**Export Controls on Technology Transfers**

**J. F. (Jim) Chester, JD, LL.M, CHB**

**Chester & Jeter LLP**

**6301 Gaston Avenue, Suite 730**

**Dallas, Texas 75214**

**Em** [**jim@chester-law.com**](mailto:jim@chester-law.com)

**Ph 214.382.0755**

**State Bar of Texas**

**advanced IP law course**

**March 20-21, 2014**

**Dallas, Texas**

**J. F. (Jim) Chester**

Chester & Jeter LLP

6301 Gaston Avenue, Suite 730

Dallas, Texas 75214

Email [jim@chester-law.com](mailto:jim@chester-law.com)

Direct 214.382.0755

I am managing partner at Chester & Jeter, LLP, a business and innovation boutique law firm based in Dallas, Texas. In my law practice, I advise entrepreneurs, start-ups and privately-held companies of all sizes in a variety of industries regarding commercial intellectual property (i.e., trademark, copyright, and trade secret) protection, licensing & enforcement in the U.S. and abroad, and I regularly represent clients before the U.S. Patent and Trademark Office and the U.S. Copyright Office.

I also assist companies in international business transactions and joint ventures, and have advised clients on business deals involving over 100 countries. I also coordinate with foreign counsel on legal projects around the world on behalf of U.S. clients, and serve as legal advisor to foreign companies doing business in the U.S. I also have significant experience handling domestic business matters, including entity formations and governance, contracts and commercial transactions, asset and stock acquisitions, and other legal issues commonly faced by innovation-based companies.

My international practice involves advising clients regarding international trade regulations, including compliance and enforcement issues involving Customs/import and export laws, foreign trade zones (FTZs), international trade agreements (e.g., NAFTA, WTO, etc.), ITAR, and the FCPA. I have represented numerous clients before U.S. Customs & Border Protection, U.S. Department of Commerce, U.S. Department of Defense Trade Controls, the Office of Foreign Asset Controls, the U.S. International Trade Administration, and other state, federal and foreign governing bodies and agencies. I am admitted to practice law in Texas, and am also a licensed U.S. Customs Broker.

In addition to my work at the firm, I have been an adjunct professor of law at Baylor University Law School since 2001, teaching courses on international business and trade law. Also, I previously served for four years as an adjunct professor of business law at the University of Dallas.

**HONORS**

* Rated A/V Preeminent® Peer Review Rating by Martindale-Hubble®
* Listed as Rising Star by Texas Super Lawyers in Texas Monthly Magazine.
* Listed as Texas Super Lawyer in Texas Monthly Magazine.
* Listed as “Best Lawyers in Dallas” in D Magazine.
* Fellow, Texas Bar Foundation.
* Fellow, Dallas Bar Foundation.
* Alumni Ambassador Award, Texas A&M University, Commerce (1998).

**EDUCATION**

* LL.M., International Economic Law, University of Houston School of Law, 2000.
* J.D., South Texas College of Law (Law Journal, Varsity Mock Trial), 1997
* B.S., Economics/Political Science, *magna cum laude*, Texas A&M University, Commerce, 1994

**Export Controls on Technology Transfers**

J. F. Chester, JD, LL.M, CHB

**I. Introduction**

It is a well-known fact that the world economy has become an increasingly integrated, and companies of all sizes source or provide their goods and services abroad. While international business transactions are becoming more common each day, they still encompass a degree of risk.

For nations such as the United States, one of the risks is that dangerous or potentially dangerous products or technologies can wind up in the hands of terrorists, drug cartels, or other persons and groups who wish to do harm to America or its allies.

As such, like most other countries that are home to innovative industries, the United States has a comprehensive regime of regulations and processes aimed at supervising and controlling the exports of dangerous or sensitive goods and technology. In some cases, export controls require special licenses prior to exporting certain products or technologies, while other items are prohibited altogether from export to certain countries or individuals.

