California Business Law
PRACTITIONER

A GUIDE TO CURRENT PRACTICE

# Export Controls on Commercial Software and Technology

by SANJAY JOSÉ MULLICK

## INTRODUCTION

**Sanjay José Mullick** is an associate with Shaw Pittman LLP, Washington D.C. He received his J.D. from Georgetown University Law Center and his M.S.F.S. from Georgetown University School of Foreign Service. He specializes in international trade.

U.S. export controls cover the transmission of U.S. origin items, such as software and technical data. They also cover the transmission of items out of the United States, regardless of their origin, *e.g.*, sending an e-mail or making information available for download on a website. Anyone doing business on the Internet should be aware of export controls and how to comply with them.

The United States imposes export controls so that it can regulate and control the extent to which certain know-how is shared abroad. Export controls have assumed heightened importance in the last several years because of concerns over terrorism. U.S. export controls are administered principally by three federal agencies: (1) the U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC), which administers export controls on transactions with sanctioned or embargoed countries; (2) the U.S. Department of State, Directorate of Defense Trade Controls (DDTC), which administers export controls on military products and services; and (3) the U.S. Department of Commerce, Bureau of Industry and Security (BIS), which administers export controls on commercial products and technology. (The BIS website, at http://www.bis.doc.gov/, offers helpful information for exporters.)

This article briefly reviews U.S. export controls on commercial products and technology administered by the BIS under the Export Administration Regulations (EAR) (15 CFR pts 730–774). These controls exist because, although the affected products are commercial in nature, they are considered to have the potential for "dual use," *i.e.*, concurrent military or strategic applications. 15 CFR §730.3. The EAR provide a list of "items" (*i.e.*, commodity, software, technology) to which commercial export controls apply, known as the

Reprinted from the California Business Law Practitioner published by Continuing Education of the Bar–California. The citation from this article is 19 CEB Cal Bus L Prac (Fall 2004).

"Commerce Control List" (CCL), at 15 CFR pt 774, Supp No. 1. See "Product Classification—Commerce Control List (CCL), Export Control Classification Number (ECCN)" below. If an item is subject to U.S. export controls, it means that an export license may be required and that certain restrictions may apply on where it may be exported, to whom it may be exported, and for what purpose it may be exported.

Export control issues can arise in many types of software and technology transactions. For example, they arise if a United States company is jointly developing software with one or more parties outside the United States, such as by outsourcing some of the code testing to programmers at an offshore facility. They arise in the license and distribution agreements the company may enter into with U.S. and foreign distributors, who may reexport the software. Finally, they may arise with respect to the company's software sales.

United States persons are responsible for complying with U.S. export controls, regardless of the conduct of any other parties to the transaction. Therefore, a U.S. company cannot simply "contract away" this responsibility when negotiating agreements with other parties. This article reviews compliance issues for managing a company's online export transactions.

***WARNING:*** Export control regulations are exceedingly complex. This article provides an overview of export control analysis as applied to commercial export of software, but practitioners should always consult the EAR directly when advising a client regarding specific transactions. Practitioners unfamiliar with export transactions should consult an experienced international lawyer.

## EXPORT CONTROL ANALYSIS

Export control analysis involves five questions: (1) What is the transaction? (2) What is the product? (3) Who is the recipient of the product? (4) For what purpose will the product be used? (5) What actions are necessary to comply with the regulations? See www.bis.doc.gov/licensing/exportingbasics.htm.

### Transactions Subject to Export Controls

The first step is to determine whether the proposed transaction is covered by export controls. Any "item" (*i.e.*, commodity, software, technology) *in* the United States may be subject to the Export Administration Regulations (EAR). 15 CFR §734.3(a)(1). Any U.S.-origin item on the Commerce Control List (CCL) (see "Product Classification—Commerce Control List (CCL), Export Control Classification Number (ECCN)," below) may be subject to the EAR, even if it is *outside* the United States. 15 CFR §734.3(a)(2). Even certain items not specifically identified on the CCL may be subject to the EAR, unless they are publicly available. 15 CFR §734.3(b)(3), (c). A foreign-origin item may also be subject to the EAR if it contains a threshold amount of "U.S. content," or if it is exported or reexported from the United States. See 15 CFR §734.3(a)(3).

### Definition of "Export"

The common notion of an export is a physical shipment of tangible merchandise out of the United States to a foreign country. For export control purposes, however, the definition of "export" is much broader. Under the EAR, an export is defined as follows (15 CFR §734.2(b)(1)):

> "Export" means an actual shipment or transmission of items subject to the EAR out of the United States, or release of technology or software subject to the EAR to a foreign national in the United States.

Because an export includes a "transmission" of items out of the United States, it could include sending an e-mail or making information available for download on a website. See, *e.g.*, 15 CFR §734.2(b)(9)(i)(A). Thus, the term "export" would include an engineer e-mailing technical specifications concerning the company's software to an offshore programming facility in India, or a sales representative instructing a customer in Singapore on how to download encryption software from the company's website.

In addition, an export includes a "release" of technology. This could include providing technical information or assistance, even informally. See 15 CFR §§734.2(b)(2)(i), (b)(3). For example, it could include a developer's explanation of how to change a software program's encryption to officials of a Spanish company meeting at a trade show in Chile.

**Because an export includes a "transmission" of items out of the United States, it could include sending an e-mail or making information available for download on a website.**

An export also includes a release of software (in source code) or technology to a foreign national, even if the foreign national is located within the United States. 15 CFR §734.2(b)(2)(ii). This could include making the item or information available for visual inspection by foreign nationals, orally exchanging information, or applying abroad technical experience acquired in the United States. 15 CFR §734.2(b)(3). For example, it could include a company manager training an employee, who is a foreign national of China, on how to debug the software at the company's headquarters in California. Because a "foreign national" is an individual who is neither a U.S. citi-

zen nor a U.S. lawful permanent resident (*i.e.*, green card holder), such a transaction is deemed an export because it is considered to be the same as actually exporting that item or information to the foreign national's country. 15 CFR §734.2(b)(2)(ii).

