Many U.S. companies distribute software and other technology products globally, whether by physical shipment or electronic transfer. With the rapid development of the technology sectors in many low-cost countries, more and more U.S. companies also outsource their software development abroad. However, what many companies fail to recognize is that in doing so, or by hiring foreign nationals who are not U.S. citizens or permanent resident aliens, they may be exporting technology and software that is subject to U.S. export controls and related licensing and other regulatory requirements that carry significant potential penalties for noncompliance.

This article addresses the following questions relating to software export activity:
- What constitutes an export of software/technology?
- How is the applicable level of control determined?
- What restrictions apply to exports of U.S. encryption items?
- How may companies export high-functionality encryption items without an export license?
- How do companies ensure compliance with U.S. export control laws?
Software that is subject to U.S. export controls can be of various types, including operating, process and encryption software. Cryptography is treated as a critical technology and is closely regulated by the U.S. Government because of national security concerns and the need for secure government communications and intelligence gathering.

While the U.S. Government has, in recent years, taken a number of steps to reduce dramatically the number of situations in which export licenses are required for such exports, as part of that process, it has imposed sometimes confusing requirements on exporters to allow them to take advantage of the license exceptions.

Failures to comply with export control requirements, whether for encryption software/technology or for other types of software/technology, are subject to significant penalties. Criminal violations are punishable by a $1 million fine, 20 years in jail, or both, per violation. Civil penalties are punishable by fines of up to almost $300,000, or twice the value of the transaction, whichever is greater, per violation. In addition, violations can result in the U.S. Government denying the violator export privileges for varying periods of time. For U.S. companies, this means that they can be prohibited from exporting. For foreign companies, this means that they can be prohibited from receiving U.S. goods, software and technology.

Here are some examples of penalty cases involving unauthorized exports of software/technology:

- Wind River Systems, Inc., an Intel subsidiary, settled allegations of improper exports of encryption software for $750,000 in October 2014.
- In February 2014, a California company, Intevac, Inc., settled, for $115,000, allegations of unauthorized disclosures of controlled technology to, inter alia, a Russian-national engineer who had been hired by the company and was provided access to the controlled technology, without a required license.
- In April 2013, the UAE-based company, Computerlinks FZCO, settled Commerce Department allegations of re-exporting controlled network devices and software to Syria, without a license, for $2.8 million.

**What constitutes an export of software/technology?**

While most companies understand that a cross-border shipment of computers or hard drives constitutes an export, the export control laws also apply to exports of encryption and other software/technology items that may not be recognized by companies not experienced in dealing with export controls.

An export of encryption software (or other software/technology) occurs when the software is actually shipped, transferred or transmitted (physically or electronically) out of the United States. Encryption software is also exported when it is transferred in the United States to a foreign country embassy or affiliate of a foreign country. In addition, releases/disclosures of U.S. encryption technology to a foreign national in the United States or overseas, and releases/disclosures of U.S. encryption source code and technology in a foreign country to a foreign national, are also governed by U.S. export control laws. These are known as “deemed exports” and “deemed re-exports,” respectively. As in the case of the Russian national engineer referenced above, deemed (re)exports also include releases/disclosures of non-encryption-related software/technology to foreign nationals.

Furthermore, for some encryption software, exporting also includes the downloading or causing the downloading of the software to locations outside the United States or making such software available for transfer outside the United States over communications facilities accessible to persons outside the United States, unless the person making the software available takes precautions adequate to prevent unauthorized transfer of the code (e.g., transfers to restricted persons or embargoed countries).

Under a new rule, effective September 1, 2016, transmitting or storing nonmilitary electronic data that is (i) unclassified, (ii) secured using “end-to-end encryption” that meets certain encryption standards and (iii) not intentionally stored in a U.S. military-embargoed country or in the Russian Federation, will not constitute an export of that data. That means that such exports of technology/software to the “cloud” will not be controlled for export, provided they meet the required criteria. Transmissions within a cloud service infrastructure also fit within this safe harbor provision when the transmission is made from one node or cloud infrastructure element to another, provided that it was appropriately encrypted before any data crossed a national border.

U.S. export controls apply not only to U.S.-origin products/software/technology, but also to foreign-origin items that enter the United States before being exported again, and foreign-origin items that contain more than a *de minimis* amount (generally 25 percent) of controlled U.S. content.
How is the applicable level of control determined?

The level of control applicable to a nonmilitary export is based on how the item is classified for export purposes, the reason for control (whether national security, non-proliferation, regional stability or other) and the country of destination. The controls for software/technology exports generally mirror the level of control applicable to the equipment they are designed to develop, produce or operate. So, if a milling machine would require a license for export to China, the software to run such a machine, and the technology to develop/produce it, also may be subject to the same licensing requirements.