Of course, while most people expect the export of products such as planes, missiles, and tanks would be tightly restricted and their shipments well scrutinized, international transfers of sensitive technologies and data are often much more difficult to police and contain. In fact, according to U.S. law, some types of technology exports can occur without the technology or data ever leaving the U.S.

By its very nature, technology products such as software, technical data and drawings, are easily transferred (or re-transferred) via USB drive, or with a simple mouse-click via email or Internet download. This article discusses the types of products and technologies that are subject to export restrictions, introduces some of the key U.S. regulatory agencies and their rules, and provides some strategies and recommendations for navigating the various U.S. export controls to ensure compliance.

**II. What are “Exports,” and What Rules and Agencies are involved?**

An export is the transfer of goods, technology, or technical data outside the U.S. Customs Territory, which is essentially the U.S., plus some insular possessions. In a more traditional export transaction, this involves the physical shipment of items from the U.S. to another country via truck, ship or plane. However, an export can also occur when technology or technical data are “shipped” via the Internet or email, such as the download of software from a web site, or the email of a CAD file attachment.

In addition, sharing technology with a foreign national, even on U.S. soil, can be considered an export. Under the “deemed export” rules of U.S. export law, if technology or technical data are displayed, disclosed or otherwise made available to foreign nationals (each, a “release”), for purposes of export control laws, the release is treated as if the technology or technical data were actually shipped or transmitted to the foreign national’s home country. Thus, if export of the technology or technical data to the foreign national’s home country would require an export license, then so would disclosure of the technology or technical data to the foreign national, regardless of the fact that the disclosure might occur in a factory in Dallas or a laboratory in Austin.

A number of U.S. trade laws could be implicated in any given export transaction, including those involving sanctions, the Foreign Corrupt Practice Act, anti-boycott laws, etc. Those laws are beyond the scope of this article, which is focused on those export laws that regulate the transfer of products, technology and technical data from the U.S.

The first step in determining whether a transfer will implicate U.S. export laws is to determine whether the goods, technology or technical data are subject to U.S. export controls. The primary U.S. export laws are based on the Export Administration Act (EAA), and its related Export Administration Regulations (EAR), as well as the more restrictive International Traffic in Arms Regulations (ITAR).

An item is subject to U.S. export regulation if it:

1. Originated in the U.S.;
2. Is a foreign-made product containing parts or materials originated in the U.S;
3. Is software that originated in the U.S. and is commingled with foreign software;
4. Is technology that originated in the U.S. and is commingled with foreign technology; or
5. Is a foreign-made product created by the use of software or technology originating in the U.S.

It is important to note that, once an item is determined to be subject to U.S. export law, it is always subject to U.S. law. Thus, if a subject item is exported to Canada, and then is exported to China a year later, *both* the export from the U.S. to Canada, and the export from Canada to China would implicate U.S. export law.

If the item is *not* subject to export regulation, exporters do not have any obligations under the EAR or ITAR – although other laws such as sanctions and embargoes might still need to be addressed. However, if the export is subject to regulation, exporters must determine whether a license is required prior to export, or else risk a violation of U.S. export law.

Bureau of Industry and Security - EAR

The Bureau of Industry and Security (BIS), an agency within the Department of Commerce, has primary responsibility for enforcing export control laws under the EAR. Other federal agencies have export-specific regulations that must also be observed, such as the EPA’s controls of exports of toxic substances, etc. However, the BIS is responsible for supervising the bulk of U.S. commercial exports, ranging from products as benign as bottled water and pencils, to more sensitive products such as chemicals and body armor. These more sensitive products are often referred to as “dual-use” since they have both civilian and potential military uses.

The “dual use” items are generally those which require a license from BIS prior to shipment. Certain telecommunications, information security and computer equipment are among the technology items specifically controlled by BIS. In addition, technology embodied within or used with EAR-controlled items will often be controlled, as well. Thus, most of the EAR-controlled items contain technology, technical data, software, etc., which may also be subject to export controls.

