way in an export transaction subject to the EAR with a denied person.

Q. How should I manage my compliance actions?

A. Create a Technology Control Plan for your business. A technology control plan (TCP) stipulates how a company will control access to its export-controlled technology and outlines the specific information that has been authorized for release. It is a plan to protect classified and export-controlled information, control access by foreign visitors, and control access by employees who are foreign persons. A TCP is a security countermeasure that is frequently overlooked by companies eager to secure business in the international marketplace. A TCP may be required by the National Industrial Security Program Operating Manual (NISPOM) and the International Traffic in Arms Regulations (ITAR) under certain circumstances. The TCP shall contain procedures to control access and provide disclosure guidelines to all export-controlled information, and should be tailored to a company's operations and the specific threats identified. Counterintelligence organizations can help identify specific threats. See also Targeting U.S. Technologies: A Trend Analysis Of Cleared Industry Reporting.