Software EXPORT RULES

By Mitchell A. Goodkin and David H. Goodkin

All commercial computer software is controlled to at least some extent under United States export statutes and regulations, even software that does not perform a high-technology or encryption function. Although the legal constraints are greatly reduced for commercially available software, such as a database system that tracks inventory for a restaurant, the export of even very low-technology items has resulted in major fines when not performed in compliance with the export rules—for example, the export of barbed wire to a friendly country purportedly for use in ranching. Computer source code, other than encryption-related, that is made generally available to the public for free or for no more than the cost of distribution generally is not subject to control under the export regulations.

Businesses desiring to sell software to international markets, to collaborate with foreign organizations, or to have foreign national employees, consultants, or visitors, must carefully consider the potential impact of the export rules. In addition, the rules can prevent, or make it very difficult to receive, payments for sales or services associated with international transactions, particularly if the transactions are with individuals, organizations, or countries considered to represent a threat to peace.

The export rules can also significantly impact the conduct of research and teaching by institutes of higher education by putting constraints on who may participate and on who may receive research results and course materials, such as sample computer code. Universities may also desire to transfer technologies to markets, and for these activities have similar concerns as industries.

Several U.S. statutes and regulations govern the export and re-export of technical information, physical items, and computer software. The primary regulations are the Export Administration Regulations (EAR)[1] administered by the Bureau of Industry and Security (BIS) in the Commerce Department, the International Traffic in Arms Regulations (ITAR)[2] administered by the Directorate of Defense Trade Controls in the State Department, and a series of regulations administered by the Office of Foreign Assets Control (OFAC)[3] in the Treasury Department. The EAR contains references to the other regulations and to relevant statutes.

The EAR is of greatest relevance to most people. It covers all types of physical items, computer software, and technical information not exclusively administered under other regulations. The ITAR is focused on items that are specifically for defense or space

applications, and the regulations administered by OFAC relate mainly to embargoed countries, organizations, and individuals.

The dual nature of software—its expressive characteristic and its functional characteristic—has created issues for the export rules just as it has in other areas of law. Generally available printed copies of source code are much less controlled than electronic copies. The main issues regarding the dual nature have related to software that is associated with encryption.[4]

Under the various regulations, government approval is required before certain activities are allowed. The required approval (often called a "license") generally is a function of the type of item involved; the country, organization, or individual to which an item is to be transferred; the expected end use of the item; and whether certain types of services are to be performed. Certain activities are totally excluded from control under each of the regulations, and exceptions from the requirement of a license exist for activities that meet specific criteria. Whether or not approval is required for a particular export, there might be a requirement for a report to the government.

There are potentially severe civil and criminal penalties for violations of the export regulations, including banning the violator from participating in any future export activities. Such a penalty could greatly impact organizations that depend heavily on international sales or that have a significant number of international employees, students, or collaborations.

DEFINITIONS

An export is the transfer out of the U.S. of a physical item, technical information, or computer software. A transfer of technical information to a foreign national in the U.S. is deemed to be an export to that person's country. A deemed export can take place by allowing a foreign national access to physical items or computer software from which controlled technical information might be ascertained.

Particular care may be needed when interacting with foreign visitors, or even foreign employees who are temporarily in the U.S. On the other hand, a transfer of information to a permanent resident of the U.S. or to certain protected persons is treated the same as a transfer to a U.S. citizen and would not be deemed an export.

Under ITAR, a "defense article"[5] means any item or technical data designated on the United States Munitions List (USML).[6] "Technical data" includes all types of technical information[7] and software directly related to defense articles, including, but not limited to, various forms of high-level descriptions of the software design and flow for all aspects of design through manufacture, test, and repair of defense articles. The manner in which technical data is defined indicates that software is treated as a special form of information.

"Defense services" under ITAR include furnishing assistance associated with USML articles to foreign nationals, transferring controlled technical data, or providing military training.[8]

EXPORT ADMINISTRATION REGULATIONS (EAR)

At the heart of the EAR are 10 basic prohibitions and the Commerce Control List (CCL). The prohibitions may only require that BIS approval be obtained for an activity, or there may be an absolute prohibition. For some activities, only notice to the government is required. In addition, certain services are subject to the EAR; for example, activities related to the proliferation of certain weapons or assistance with respect to encryption software.[9]

The CCL contains detailed lists of items arranged in 10 categories. Each category contains a "catch-all" item, called EAR 99, for everything not specifically listed. If only EAR 99 applies, a license will be required only if one of the less likely basic prohibitions applies (for example, the export is intended for an embargoed country). Each category contains five subcategories, including one devoted to software.