Encryption software, however, is generally controlled based on the level and type of encryption involved and will generally be controlled under unique encryption export rules, even if it is incorporated into another item. For export control purposes, software is defined as “a collection of one or more programs or microprograms fixed in any tangible medium of expression.” Encryption software includes that which performs cryptography, cryptographic activation, cryptanalysis and computer security functions.

What restrictions apply to exports of U.S. encryption items?

The Commerce Department’s controls on exports of encryption items under the Export Administration Regulations (EAR) are divided into two basic categories, with extremely distinct ramifications. Nonmilitary items with high-encryption functionality are generally classified under a 5X002 export classification. Unless these items qualify for a License Exception, as discussed below, they will require an export license from the Department of Commerce for export to any destination except Canada. Similar license requirements will apply to exports of military encryption items under the State Department’s International Traffic in Arms Regulations (ITAR).

Nonmilitary encryption items with lower encryption functionality are controlled less stringently and will generally be classified under a 5X992 classification. These items only require an export license if they are destined for one of the terrorism-supporting/embargoed countries/regions (defined as Cuba, Iran, North Korea, Sudan, Syria and the Crimea region of Ukraine) unless they qualify for a license exception/exemption.

In addition to software with low encryption functionality, items classifiable under 5X992 include digital techniques used to perform digital signatures or authentication and items specially designed and limited for banking use or money transactions.

Some “mass market” encryption items can also be classified under 5X992 if they are available to the public at retail selling points and meet certain other requirements. In some cases, this will require the producer or exporter to file an encryption registration and/or export reports with the Bureau of Industry and Security (BIS) at the Department of Commerce.

How may companies export 5X002 encryption items without an export license?

For high-encryption functionality items classifiable under 5X002, License Exception ENC may authorize export, without a license, to any country, except the terrorism-supporting or embargoed countries/regions, if the item is being exported either (i) to a subsidiary of a U.S. company, including to foreign nationals who are employees, contractors or interns of a U.S. company or its subsidiaries, for internal company use; or (ii) to private sector end users, headquartered in what is defined as a Favorable Treatment Country (NATO and certain other closely allied countries) for internal development or production of new products.

If an export of an encryption item does not fall under either of these circumstances, it still may be eligible for export under the License Exception, either as “ENC-Unrestricted” or “ENC-Restricted.” Items eligible for export under ENC-Unrestricted may be exported, without a license, to any country, except the terrorism-supporting or embargoed countries/regions.

However, in order to qualify for the exception, the exporter will have to register with the Commerce Department and, in certain cases, may need to submit a formal export classification request. Annual reports of exports may also be required. Chips, chipsets, cryptographic tool kits and some items that provide vulnerability analysis are among the items that may be eligible for License Exception ENC-Unrestricted.

In general, items eligible for License Exception ENC-Restricted may only be exported, without a license, to nongovernmental end users, or to any user in a Favorable Treatment Country, after registration, export classification and reporting requirements have been met. Export licenses will be required for exports of items eligible under License Exception ENC-Restricted to governmental end users outside the Favorable Treatment Countries. As with ENC-Unrestricted items, ENC-Restricted items cannot be exported, without a license, to the terrorism-supporting or embargoed countries/regions. Encryption items that are designed or customized for a governmental end user, cryptanalytic items and open cryptographic interface items are among the items that may be eligible for export under License Exception ENC-Restricted, provided its conditions are met.
Can controlled publicly available encryption software be exported without a license?

In certain cases, yes. Encryption source code that is classified under 5X002, even if it is publicly available, is still subject to the EAR. However, another License Exception, TSU, authorizes export without a license of encryption source code that is not incorporated into proprietary software, after a notification is submitted by email to BIS and the National Security Agency. That notification must either state where the source code is posted on the internet or include a copy of the source code that is posted. Updates or modifications of the source code and changes in internet location must be similarly provided to BIS and the National Security Agency. Publicly available encryption software in object code that corresponds to encryption source code made eligible for export under License Exception TSU is not subject to the EAR.

How do companies ensure compliance with U.S. export control laws?

Companies involved in exporting software, particularly encryption software, should have an export control compliance system and procedures in place to make sure they do not commit violations. That system and these procedures should begin with determining their software’s appropriate export classification(s). Once that determination is made, companies can assess the nature and extent of applicable licensing, registration, reporting or other requirements and implement procedures to ensure they are met. Because software products regularly undergo updates that alter encryption functionality, and because encryption controls are likely to evolve further, companies should regularly re-evaluate the appropriate classifications for their software, the attendant requirements for export and their export compliance procedures.

Contact

Melvin S. Schwechter
T 202.961.1559
mschwechter@bakerlaw.com