### Fines and Penalties for Violations

Violations of the EAR are punishable with severe sanctions, including criminal and civil penalties. Companies may be fined up to the greater of $1 million or five times the value of the exports for each violation. 15 CFR §764.3(b)(2)(i). Individuals may be fined up to $250,000 or imprisoned for up to ten years for each violation. 15 CFR §764.3(b)(2)(i). In addition, any violation of the EAR may also result in the imposition of a civil penalty of up to $120,000 for each violation, as well as the suspension or revocation of the authority to export goods or technology from the United States or to receive or participate in an export from the United States. 15 CFR §§6.4(a)(6), (7), 764.3(a)(1)(i), (a)(2). Note that because the Export Administration Act of 1979 expired in 2001, the provisions above have continued in effect under the International Emergency Economic Powers Act (50 USC §§1701–1706).

## PRODUCT CLASSIFICATION

If the company will be engaged in an export transaction, it will next need to identify how the product is classified for export control purposes.

### Commerce Control List (CCL), Export Control Classification Number (ECCN)

The Commerce Control List (CCL) (15 CFR pt 774, Supp No. 1) is a comprehensive listing and description of categories of items subject to export controls. Of its ten categories, the three categories usually most relevant to software companies are: Category 3: Electronics; Category 4: Computers; and Category 5: Telecommunications and Information Security (encryption capability). See 15 CFR §738.2(a). Each category is divided into groups, and each group comprises individual types of products identified by an alphanumeric code called an Export Control Classification Number (ECCN). See 15 CFR §738.2(d). The ECCN identifies the section and category in which the product is listed, as well as the reasons why export of the product is controlled, *e.g.*, anti-terrorism (identified as "9") or national security (identified as "0"). For example, ECCN 5D002 identifies software with encryption controlled for purposes of national security. Even if a product does not fall under a specific ECCN, it will still be subject to the EAR if it is classified as EAR99, which is a general designation on the CCL. 15 CFR §§734.3(c), 732.3(d)(5). The export control restrictions applicable to these classifications are reviewed in "Development, Distribution, and Sales" below.

### Country Chart

Included in the Commerce Control List (CCL) is a Country Chart that indicates the controls applied to different countries. If the Export Control Classification Number (ECCN) listing identifies a reason for control that matches one marked for the particular country of export, it means that the export of that product to that country would require a license, unless a license exception applies. The Country Chart is located at 15 CFR pt 738, Supp No. 1. Generally, the level of control for each ECCN depends on the ultimate destination to which it will be exported. For example, anti-terrorism export controls apply only with respect to six countries (Cuba, Iran, Libya, North Korea, Sudan, and Syria), but national security export controls can apply with respect to several countries. See "Software With Encryption," below. The more "reasons for control" that apply to an item, the greater the likelihood that its export will require a license.

### Software Without Encryption

#### Publicly Available Software

For software without encryption, the first question to ask is whether it is publicly available. "Publicly available" software is defined as that which (1) has already been or will be made generally available to the public by being published; (2) arises during, or results from, certain fundamental research; (3) is released by instruction at academic institutions; or (4) is included in certain patent applications. 15 CFR §734.3(b)(3). Publicly available software is *not* subject to the EAR, although export controls administered by other agencies for other purposes may still apply (*e.g.*, embargoes). 15 CFR §734.3(b)(3).

#### Object Code or Source Code

In the more likely event that the company is exporting proprietary software, the next question to ask is whether the software without encryption is in object code or source code. See 15 CFR §772.1. The EAR defines "object code" to be "[a]n equipment executable form of a convenient expression of one or more processes ('source code') that has been converted by a programming system," and "source code" to be "[a] convenient expression of one or more processes that may be turned by a programming system into equipment executable form ('object code')." 15 CFR §772.1. In short, software in object code is a program that can be directly executed by a computer, while software in source code provides the instructions for that program. If the software is in object code, it will likely be classified as EAR99. If it is in source code, the next question to ask is whether it is for an application or for an

operating system. If the source code is for an application, it will still likely be classified as EAR99. If it is for an operating system, however, it may be classified as ECCN 4D003, meaning "operating system software . . . designed for multi-data stream processing equipment, in source code." 15 CFR pt 774, Supp No. 1. An export license would be required to export such source code to countries for which national security and/or anti-terrorism controls apply.

### Software Incorporated in Computer Hardware

In some cases, software will be exported when incorporated into computer hardware. The most common classification for high performance computers is ECCN 4A003. Although the export of such computers is controlled to several countries, these computers are usually eligible for an exception to the licensing requirement known as License Exception CTP (Computers). See 15 CFR §740.7. CTP (which stands for composite theoretical performance) measures a computer's computational performance in "millions of theoretical operations per second" (MTOPS). 15 CFR pt 774, Supp No. 1. Under License Exception CTP, computers of up to 190,000 MTOPS may be exported without a license, except to Cuba, Iran, Libya, North Korea, Sudan, and Syria, or foreign nationals of those countries. See 15 CFR §§740.7(b)(2), (d)(2), 742.12(a)(2), (b)(4)(i). Because of the general availability of this license exception for computer hardware, the classification and licensing requirements for the entire item will usually be determined by the software.

## Software With Encryption

Software with encryption is subject to special export controls. Encryption refers to the process of encoding text and data, akin to scrambling. When information is encrypted, it cannot be read or understood unless the recipient has a "key" to decipher the code. Information can be encrypted using one of two types of mathematical computer instructions (algorithms): (1) a "symmetric" one, which uses the same key both to encrypt and to decrypt, and (2) an "asymmetric" one, which uses one key to encrypt and a different key to decrypt. See generally Becker, *U.S. Restrictions on Exports of Cryptographic Equipment and Software*, 32 J World Trade 6 (1998). Encryption can thus be used to transmit information in secret, and encryption techniques can also be used to decipher encrypted information transmitted by others. See 15 CFR §742.15.