Although EAR controls must be observed, obtaining a license where needed is generally a relatively quick and easy process. Licenses can generally be obtained online through a BIS portal, and licenses are typically approved.

Department of Defense Trade Controls – ITAR

The Department of Defense Trade Controls (DTC), an agency within the Department of State, is the primary watchdog for items subject to ITAR controls. Such items are listed on the “U.S. Munitions List,” and include items more directly associated with military goods, such as missiles, assault tactical gear, nuclear materials, and military aircraft goods and parts. Of course, in addition to these goods, themselves, any technology or technical data that are used with or embodies within them may be subject to ITAR.

Due to the particularly dangerous subject matter controlled, ITAR controls are much more onerous than EAR controls. License requirements are very specific and lead times a longer.

The decision regarding whether an export is required to follow ITAR or EAR is simple: ITAR trumps EAR. Therefore, if an item is controlled by ITAR, follow ITAR. Otherwise, follow EAR.

Sometimes, an item may not clearly be controlled by ITAR or EAR. In those situations, companies can obtain a ruling from the DTC, called a “Commodity Jurisdiction” or “CJ”, to determine which control regime to follow for the product.

Because of ITAR’s greater restrictions, if a company has an item that could possibly be controlled under EAR or ITAR, when submitting a CJ the company should advocate for a finding by DTC that the goods are EAR controlled.

The information herein is a summary of U.S. export controls and their specific impact on technology transfers from the U.S. For further guidance, I have included chapter excerpts from “Chester’s Handbook of International Business & Trade Law,” an informally published textbook used in the international trade law course at Baylor Law School, as **Appendix A**. The materials in the Appendix A provide a more comprehensive discussion of export controls under EAR and ITAR.

**III. Why is Export Compliance Important?**

Export compliance is critical to U.S. companies, as failure to observe export laws can result in significant penalties.

For violating the EAR or ITAR, companies can face monetary penalties up to five times the value of the export involved or $1 million, whichever is greater. Individual violators risk fines, as well, and may be imprisoned for up to 10 years.

In addition to potential prison sentences and expensive monetary penalties, export violations can result in a number of other punishments, such as seizure and forfeitures of goods (as well as vessels and aircraft involved in the export), and denial of export privileges, which can cripple an export-based company. Furthermore, export enforcement actions can wreak havoc on a company’s operations, personnel, and its business reputation.

Once a company understands why export compliance is important, the next question they often must address is: “How much compliance is needed?”

While U.S. export control law is fairly comprehensive, there are a number of exceptions, not to mention “gray“ areas where regulatory protocol is unclear. Faced with the restrictions, delays and expenses related to export controls, companies often wonder how much compliance is too much. There is no simple answer to this question, and each company must decide what is commercially reasonable, given their products, customers, number of transactions, etc.

To help clients gain perspective on how they should think about export controls, I often ask them to envision a hypothetical in which a tragedy such as a U.S. embassy bombing or similar act of terror has occurred, and the only piece of the harmful device recovered is a small fragment that contains the company’s logo.

That company will be asked questions, most notably: “How could one of your products have ended up in the hands of such bad people?”

If the answer to that question involves a list of compliance checks that show how the company took every commercially feasible action to try to prevent such a thing from happening, while it can’t alleviate the suffering the event causes, few, if any, will blame the company for the tragedy.

If, however, the company simply responds with “we don’t know. . .,” or “we had no reason to believe . . .,” without citing any other checks or protocols that were observed, then the company will be held responsible to some degree, whether by the U.S. government, or in the court of public opinion.

**IV. What is involved in export compliance?**

Export compliance essentially refers to evaluating whether an export item is controlled and, if so, obtaining any necessary approvals or licenses prior to export, and then maintaining good records of the transaction.

Of course, depending on the product and circumstances of the transitions, the details can often involve much more complex issues and analyses.