The EAR contains detailed directions on how to determine if an activity is subject to, or excluded from, control by the EAR; and, if the EAR does apply to an activity, whether a license is required.[10] In general, the need for a license depends on the CCL items, the reason for control (e.g., national security), the end use, and the recipient country, organization, and individual. For embargoed countries, there are special rules that don't follow the usual directions.

EAR EXCLUSIONS

Activities exclusively controlled by other regulations are not subject to control by the EAR. The same is true for published information. In addition, publicly available technology and software, other than certain encryption software, is excluded from EAR control. Detailed definitions and constraints are given in EAR part 734, which should be carefully reviewed before assessing the applicability of the exclusions.

Generally, for software to be considered publicly available, the source code must be available for free or for no more than the cost

FAST FACTS:

All commercial computer software is controlled to some extent under U.S. export statutes and regulations.

Giving technical information to a foreign national, even within the U.S., can potentially violate export regulations.

of distribution. If the source code is publicly available, then code compiled from it can also be considered publicly available.

Of particular importance to the academic community are the exclusions for publicly available technology and software that arise during, or result from, fundamental research (a defined term in the regulations), and technology and software that are released by instruction in catalog courses and associated teaching laboratories of academic institutions.

The exclusions are also of particular importance for people who desire to share software, such as under various open-source activities.

EAR EXCEPTIONS

In many cases, when a license might otherwise be required under the EAR, an exception might exist. Part 740 describes 16 potential exceptions. Each exception has constraints on its applicability, including the countries to which it applies. Depending on the software and the circumstances, almost all of the potential exceptions might apply to software exports.

Among the broader potential exceptions for software are those for shipments of limited value (LVS); civil end-users (CIV); technology and software under restriction (TSR); key management infrastructure (KMI); temporary imports, exports, and re-exports (TMP); technology and software—unrestricted (TSU); baggage (BAG); and encryption commodities and software (ENC).

License exception TSU is available for "mass-market" software to all destinations, except for countries that are identified as supporting terrorists. For TSU to apply, the software must be (a) sold from stock at retail selling points without restriction by means of over the counter, mail order, electronic, or telephone call transactions; and (b) designed for installation by the user without further substantial support by the supplier.

SPECIAL EAR RULES FOR ENCRYPTION SOFTWARE

The export of encryption equipment, technology, and software has many special and complex rules under the EAR, and the scope of what are considered encryption items is fairly broad. Included are commodities and software that allow the end-user to activate or enable cryptographic functionality that would otherwise remain disabled.[11]

An important exclusion from control under the EAR is for printed material setting forth encryption source code, though such code in electronic form remains subject to the EAR, even when there is an intention to make it freely available to the public.[12] The reason is explained at § 742.15: "As the president indicated in Executive Order 13026…of November 15, 1996, exports and re-exports of encryption software…are controlled because of [the] functional capacity…and not because of any informational or theoretical value that such software may reflect…."

There are greater controls for stronger encryption, for encryption used for longer distance transfers of information, and when users have the ability to select or control the strength of the encryption. The controls tend to be less for user authentication and for such local uses of security as the protection of stored data files and short distance wireless transmissions.

Mass-market encryption software has additional constraints not required for other software. Also, there are special requirements for review by, notice to, and reporting to the government. Some examples of mass-market encryption software include operating systems, e-mail browsers, games, and word processing software.[13]

INTERNATIONAL TRAFFIC IN ARMS REGULATIONS (ITAR)

Activities are controlled under ITAR only if they involve defense articles (i.e., physical items, technical information, and computer software) specifically on the USML. The USML has 22 categories. Each category has a subcategory for technical data, including software, and defense services directly related to the defense articles in the category. Some software is specifically listed on the USML (e.g., military security software in category XIII(b)). Category XXI covers any article not specifically listed in the other categories that has substantial military applicability and that has been specifically designed or modified for military purposes. Category XV covers spacecraft systems and associated equipment, even though not specifically for defense.

ITAR EXCLUSIONS

The definition of technical data at § 120.10 excludes information in the public domain (i.e., publicly available) as defined at § 120.11. Thus, publicly available information is excluded from control under ITAR. Included in this exclusion is information made publicly available through fundamental research in science and engineering at accredited institutions of higher learning in the U.S., where the resulting information is ordinarily published and shared broadly in the scientific community. Fundamental research includes both basic and applied research. Also excluded

The export rules can prevent, or make it very difficult to receive, payments for sales or services associated with international transactions, particularly if the transactions are with individuals, organizations, or countries considered to represent a threat to peace.

are commonly taught technical principles. Given that software apparently is treated as a form of information in the definition of technical data, public domain software apparently also would be excluded from that definition. It should be noted that defense services might be controlled even though all of the information used is publicly available.

