



P.O. Box 211415
Royal Palm Beach, FL 33421
561.641.5036
www.WeAreCompliant.com

**Attention Exporters:
What You Don't Know Can Hurt You**

By James Anzalone, President

February 12, 2008

Contents

Background	2
The Problem for US Exporters	2
Historically...	3
Benefits of compliance	4
What must companies do to ensure compliance	4
Summary	6
About the author	6

Background

Since the terrorist attacks of 9/11, the U.S. government has taken a serious look at vulnerabilities in the nation's infrastructure in an effort to prevent future exploitation by our enemies. The 'big three' – chemical and biological, nuclear, and missile technology – are frequently mentioned in the news media. Most people give little thought as to how the underlying enabling technologies for these 'big three' are controlled. Even fewer people are aware of the numerous other 'dual-use' technologies controlled by the U.S. government for reasons of national security, anti-terrorism, crime control and regional stability.

Dual-use items are any items that can have both military and commercial applications. These items may appear to be innocuous but, in the hands of the wrong people, can be used for destructive purposes. Examples of dual-use items include communications equipment, machine tools, handcuffs, information security, electronics, lasers, and encryption software. In addition, there are thousands of metals, compounds and chemicals that are controlled because they can be used for military applications.

The issue of control is not limited to the export of items. It also includes technology such as drawing, blueprint and technical 'know how' and software. Technology transfers to non-U.S. persons are referred to as deemed exports. Like product exports of controlled items, deemed exports are controlled by the Department of Commerce, Bureau of Industry and Security (BIS) through the procurement of export licenses.

The Problem for US Exporters

The challenge for our government in controlling the transfer of these technologies

into the wrong hands is also a challenge for U.S. businesses. The Federal regulations governing the control of such technology is contained in Chapter 7 of the Code of Federal Regulations (CFR) Title 15. This section is the Export Administration Regulations or EAR.

Most companies in sensitive industries such as aerospace and defense are well aware of these regulations because most of what they produce is subject the EAR or International Traffic in Arms Regulations (ITAR). The problem is that many firms whose primary business is not considered 'sensitive' are unaware of their obligations under the EAR. Companies are proud to export U.S. products overseas but many have never given much thought to the consequence of these activities.

The penalties for violations of export laws can be severe. Many companies considered household names have paid significant fines for violations of U.S. export laws. Many smaller companies have been penalized as well. Recent examples include a Florida company having paid a \$1,102,200 civil penalty for illegal exports of fingerprint equipment and other crime control items. A New Jersey-based freight forwarder was sentenced to a \$250,000 criminal fine and five years probation as well as a \$399,000 administrative penalty for the shipment of items to India without the required export license. In a deemed export case, a U.S. division of a Japanese company agreed to pay a \$125,000 administrative penalty

for the release of controlled technology to foreign nationals from China and the Ukraine who were employed at their U.S. division to conduct research on the development of commercial digital fiber optic transmission and broadband switching equipment.

The penalties for violations have recently been increased in an effort to improve compliance with the BIS regulations. On October 16, 2007, President Bush signed into law the International Emergency Economic Powers (IEEPA) Enhancement Act. The Act provides for civil penalties amounting to the greater of \$250,000, or twice the value of the transaction that is the basis of the violation, that may be imposed for each violation of IEEPA. Willful violators can expect criminal penalties including fines up to \$1,000,000 and/or up to 20 years in prison.

In addition to civil and criminal penalties, the Department of Commerce regularly publishes the names of companies, their officers, the offense and subsequent penalties in Federal Register notices which are publicly available. This information makes for interesting stories in the financial news and can be used by companies' competitors against them.

Historically...

Prior to the terrorist attacks of 9/11 most Americans did not think much about how our government controls the export of technology. The laws and regulations described here were codified well before 9/11, but most companies did not have an export compliance program in place unless they incurred a violation or were regularly involved in the export of sensitive technologies.

Questions Every Exporter Must Ask

- Have we had all of our items, technology and software classified by the BIS or other competent expert?
- Do we know our customer (i.e. do we check our customers against the government lists of denied parties, specially designated nationals, and other required databases)?
- Have our employees involved in export transactions received the necessary training to ensure compliance?
- Do we have adequate recordkeeping practices in the event of a BIS enforcement audit?
- Do we have a formal export compliance program in place to ensure compliance to U.S. laws and regulations?