Generally speaking, export compliance analysis can be summed up by requiring exporters to answer the following questions regarding the items and the transaction:

1. What is it?
2. Where is it going?
3. Who is receiving it?
4. How will it be used?

What

The details of the product or technology to be exported will have a significant impact on the degree of export control involved with its export. First, the exporter must determine whether the item is subject to U.S. export law.

Then, assuming the item is subject to U.S. export law, the exporter must determine whether the item is controlled under EAR or ITAR. Although ITAR and EAR vary substantially in their specific application, the steps for compliance with each are, conceptually speaking, very similar.

Different items are subject to varying levels of control. The specific classification of an item within the EAR or the ITAR will provide the specifics related to the export restrictions, as well as any exceptions or exemptions that may apply.

Most commercial items subject to the EAR are classified under “EAR99,” which enjoy lowest level of export controls. However, even exports of these items might require a license if, for example, some software related to the item contained high levels of encryption.

Where

Once the item is classified within the EAR or ITAR, the next factor in the analysis is the intended destination country of the item. Although the ITAR is generally much more restrictive of all exports, there are a number of countries such as NATO countries, Canada, etc., that enjoy broad exemptions from many of the ITAR export license requirements.

For EAR items, the destination country, when cross referenced with the classification of the item, is a key factor in determining whether an export license will be required. U.S. export controls under the EAR generally restrict exports of certain types of goods to certain groups of countries for specific reasons, such as anti-nuclear proliferation, missile technology controls, etc.

By comparing the type of item and the reasons it is controlled to the destination country and the reasons, if any, that export to that country may be controlled, exporters can determine whether an export license is required prior to shipment.

In addition, the U.S. currently has comprehensive sanctions against entire countries, prohibiting any sort of trade with nationals and entities of the embargoed countries. These sanctions are outside the EAR, and exporters must be aware of these sanctions and avoid any export transactions with the countries or their nationals.

Companies who deliver technology or software via the Internet should ensure they obtain country information from recipients prior to allowing downloads, and should flag any requests from prohibited countries, or from countries that require a license prior to export.

Who

In addition to export controls defined broadly by type of product and destination country, the U.S. restricts trade with specific persons and entities by placing such persons and entities on various “bad guy” lists. The principal reasons persons and entities wind up on such a list is through their involvement with terrorist groups or drug cartels, although some lists punish other activities such as convictions for past export law violations. The fastest way to find your own name on a list is to conduct business with a party already on the list.

Thus, whether or not an export license is required based on the “where” and the ”what”, exporters should check the “bad guy” lists prior to any export transaction.

A number of programs currently exist that allow for automated checks of vendors, customers and business partners against the “bay guy” lists. Given the availability of the information and current technology, a company would have difficulty claiming that failure to check against these lists was commercially unreasonable.

How

For items that have a “dual use”, an exporter must have some reasonable knowledge of how the recipient intends to use the product. For example, if the export item is aircraft control systems software, an export to a civilian airport might not be controlled, while an export of that same software may be controlled if sent to a military airbase.

Exporters has an affirmative duty under U.S. export law not to be willfully ignorant of and “red flags” or suspicious circumstances, and must refrain from continuing any export transaction until the exporter has investigated the circumstances and resolved all suspicions.

Recordkeeping

Finally, exporters must maintain full records of all export transactions for a minimum of five years from the date of export. Failure to produce a record upon request from BIS or ITAR is punishable, in itself, as a recordkeeping violation. In addition, the BIS or DTC might presume that the records were willfully destroyed to hide wrongdoing, and then might enhance the claims and charges again the company.

**VI. How do Export Controls affect Patents (and Vice Versa)?**

The interaction between the U.S. patent application process and U.S. export controls creates some interesting and sometimes confusing situations.

For example, one of the exceptions to when an item is “subject to the EAR” covers technology that has been made “publicly available” 15 CFR §§ 734.3 & 734.7. While that term is defined in the EAR, it is unclear if technology described in patent applications would be exempt from the EAR.