ITAR EXEMPTIONS

The available ITAR exemptions from the requirements for government approval are considerably fewer and narrower in scope than under the EAR. One of the most significant areas with exemptions is for collaborations involving space programs. Even when exemptions apply, various reports to the government might be required before, during, or after an export takes place.

OFFICE OF FOREIGN ASSETS CONTROL (OFAC)

The OFAC regulations control transactions and services with regard to various countries and the nationals of those countries, especially Cuba, Iran, North Korea, Sudan, and Syria. The regulations also have controls for terrorist support, narcotics trafficking, proliferation of weapons of mass destruction, and trading of raw diamonds. There are extensive and complex rules under the OFAC regulations controlling financial transactions.

The primary relevant broad statutes behind the OFAC regulations are the Trading with the Enemy Act (TWEA), International Emergency Economic Powers Act (IEEPA), and Antiterrorism and Effective Death Penalty Act. There are also acts specific to various countries or controlled activities. Other than when there are common statutes being implemented, the various OFAC regulations are completely independent of each other.

Information and information materials are excluded from control under TWEA and IEEPA, and thus from those regulations that implement these statutes. Although not specifically addressed in the statutes and regulations, some activities involving software might have the benefit of that exclusion. The dual nature of software might be a factor. In general, special care is needed with any activity involving embargoed countries, organizations, or individuals.

Although a software activity might be allowed under the OFAC regulations, with or without government approval, the controls on financial transactions might result in difficult and costly complications for payments.

PENALTIES FOR VIOLATIONS OF THE REGULATIONS

Penalties under the EAR can be both civil and criminal. A willful violation can result in criminal penalties of a fine of up to the greater of $1,000,000 or five times the value of the exports for each violation for a corporation, or a fine of up to $250,000 or imprisonment for up to 10 years, or both, for an individual. Knowing violations can result in a fine of up to the greater of $50,000 or five times the value of the exports for each violation for a corporation, or a fine of up to the greater of $50,000 or five times the value of the exports or imprisonment for up to five years, or both, for an individual.

Civil and administrative penalties for violating the EAR can include the imposition of a fine of up to $11,000 for each violation, up to $120,000 per violation for violations involving items controlled for national security reasons, exclusion from practice, and even the denial of export privileges, a penalty that could have severe implications for an international company.

Willful violations under ITAR can result in criminal penalties of up to $1,000,000, 10 years in prison, or both, per violation. Civil and administrative penalties are up to $10,000 per violation, or up to $100,000 per violation involving national security or defense articles or services.

It is also important to note that, as is often the case with government enforcement and prosecutions, authorities will attempt to find as many possible technical violations out of even a single incident, potentially leading to multiple penalties. ■

The opinions expressed in this article are solely those of the authors and do not necessarily represent those of their employers.

Mitch Goodkin is an assistant general counsel in the Office of the General Counsel at the University of Michigan, where his primary focus is export issues. An attorney since 1983, Mitch is also a professional engineer. At U-M and in private practice, he has extensively addressed technology and business legal issues. He is a past chair of the State Bar Computer Law Section.

David Goodkin is currently a prehearing attorney for the Michigan Court of Appeals. Before his admission to the Bar in May 2006, he was a professional computer programmer for seven years, the last three of which were concurrent with law school.

FOOTNOTES

1. 15 CFR, ch 7, subch C, parts 730 to 774.
2. 22 CFR parts 120 to 130.
3. 31 CFR parts 500 to 598.
4. See, e.g., *Bernstein v US Department of Justice, et al.*, 176 F3d 1132 (1999) (subsequently withdrawn with an order that the case be reheard by the en bank court, which apparently did not take place. 192 F3d 1308 (1999)); and *Junger v Daley*, 209 F3d 481 (2000).
5. ITAR § 120.6.
6. ITAR § 121.1.
7. ITAR § 120.10.
8. ITAR § 120.9.
9. See EAR § 734.5.
10. See EAR part 732 and supps 1 and 2.
11. See EAR § 742.15(b)(4).
12. See note to ¶¶ (b)(2) and (b)(3) of EAR § 734.3(b) and also § 742.15(b)(5).
13. See EAR § 742.15(b)(5).