**Software with encryption is subject to special export controls.**

Encryption items generally can be divided into two groups: those with "weak" encryption and those with "strong" encryption. Encryption strength is determined by the number of binary digits (bits) in the key length, which is a measure of how many combinations of keys with an encryption algorithm would be required to obtain a readable text.

### "Weak" Encryption Software

The BIS considers items with "weak" encryption to include those with limited cryptographic functionality that do not allow for encryption of files or text, as well as those that perform only authentication functions. Weak encryption software is usually classified as ECCN 5D992. The export of weak encryption software is generally controlled only for anti-terrorism purposes, *i.e.,* to countries considered to be terrorist-supporting. See 15 CFR pt 774, Supp No. 1, Category 5, Information Security, ECCN 5D992.

*Limited Cryptographic Functionality.* Items with limited cryptographic functionality include certain wireless products that provide encryption functions only over an operating range typically not exceeding 100 meters, such as "Bluetooth" and "Wi-Fi." 15 CFR §742.15(b)(3)(ii). Items with limited cryptographic functionality also include "finance specific items," which are items limited to banking use or financial transactions, such as the collection and settlement of fares or credit functions. 15 CFR §742.15(b)(3)(iii), 15 CFR pt 774, Supp No. 1.

*Authentication Items.* Authentication items are those that provide only access control, meaning that they perform encryption only for the protection of passwords, Personal Identification Numbers (PINs), or similar data to prevent unauthorized access. 15 CFR pt 774, Supp No. 1, Category 5, Technical Note 2. Such items may include "personalized smart cards," those that provide for digital signature, and those that permit execution of copy-protected software. 15 CFR pt 774, Supp No. 1, ECCN 5A002, 15 CFR §742.15 (b)(3)(iii).

### "Strong" Encryption Software

For a "strong" encryption item, the level of control depends on whether or not it is "mass market" and on the number of bits of the key length for the symmetric algorithm. Strong encryption software is usually classified as ECCN 5D002.

*Mass Market Items.* A "mass market" item is defined as one that is generally available to the public for sale from stock at retail selling points in over-the-counter, mail order, online, or telephone transactions. 15 CFR pt 774, Supp No. 1, Category 5, Information Security, Cryptography Note 3. A mass market item is also one in which the cryptographic functionality cannot be easily changed by the user and which is designed for installation by the user without further substantial support by the supplier.

15 CFR pt 774, Supp No. 1, Category 5, Information Security, Cryptography Note 3. Examples of mass market items include (15 CFR §742.15(b)(5)):

- General purpose operating systems and desktop applications designed for, bundled with, or pre-loaded on single CPU computers, laptops, or hand-held devices (*e.g.,* e-mail, certain web browsers, games, word processing, database, financial applications, and utilities);
- Commodities and software for client Internet appliances and client wireless LAN devices;
- Home use networking commodities and software (*e.g.,* personal firewalls, cable modems for personal computers, and consumer set-top boxes);
- Portable or mobile civil telecommunications commodities and software (*e.g.,* personal digital assistants (PDAs), radios, and cellular products); and
- Commodities and software exported via free or anonymous downloads.

Mass market software with no key length greater than 64 bits for the symmetric algorithm is controlled only for anti-terrorism. Otherwise, it is controlled for national security as well as anti-terrorism purposes. If an item is controlled for national security purposes, there are many more countries for which an export license will be required. 15 CFR §742.15(b)(1)(i), (b)(2).

*Non-Mass Market Items.* If software with strong encryption does not qualify as mass market, it may still be classified under ECCN 5D992 and be controlled only for anti-terrorism purposes if it implements key lengths not exceeding 56 bits for symmetric algorithms, 512 bits for asymmetric key exchange algorithms, or 112 bits for elliptic curve algorithms. 15 CFR §742.15(b)(1)(ii). Otherwise, it will be classified under ECCN 5D002 and be controlled for both national security and anti-terrorism purposes.

## Classification Procedures

Although an exporter may attempt to "self-classify" an item under the EAR, only a formal BIS classification ruling is binding for export control purposes. 15 CFR §748.3(a). Depending on whether the product contains encryption, the BIS may require formal classification before export, and the BIS suggests that exporters submit encryption items for formal classification if the exporter is unsure of the classification. 15 CFR §742.15(b)(1).

### Commodity Classification Requests

There are different procedures applicable to classification of products with and without encryption capability. See 15 CFR §742.15(b)(1); 15 CFR pt 742, Supp No. 6; 15 CFR §§748.3(b), 748.4; 15 CFR pt 748, Supp No. 1. For helpful guidance on filing a commodity classification request with the BIS, see http://www.bis.doc.gov/licensing/cclrequestguidance.html. A commodity classification request may be filed by a party other than the product's manufacturer. 15 CFR §748.3(a). The applicant must complete a BIS-748P form and submit a description of the product, its uses, and its technical specifications in sufficient detail for the BIS to make its ruling. 15 CFR pt 748, Supp No. 1. The applicant must also identify the ECCN that it believes is applicable and set forth its reasons in support of that classification. 15 CFR §748.3(b)(2). An exporter or its representative may request classification of up to six items in one classification request. 15 CFR §748.3(b)(1). All information in a request is kept confidential by the BIS and will not be disclosed to the public or third parties. 15 CFR §748.1(c).