In an opinion from January 2006, the BIS clarified that technology covered in an issued patent, a published patent application, or in an application approved for foreign filing, would be considered outside the scope of the EAR.

However, prior to publication of the patent, the technology would still be controlled by EAR. In addition, because encrypted software is subject to special additional controls, any aspects of the patent relating to such encrypted software might still be subject to U.S. export controls.

That same BIS opinion addresses a number of related patent questions, such as the implications of patents submitted by foreign developers and deemed export requirements. A copy of the January 2006 BIS opinion discussing many of the issues involving patents and export controls is attached as **Appendix B**.

**V. What are some Common Pitfalls**

Although there are a number of ways in which a company can unwittingly run afoul of ITAR and EAR requirements, some common pitfalls include:

No Export/Re-export License.

The most common exporting error is the failure to obtain an export license when one is required. Frequently, the principal reason for the failure is that the company was not aware a license was required.

This generally happens when a company is a novice or infrequent exporter and they have little to no internal export compliance policies. When a violation is discovered, the BIS and DTC can be especially tough on such companies who have not taken export compliance seriously.

Recordkeeping/Reporting.

Although companies are often aware of the hurdles they must overcome when exporting goods and technology, many forget that recordkeeping is a critical part of export compliance.

Not only are there separate penalties for failure to maintain records, the inability to produce a record upon request might actually lead to enhanced penalties for willful or intentional misconduct. Moreover, a missing record might actually have been helpful and exonerated the exporter from any wrongdoing.

Shipments to Affiliates.

When a company exports goods or technology to a subsidiary, developer, vendor, venture partner or some other related party, they often fail to treat the transaction as an export. In some cases, the recipient may actually be a U.S. citizen working abroad.

However, a commercial sale or similar transaction is not required to constitute an “export.” Any transfer of controlled products or technologies outside the U.S. should be treated as an export unless a specific exemption applies.

Email and Downloads.

As previously mentioned, emails, software downloads and similar electronic transfers are exports if they are received by a foreigner or in a foreign country.

Shipments outside Regular Channels.

Companies who regulatory export products often have protocols for handling commercial export shipments. However, when an item is shipped outside the standard channels, the transaction often does not follow those protocols. For example, when engineers request samples or are collaborating with a foreign affiliate, or when defective items are returned for repair.

“Deemed” Exports.

Although already discussed above, Deemed Exports bear repeat mention due to the fact that they can occur although no products or items are actually leaving the U.S. Given the current need in the U.S. for foreign engineers and the activities of foreign interns and students working on research projects, a company might be accidentally exporting controlled technology without even knowing it.

**VI. Keys to Export Compliance**

The key to export compliance is for companies to understand the requirements of export laws and ensure that their employees and agents follow the rules.

A company should develop a written export compliance program, and ensure that all relevant personnel are trained on U.S. export law and the company’s own compliance policies.

For technology-based companies, the scope of employees who need to be aware of such rules should be expanded to include engineers and developers, as well as human resources personnel (i.e., for deemed exports).

After implementing a compliance program and training, a company should periodically check for weaknesses or gaps in its policies by performing internal reviews and audits. Such reviews can help repair flawed protocols, and may uncover violations previously unnoticed, thus cutting off contingent liabilities. For any such violations, the company may choose to voluntarily report itself to the BIS or ITAR, and will typically receive favorable mitigation of any punishment.

**VII. Conclusion**

Exports are subject to a wide range of rules and regulations, and exporters must be mindful of these requirements or risk punishment.

Technology companies are particularly susceptible to inadvertent violations due to the ease and speed in which technology and technical data can be sent abroad.

Failure to be diligent with trade compliance can result in lost opportunities, substantial penalties, and interruptions in global supply chain.

Companies can typically budget and plan for compliance, but not for enforcement.