Benefits of Compliance

Development and implementing an Export compliance program is not another cost of doing business - it is the law. Firstly, it benefits all free countries by limiting the spread of technologies that can be used for harmful purposes. Secondly, it supports U.S. foreign policy and treaty initiatives. Finally, it promotes U.S. economic objectives.

Avoid Fines and Penalties

The obvious benefit of a compliance program is the avoidance of financial penalties. Understanding your company's potential exposure to violations will allow you to use your

assessment to make the required changes in your export program and greatly reduce the likelihood of incurring civil or criminal penalties. Additionally, having a comprehensive export compliance program is often a mitigating factor in reducing penalties for violations. By the same token, it is often a requirement for those companies that get caught violating export law.

Avoid Bad Publicity

Having your products classified is the first step in ensuring your compliance to the export regulations. Knowing that your organization is not illegally exporting your products will give you the peace of mind that you need in knowing that your firm will not make news in the local or national media. Companies involved in government contracting may also risk debarment from government contracts as a penalty for export violations.

Improved Export Shipment Flow

Having control of your export program can significantly improve the speed and accuracy of your export orders by ensuring that all of the product, license and customer checks are performed up front. Proactive control of exports eliminates order holds and other costly delays allowing your firm to provide world class customer service.

What Must Companies Do To Ensure Compliance

Exporters must first take an inventory of their current state of compliance by answering the questions in the preceding section. A company will likely face some level of exposure to potential violations if it answers "no" to one or more of the questions.

The most important elements of export compliance are knowing your product (note: these may not be your company's products but those that you purchase) and knowing your customer.

Defense articles and services generally fall under the jurisdiction of the Department of State, Directorate of Defense and Trade Controls (DDTC) while most dual-use items are licensed under the BIS. Questions regarding commodity jurisdiction should be addressed to the DDTC. Companies exporting dual-use items should have their products and end-uses of their core technologies reviewed against the Commerce Control List (CCL) by the BIS or an outside expert to determine whether any of the technologies may be controlled for export.

Once products have been classified with their respective Export Control Classification Numbers or ECCN's, they should be cross-referenced against the Commerce Country Chart to determine whether a license is required. Note: there are many valid license exceptions and this determination should be made by a qualified expert.

The second key consideration is knowing your customer. Knowing your customer does not simply mean knowing their name and address. It means knowing what business they are in and how they intend to use your products. For example, the shipment of electronic equipment to China may not be controlled for export, but that same export to the

Beijing Huahang Radio Measurements Research Institute may require an export license. Having a program in place to check the Entity List in Supplement No. 4 to part 744 of the EAR would notify the exporter of this requirement.

The underlying concept behind knowing one's customer is looking for 'red flags'. Red flags are any data points that alert an exporter that the export may be destined for an inappropriate end-use, end-user or destination. The absence of red flags (or express requirement in the EAR) obliges no confirmatory duty upon the exporter to second guess the customer's representations. However, it is incumbent upon the exporter to avoid 'self blinding' behavior. That is, purposeful behavior which restricts the flow of information so as to avoid any knowledge of actual end-use, end-user or country of ultimate destination.

Although companies are not required to second guess their customers representations regarding ultimate destination, they must include a destination control statement on all export documentation. At a minimum, the statement must state: "These commodities, technology or software were exported from the United States in accordance with the Export Administration Regulations. Diversion contrary to U.S. law is prohibited." Companies are also advised to include similar language on quotations, responses to proposals and distributor agreements to avoid entering into contracts that later can not be fulfilled due to a conflict with EAR regulations.

In addition to knowing your products and customers, exporters must abide by the ten general prohibitions stated in Part 736 of the EAR. Does your export manager know and understand these laws?

Summary

The mission of the Department of Commerce – BIS is to advance U.S. national security, foreign policy, and economic objectives by ensuring an effective export controls and treaty compliance system and promoting continued U.S. strategic technology leadership. Achieving this objective is the job of every member of the exporter community.

Maintaining control of your exports is not a cost of doing business. Aside from being the ‘right thing to do’, it can save money, avoid negative publicity and improve export shipment flows. What you don’t know can hurt you.

About the Author

James Anzalone is the president of Compliance Assurance LLC, a firm specializing in global trade compliance solutions.