**If an item is controlled for national security purposes, there are many more countries for which an export license will be required.**

### Notification

For encryption items, the BIS generally requires advance notification of any export of mass market items with a symmetric key length of 64 bits or less, or non-mass market items with either a symmetric key length of 56 bits or less, an asymmetric key length of 512 bits or less, or an elliptic curve key length of 112 bits or less. 15 CFR §742.15(b)(1). In addition to the information required in a classification request, the notification must include responses to a series of questions asking for, among other things, an explanation of the product's encryption algorithms and key lengths, encryption modes, and communications protocols. 15 CFR pt 742, Supp No. 6. If applicable, the notification must also provide specific information on how the product qualifies for mass market treatment. 15 CFR §742.15(b)(1). No notification is required for certain wireless commodities or software, as well as items with certain limited cryptographic functionality (*e.g.,* finance specific items and authentication items).

### ENC Review Request

Exporters of encryption products with "strong" encryption, including certain mass market items, are required to submit their products for a one-time review before export under License Exception ENC (Encryption Commodities and Software). 15 CFR §742.15(a)(1). Absent this provision, exporters would be required in many cases to obtain a license to export these products because they are controlled for national security reasons. Compliance with License Exception ENC, however, eliminates the license requirement. License Exception ENC is discussed further

in "Compliance Measures; Reporting and Recordkeeping," below. Once a product is classified under ENC, it may be upgraded to an increased key length without further review, provided that the exporter certifies that there is no other change in cryptographic functionality. 15 CFR §740.17(d)(3).

## DEVELOPMENT, DISTRIBUTION, AND SALES

Once the product is classified, the next step is to determine whether an export license is required to provide the item to others. Most commercial software can be exported either outright without a license or after qualifying for a license exception.

### General Rules

#### Software Without Encryption

Even if the Commerce Control List (CCL) and Country Chart do not require an export license, the Export Administration Regulations (15 CFR pts 730–774) require a license to export software without encryption to certain end users or for certain end uses. See "Compliance Measures; Prohibited End Users" and "Prohibited End Uses," below. To cover these situations, the EAR includes the classification EAR99. 15 CFR §732.3(d)(5). Although a product classified as EAR99 does not fall under a specific ECCN subject to country restrictions, it is still subject to end user and end use restrictions. 15 CFR §732.3(h)(1).

#### Software With Encryption

The rules noted in "Software Without Encryption," above, apply to all software, but software with encryption is subject to certain additional rules, depending on whether the software is for internal company use only or whether it will be transferred outside the company. The rules for software with weak encryption (classified as ECCN 5D992) apply to software in both source code and object code, while the rules for software with strong encryption (classified as ECCN 5D002) apply to object code only.

Software with either weak or strong encryption may be exported to foreign subsidiaries of U.S. companies without prior notification or review by the BIS, if the item is for internal company use. 15 CFR §§742.15(b)(3)(i), 740.17(b)(1). Providing encryption software in source code or technology to foreign nationals working as contractors, interns, or employees of U.S. companies in the U.S., or their foreign subsidiaries, is not deemed to be an export if the software is for internal company use. 15 CFR §740.17(b)(1). Software in object code does not trigger the deemed export rule.

**Software with either weak or strong encryption may be exported to foreign subsidiaries of U.S. companies without prior notification or review by the BIS, if the item is for internal company use.**

All items produced or developed by U.S. subsidiaries (see "U.S. Subsidiaries," below) with weak or strong encryption software, however, must be submitted to the BIS for review and authorization before any sale or retransfer outside of the U.S. company. 15 CFR §§742.15(b)(3)(i), 740.17(b)(1). Note that this provision permits exports to subsidiaries of any U.S. company, not just from the U.S. parent to its own subsidiary.

*U.S. Subsidiaries.* The Export Administration Regulations (EAR) (15 CFR pts 730–774) define a "U.S. subsidiary" as a "foreign branch of a U.S. company," or a "foreign subsidiary or entity of a U.S. entity" in which (1) the U.S. entity beneficially owns or controls (directly or indirectly) 25 percent or more of the voting securities of the foreign subsidiary or entity, if no other person owns or controls (directly or indirectly) an equal or larger percentage; (2) the foreign entity is operated by the U.S. entity under the provisions of an exclusive management contract; (3) a majority of the members of the board of directors of the foreign subsidiary or entity also are members of the comparable governing body of the U.S. entity; (4) the U.S. entity has the authority to appoint the majority of the members of the board of directors of the foreign subsidiary or entity; or (5) the U.S. entity has the authority to appoint the chief operating officer of the foreign subsidiary or entity. 15 CFR §772.1.

*"Prohibited" Countries.* No encryption item may be exported to any end-user (including a U.S. subsidiary) in Cuba, Iran, Libya, North Korea, Sudan, or Syria ("prohibited" countries). 15 CFR §740.17. These are the six countries for which exports are controlled for anti-terrorism purposes and to which the BIS generally adopts a "policy of denial" toward export license applications. See, *e.g.*, 15 CFR §746.1(a)(1). As of July 30, 2004, the BIS removed Iraq from this list. 69 Fed Reg 46069. In addition, no encryption source code or technology may be exported to a national of any of these countries, wherever that person may be located. 15 CFR §740.17. Anyone considering making an export to Iraq or any of these six countries should first consult legal counsel. Further, U. S. embargos administered by the U. S. Department of the Treasury's Office of Foreign Assets Control (OFAC) completely prohibit any transactions with certain countries. 31 CFR pts 500–597. The list of countries for which the United States maintains an embargo may be accessed on the OFAC website at http://www.treas.gov/offices/enforcement/ofac/.

**[B]oth strong and weak encryption software may be exported to Canada without regard to notification or review requirements.**

*"Preferred" Countries.* Software with weak encryption may be exported to both government and non-government end users in any non-prohibited country after submitting a notification to the BIS. 15 CFR §742.15(b). Software with strong encryption may be exported to both government and non-government end users in Austria, Australia, Belgium, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Poland, Portugal, Spain, Sweden, Switzerland, and the United Kingdom ("preferred" countries) after the information required for a one-time review is "registered" with the BIS. 15 CFR pt 740, Supp No. 3; 15 CFR §742.15(b)(2)(iii). An application is "registered" with the BIS when it is entered into the BIS's electronic export license tracking system. 15 CFR §750.4(a)(2). Note that both strong and weak encryption software may be exported to Canada without regard to notification or review requirements. 15 CFR §742.15(a)(1).

*"Permitted" Countries.* For all countries that are not either "prohibited" countries or "preferred" countries ("permitted" countries), exports of encryption items are permitted, but not to the same extent as exports to preferred countries. As noted with regard to preferred countries above, software with weak encryption (classified as ECCN 5D992) may be exported to any non-prohibited country end-user after notifying the BIS. Software with strong encryption (classified as ECCN 5D002), however, may be exported only to non-government end users in the permitted countries 30 days after the BIS registers the one-time review application. 15 CFR §740.17(b)(2). Whether strong encryption software may later also be exported to government end users depends on whether the BIS rules that the software is either a mass market or retail item. Items that qualify may be exported to both types of end users while those that do not qualify may be exported only to nongovernment end users. 15 CFR §740.17(b)(3).

*"Retail" Encryption Items.* Like mass market items, which generally involve non-ENC items, similar items subject to License Exception ENC can be designated as "retail." Such items include those generally available to the public by being (1) sold through retail outlets independent of the manufacturer; (2) sold (or to be sold) in large volume through mail order, online, or telephone transactions; and (3) specially designed for individual customer use, which also have cryptographic functionality that cannot easily be changed by the user, do not require substantial support for installation and use, and do not have cryptographic functionality that has been modified or customized to a customer's specification. 15 CFR §740.17(b)(3)(i). The regulations specify maximum key lengths for retail encryption products (64 bits for symmetric algorithms, 1024 bits for asymmetric key exchange algorithms, and 160 bits for elliptic curve algorithms). See 15 CFR §740.17(b)(3)(ii)(A). The regulations also include a helpful list of specific products that qualify as retail encryption items, as follows (15 CFR §740.17(b)(3)(iii)):

- General purpose operating systems that do not qualify as mass market;
- Desktop applications (*e.g.,* email, browsers, games, word processing, database, financial applications, or utilities) that do not qualify as mass market;
- Short-range wireless components and software that do not qualify as mass market;
- Nonprogrammable encryption chips, and chips that are constrained by design for retail products;
- Retail networking products, such as low-end routers, firewalls, and virtual private networking (VPN) equipment designed for small office or home use;
- Programmable database management systems and associated application servers;
- Low-end servers and application-specific servers (including client-server applications, *e.g.,* Secure Socket Layer (SSL)-based web applications and applets, servers, and portals); and
- Network and security management products designed for, bundled with, or pre-loaded on single CPU computers, low-end servers, or retail networking products.

Retail items also include those encryption products and network-based applications that provide "equivalent functionality" to other mass market or retail encryption items. 15 CFR §740.17(b)(3)(ii)(B).

A determination that an encryption item qualifies as retail requires a BIS review. If the BIS rules that the item qualifies as retail, strong encryption items (classified as 5D002) may be exported to both government and non-government end users in "permitted" countries. 15 CFR §740.17(b)(3).

### "Cryptanalytic" Items

"Cryptanalytic" items may be exported only to non-government end users. 15 CFR §740.17(a). A "cryptanalytic" item is defined as one that engages in the "analysis of a cryptographic system," *i.e.,* an encryption "decoder" or "breaker." 15 CFR pt §772.1.

There are other restrictions on "cryptanalytic" items. An item with an "open cryptographic interface" may be exported only to "preferred" countries. 15 CFR §§740.17(a), (b)(2). The Export Administration Regula-

tions (15 CFR §§730–774) define an "open cryptographic interface" as (15 CFR pt 772.1):

[A] mechanism which is designed to allow a customer or other party to insert cryptographic functionality without the intervention, help or assistance of the manufacturer or its agents, *e.g.,* manufacturer's signing of cryptographic code or proprietary interfaces.

In an item with an open cryptographic interface, a party can change the cryptographic algorithms, key lengths, or key exchange mechanisms. 15 CFR pt 772.1, §740.17(a)(5)(ii). The regulations provide that if the (15 CFR pt 772.1):

cryptographic interface implements a fixed set of cryptographic algorithms, key lengths or key exchange management systems, that cannot be changed, it will not be considered an "open" cryptographic interface.

## Special Rules

### Beta Test Software

Beta test software may be exported under License Exception TMP (Temporary Exports), except to prohibited countries. 15 CFR §740.9(c)(2). For beta test software to be eligible for this license exception, the software producer must intend to market the software to the general public after completion of beta testing. 15 CFR §740.9(c)(4)(i). In addition, the software producer must provide the beta test software to the consignee free of charge (or at a price not exceeding the cost of reproduction and distribution), and the software must be designed for installation by the end user without further substantial support from the supplier. 15 CFR §740.9(c)(4)(ii), (iii).

For strong encryption beta test software (classified as ECCN 5D002), the producer must give the BIS advance notice prior to export, with the names and addresses of the testers (except for individuals) and the name(s) and version of the software to be tested. 15 CFR §740.9(c)(8). Before exporting the software, the exporter must obtain the following statement from the tester (15 CFR §740.9(c)(5)):

**We certify that this beta test software will only be used for beta testing purposes, and will not be rented, leased, sold, sublicensed, assigned, or otherwise transferred. Further, we certify that we will not transfer or export any product, process, or service that is the direct product of the beta test software.**

All beta test software must be destroyed or returned to the exporter within 30 days of the end of the testing period. 15 CFR §740.9(c)(7).

### Encryption Source Code

The rules for export of encryption source code vary depending on the source code's technical classification. See 15 CFR §§740.17(b)(2)(ii), 742.15(b). It is permissible to export weak encryption source code (classified as ECCN 5D992) employing no symmetric key length greater than 64 bits after filing a notification with the BIS. 15 CFR §742.15(b)(1). Encryption source code employing a symmetric key length greater than 64 bits and encryption source code otherwise classified as ECCN 5D002 may be exported to nongovernment end users after filing with the BIS an application for one-time review along with a copy of the source code. 15 CFR §§742.15(b)(2), 740.17(b)(2)(ii).

Encryption source code may not knowingly be exported to any of the prohibited countries. 15 CFR §740.13(e)(4).

### Publicly Available Source Code

Source code may be exported without BIS review if it is "publicly available." See 15 CFR §734.3(b)(3). As discussed in "Product Classification; Software Without Encryption; Publicly Available Software," above, publicly available source code is that which (1) has already been or will be made generally available to the public by being published; (2) arises during, or results from, certain fundamental research; (3) is released by instruction at academic institutions; or (4) is included in certain patent applications. 15 CFR §734.3(b)(3). Source code may still be considered publicly available even if it is subject to an express agreement for the payment of a licensing fee or royalty for commercial production or sale of any product developed using the source code. 15 CFR §740.13(e)(2). Before exporting publicly available source code, the exporter must provide the BIS with either a copy of the source code or the Internet location where it is posted. 15 CFR §740.13(e)(5).

### Related Technology

In addition to the software itself, it may also be necessary to export associated "technology," particularly when jointly developing software with foreign entities or when engaging foreign distributors to market and sell the software. The Export Administration Regulations (15 CFR pts 730–774) define "technology" as (15 CFR §772.1):

[s]pecific information necessary for the "development," "production," or "use" of a product. The information takes the form of technical data or technical assistance.

The regulations state that technical assistance may take forms such as instruction, skills training, working knowledge, and consulting services, and that it may involve the transfer of technical data. The regulations provide that "technical data" may (15 CFR §772.1):

take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and

instructions written or recorded on other media or devices such as disk, tape, read-only memories.

The export of technology often provides a foreign national with the greatest opportunity to understand or reproduce a product.

*License Exceptions for Related Technology.* Although exports of technology are generally more regulated than exports of corresponding equipment or software, certain license exceptions may be available for technology related to software products. License Exception TSU (Technology and Software Unrestricted) authorizes the export of "operation technology," which is defined as "the minimum technology necessary for the installation, operation, maintenance (checking), and repair" of the underlying products. 15 CFR §740.13(a). This exception also authorizes the export of "sales technology," which is defined as "data supporting a prospective or actual quotation, bid, or offer to sell, lease, or otherwise supply any item." 15 CFR §740.13(b). License Exception TSR (Technology and Software Under Restriction) authorizes the export of technology sufficient for a product's development or production, but only to specified countries. See 15 CFR §740.6(a).

*As Applied to Encryption Items.* The license exceptions discussed above may not apply to exports of encryption technology. Certain types of encryption technology may be exported to any end users, except ones in a prohibited country or foreign nationals thereof, without regard to a license or license exception, provided that notification and review requirements have been met. See 15 CFR §742.15(a)(2)(i). If such encryption technology has certain limited cryptographic functionality, exports are allowed to most destinations without notification and review. 15 CFR §742(b)(3)(iii). This would include technology for finance-specific items and for authentication items (see "Product Classification; Software With Encryption; 'Weak' Encryption Items," above). After filing a notification with the BIS, it would also include mass market items with no key length exceeding 64 bits in the symmetric algorithm and non-mass market items with no key length exceeding 56 bits in the symmetric algorithm. 15 CFR §740.13(d)(2).

**Although exports of technology are generally more regulated than exports of corresponding equipment or software, certain license exceptions may be available for technology related to software products.**

Certain other types of encryption technology, however, may be exported without a license only to U.S. subsidiaries, or to the preferred countries after filing an application for one-time review. 15 CFR §§740.17(b), 744.9(a). Any export of such encryption technology to any other destination or end user requires a license.

### Software and Technology Developed Abroad

Exporters must be mindful of U.S. export controls even when developing software abroad. Foreign-origin items incorporating controlled U.S. content are subject to the Export Administration Regulations (15 CFR §§730–774) unless they qualify for de mimimis treatment. 15 CFR §734.3(a)(3). Under the de minimis rule, if the value of U.S. software incorporated into foreign-origin software is 25 percent or less of the total value of the product, the end product will not be subject to the EAR. 15 CFR §734.4(d)(2). The de minimis threshold drops to 10 percent for exports to embargoed or prohibited countries. 15 CFR §734.4(c)(2). The value of the U.S. content is its "delivered cost" to the foreign developer under an arm's-length transaction, while the value of the foreign content is the "normal selling price (f.o.b. factory)" of the foreign end product, excluding value-added taxes or excise taxes. 15 CFR pt 734, Supp No. 2(a)(1)–(2).

Exporters seeking to obtain de minimis treatment to exempt the foreign end product from the EAR must first file a one-time report with the BIS 30 days before export. 15 CFR pt 734, Supp No. 2(b). The report must include (1) a description of the foreign software and its fair market value, along with the rationale and basis for its selection and valuation, and (2) the percentage of U.S.-content value and the basis (assumptions and methodologies) of its calculation. 15 CFR pt 734, Supp No. 2(b)(1), (4). The report does not need to include information regarding destinations or end users. 15 CFR pt 734, Supp No. 2(b)(4). The exporter may accord de minimis treatment to the foreign end product 30 days after filing the report, unless the BIS advises to the contrary. 15 CFR pt 734, Supp No. 2(b)(5).

Special rules apply to source code and encryption software developed abroad.

## COMPLIANCE MEASURES

A U.S. company is responsible for ensuring that it does not knowingly violate U.S. export controls and must caution recipients of its products and technology not to violate U.S. export controls. In addition, the company should take steps to protect itself should export control violations occur without its knowledge. Implementing effective compliance measures requires a company to understand and document its transactions.

### Knowledge of Export Control Violations

No export to any country may be made if the exporter has "reason to know" that the item will in turn be reexported to an embargoed country, a prohibited country, a

foreign national of one of those countries, or anyone on the lists discussed in "Prohibited End Users," below. 15 CFR §§736.1(c), 736.2. The Export Administration Regulations (15 CFR pts 730–774) define "knowledge" as follows (15 CFR §772.1):

> Knowledge of a circumstance (the term may be a variant, such as "know," "reason to know," or "reason to believe") includes not only positive knowledge that the circumstance exists or is substantially certain to occur, but also an awareness of a high probability of its existence or future occurrence. Such awareness is inferred from evidence of the conscious disregard of facts known to a person and is also inferred from a person's willful avoidance of facts.

An exporter may therefore be liable if it had an awareness of a high probability of a present or future export control violation, not only if it had actual knowledge of a violation. Accordingly, for every export transaction, the exporter should know the ultimate destination, the end user, and the end use of an item, or else be able to demonstrate that it made a sufficient inquiry about the same.

**If there are red flags, . . . the exporter has an affirmative duty to inquire, and must obtain documentary evidence concerning the suspicious aspects of the transaction.**

The EAR provides a set of six illustrative due diligence measures that should be undertaken for every export transaction to "know your customer" and to check for "red flags." See 15 CFR pt 732, Supp No. 3 ("Know Your Customer" Guidance). The regulations list a series of indicators, termed "red flags," that should create suspicion that an export control violation may occur. See 15 CFR pt 732, Supp No. 3 ("Red Flags"). Indicators that the regulations list as possible "red flags" include the following:

- The customer is reluctant to offer information about the end use of the product;
- The customer is evasive about whether the product is for domestic use, export, or reexport;
- The product's capabilities do not fit the buyer's line of business; and
- The shipping route is abnormal for the product and destination.

If there are no red flags, the exporter can rely on the customer's representations and is under no obligation to verify them or inquire further. If there are red flags, however, the exporter has an affirmative duty to inquire, and must obtain documentary evidence concerning the suspicious aspects of the transaction. If questions still remain, the exporter should not complete the transaction and should advise the BIS. See 15 CFR pt 732, Supp No. 3.

### Knowledge of Ultimate Destination

The exporter is responsible for knowing the ultimate destination of its export. This means the exporter must be aware not only of where its software or technology will be exported, but also where it will be reexported, if applicable. The Export Administration Regulations (15 CFR pts 730–774) define a "reexport" as an actual shipment or transmission of items subject to the EAR from one foreign country to another foreign country. A reexport also occurs when technology or source code subject to the EAR is released to a foreign national outside the United States. 15 CFR §734.2(b)(4)–(5). Export or reexport further includes transshipments or transmissions through a country. 15 CFR §734.2(b)(6). Under the EAR, any such exports or reexports are deemed to be exports to the final destination country. 15 CFR §734.2(b)(6).

### Prohibited End Users

Regardless of the ultimate destination, the exporter must know exactly to whom it is exporting, because U.S. export controls also prohibit or require licenses for exports to certain "listed" individuals and organizations. The exporter should refrain from hiring, working with, or engaging in any transactions with any individuals or organizations on the following lists:

- Specially Designated Nationals and Blocked Persons List, maintained by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), consisting of individuals and organizations deemed to represent restricted countries or known to be involved in terrorism and narcotics trafficking. 31 CFR Ch V, App A. This list is available at http://www.treas.gov/offices/enforcement/ofac/sdn/index.html.
- Denied Persons List, maintained by the BIS, consisting of individuals who have had their export privileges suspended for either violating export controls or posing a risk of violation. This list is available at http://www.bis.doc.gov/DPL/thedeniallist.asp.
- Entity List, also maintained by the BIS, primarily composed of military, government, and scientific research organizations determined by the BIS to be involved in or posing a risk of developing weapons of mass destruction. Exports to these entities generally may not be made without a license. 15 CFR pt 744, Supp No. 4. This list is available at http://w3.access.gpo.gov/bis/ear/pdf/744spir.pdf.
- Unverified List, also maintained by the BIS, consisting of organizations that in the past were parties to a transaction with respect to which the BIS could not conduct a pre-license check (PLC) or a post-shipment verification (PSV), which raises a "red flag." This list is availableat http://www.bis.doc.gov/Enforcement/UnverifiedList/unverified_parties.html.

- List of Debarred Parties, maintained by the Department of State Directorate of Defense Trade Controls (DDTC), consisting of individuals and organizations that have been convicted of violating the Arms Export Control Act. See 22 CFR §§127.7, 120.27. This list is available at http://www.pmdtc.org/debar059.htm.

### Prohibited End Uses

The exporter must also be aware of what the export will be used for. The Export Administration Regulations (15 CFR pts 730–774) prohibit exports without a license of all items intended for certain end uses. 15 CFR §§736.2(b)(5), 744.1. Such end uses include nuclear and missile-related end uses, and the design, development, production, stockpiling, or use of chemical or biological weapons. See 15 CFR §§744.2(a), 744.3(a), 744.4(a). An exporter should inquire about a potentially prohibited end use if the export is for a military or scientific research application, and should obtain a statement from the customer warranting that the items will not be used for any prohibited purposes. If an exporter believes that its product might be used for any prohibited purpose, the exporter should contact legal counsel.

## Export Transaction Documentation

### Shipper's Export Declaration

In general, exporters must file a Shipper's Export Declaration (SED) form before export. 15 CFR §30.12. The SED is primarily used by the Census Bureau to track export statistics, but is also used by the BIS to check whether transactions are in compliance with export controls. 15 CFR §§30.2(b), 758.1(f). Information to be provided on the SED includes the parties to the transaction; the ECCN; the description, quantity, and value of the items; and the license authority for the export. 15 CFR §§30.7, 758.1(a). The SED form is available at http://www.census.gov/foreign-trade/regulations/forms/7525v.pdf.

Certain export transactions are exempt from the SED filing requirement, including:

- Exports to Canada or to a "U.S. Possession," such as Guam, of items that do not require an export license (15 CFR §§30.58, 30.1(a)(2) fn 1);
- Exports of items that do not require an export license, if the total value of items in the same class that are exported from one exporter to one recipient does not exceed $2500 (15 CFR §§30.55(h), 30.63(a)(3), 758.1(b)(3));
- Exports of software and technology by intangible means (such as e-mail or web download) (15 CFR §30.55(o)); and
- Exports of software and technology that do not require an export license, unless they are mass market. 15 CFR §§30.55(n), 758.1(b)(3).

If an exception applies, the exporter must inform the carrier, declare to the Customs Service that no SED is required, and identify the basis for the exemption. 15 CFR §30.50. For example, for an export of mass market software classified as ECCN 5D992 valued at $2500 or less, the exporter should state "No SED Required, FTSR Section 30.55(h)—NLR."

**If a company is planning to sell software products over the Internet, it should establish a procedure on its website to screen prospective purchasers for ultimate destination, end user, and end use**

### Destination Control Statement

The shipping documentation accompanying all exports subject to the EAR (except those classified as EAR99) must also include the following Destination Control Statement (DCS) (15 CFR §758.6):

**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.**

The DCS must appear on the commercial invoice, and may appear on the export's bill of lading, air waybill, or other export control document that accompanies the shipment. 15 CFR §758.6. For nonphysical exports, such as those made via e-mail or web download, the exporter may display this language on the computer screen for consent before permitting the end user to receive the export.

### Contractual Certifications

United States companies may enter into licensing and distribution agreements for their software with third party vendors and customers. Even if the other party to the contract is located within the United States, such licensing and distribution agreements should include provisions stating that the company provided the software within the United States, and that the vendor or customer agrees to not export or reexport the software in violation of U.S. export control laws.

United States companies may also enter into outsourcing agreements with offshore suppliers, or onshore suppliers employing foreign nationals, for the joint development of software or for the sharing of technology. In such a case, the U.S. company should notify the supplier of U.S. export controls and obtain certifications that it (and any third party supplier it may subcontract with) will comply with U.S. export controls. Such certifications may include statements that the supplier will not

reexport any encryption software to a prohibited country and that it will not release any technology for that software to certain foreign nationals, including its own employees.

### Website Screening System

If a company is planning to sell software products over the Internet, it should establish a procedure on its website to screen prospective purchasers for ultimate destination, end user, and end use (*e.g.,* embargoed countries, "listed" individuals and organizations, and prohibited end-uses). The procedure can require that the purchaser make appropriate certifications before proceeding to the ordering screen, and there should be a mechanism to screen the names, addresses, and affiliations that are entered in the ordering screen.

### Access Control System

For exports of encryption software or technology over the Internet, the exporter should also have in place an access control system that checks the address of every non-U.S. party requesting or receiving the software to verify that it does not have a domain name or Internet address of a foreign government, such as ".gov" or ".mil." See 15 CFR §734.2(b)(9)(iii). In addition, the posted Destination Control Statement (DCS) should state that the transfer includes encryption software that may not be exported without authorization. The exporter should also require the recipient to certify that the software is not intended for use by a government end-user and that the recipient understands that the encryption software or technology may not be reexported without a license or authorization. 15 CFR §734.2(b)(9)(iii)(C).

## Reporting and Recordkeeping

### Encryption Exports Reports

One of the requirements of License Exception ENC (see 15 CFR §742.15(a)(1), discussed above at "Product Classification; Classification Procedures") is that the exporter must file semi-annual reports with the BIS concerning its exports of these encryption items. See 15 CFR §740.17(e)(2).

Reports for each encryption item exported must include the classification ruling number and the ECCN. For items exported through direct sale, the exporter must provide the name and address of the recipient, the item, and the quantity exported. 15 CFR §740.17(e)(2)(ii). For items exported to a distributor or other reseller (including subsidiaries of U.S. firms), the exporter must provide the name and address of the distributor or reseller, the item and quantity exported, and the end-user's name and address, if such information is normally collected as part of the exporter's distribution process. 15 CFR §740.17(e)(2)(i). The BIS requires that the reports be provided in electronic form, such as "spreadsheets, tabular text or structured text." 15 CFR §740.17(e)(5). Reports must be submitted semi-annually. For exports made between January 1 and June 30, the report is due by August 1 of that year; for exports made between July 1 and December 31, the report is due by the following February 1. 15 CFR §740.17(e)(5).

The following items and transactions are excluded from the reporting requirements (15 CFR §740.17(e)(4)):

- Any encryption items exported to U.S. subsidiaries for internal company use;
- Encryption commodities or software with a symmetric key length not exceeding 64 bits;
- "Retail" products exported to individual consumers;
- Encryption items exported via free or anonymous download;
- Encryption items from or to a U.S. bank, financial institution, or their subsidiaries, affiliates, customers, or contractors for banking or financial operations;
- Items that incorporate components limited to providing short-range wireless encryption functions;
- Retail operating systems, or desktop applications (*e.g.,* e-mail, browsers, games, word processing, database, financial applications, or utilities) designed for, bundled with, or pre-loaded on single CPU computers, laptops, or hand-held devices;
- Client Internet appliance and client wireless LAN cards; and
- Foreign products developed by bundling or compiling of source code.

### Records Maintenance

An exporter of software or technology is required to retain for five years detailed records of its transactions, including all export control licenses, applications, documents submitted in support of license applications, memoranda, notes, correspondence, contracts, invitations to bid, books of account, and financial records. The complete list of records required to be retained can be found at 15 CFR §762.2(a).

## Export Control Compliance Program

If a company anticipates that the volume or type of its exports will likely increase over time, it should consider implementing an export control compliance program. An export control compliance program should serve to document the company's policies and procedures for export compliance, including identification of controlled items, recordkeeping, screening of future activities, and hiring of foreign nationals who may require an export license.