Expert Analysis

Software Development and U.S. Export Controls

By D.E. Wilson Jr., Esq., and Andrew Bigart, Esq.
Venable LLP

Earlier this year, the Wall Street Journal noted a growing trend among U.S. companies to develop software overseas and use cloud computing to deliver the product to customers in the U.S. and throughout the world.[1] According to the article, the reason for offshoring the design and production of software is that it may allow companies to keep their profits "outside the reach of U.S. taxes." Left unmentioned, however, is the extent to which software development collaborations between U.S. and offshore sites may implicate U.S. export laws.

These laws apply broadly to U.S. persons, wherever located, as well as to goods that contain a certain amount of U.S. content or were made using certain U.S.-origin technology. Physical transfers; cloud computing; or even providing a foreign national with access to technical data, source code or other information may require an export license from U.S. authorities, depending on the product and countries involved. Thus, the very tools that allow teams of developers in different countries to collaborate on designing software can create challenges for export compliance.

BOOTING UP: AN OVERVIEW OF U.S. EXPORT CONTROLS AND ECONOMIC SANCTIONS

The U.S. government regulates the export of goods, technology and services through a maze of regulatory acronyms. The State Department's Directorate of Defense Trade Controls (DDTC) regulates the export of defense articles, related technical data and defense services listed on the U.S. Munitions List (USML) through the International Traffic in Arms Regulations (ITAR). The Department of Commerce's Bureau of Industry and Security (BIS) enforces the Export Administration Regulations (EAR), which govern the export and re-export of commercial and "dual use" commodities (generally those items not listed on the USML).

Because most commercial software is subject to the EAR, this article focuses on the BIS' regulatory framework. It bears noting, however, that some software developed or designed primarily for defense purposes may fall under ITAR licensing requirements administered by DDTC. In addition, all export transactions should be reviewed for compliance with the U.S. economic sanctions programs administered by the U.S.

Department of Treasury's Office of Foreign Assets Control. (These sanctions apply against Iran, Syria, international terrorists and terrorist organizations, and narco-traffickers, among others.)

What is an export?

Most U.S. companies understand that the export or re-export of a finished product implicates export laws. Less often appreciated is that U.S. export controls also cover the transmission of software source and object code overseas, and the sharing of technology or source code with foreign persons, including foreign entities, whether located in the U.S. or abroad. Once controlled technology or source code is shared or released to a foreign national (wherever located, even in the U.S. or over the phone), the rules consider this a "deemed export."[2] This means that technology, software, or source and object code can be exported through visual inspection, release on a website, e-mail transmission or oral exchange of information.

Software development collaborations between U.S. and offshore sites may implicate U.S. export laws.

Beware deemed exports!

The potential for "deemed exports" is real for many U.S. software companies, especially those that take advantage of lower costs and taxes, etc., outside the U.S. This may include, for example, using operations offshore for software coding and development; back office support services, including application support and maintenance; or the managing of a data room overseas. All these activities raise the possibility of a deemed export. Depending on the nature of the technology and the country of citizenship and residence to which the technology is disclosed, releasing controlled technology to a foreign person (wherever located) may require an export license.

When is software subject to licensing requirements?

Just because an item is subject to the EAR does not necessarily mean that an export license is required. All items subject to the EAR are categorized within an export control classification number, or ECCN. This number determines the item's licensing requirements on a country-by-country basis, or as EAR99, meaning the item may be exported to most countries without a license. Factors that determine whether a BIS export license is required include the classification of the commodity, software and/or technology, the country of ultimate destination, the identity of the ultimate end-user of the item, and the intended end-use.

For software and related source code, etc., determining whether a particular transaction requires an export license can be complicated[3]:

- Several ECCN categories cover both the finished product (such as semiconductors) as well as any software specially designed for the development, production or use of the finished product (such as CAD software used to design nuclear reactors). The export of such specialized software can require a license to certain destinations or end -users.

- Software — regardless of focus — that contains a certain level of encryption functionality or features may be subject to certain BIS prior review and reporting requirements. These ECCNs frequently cover software designed for cybersecurity, defense and other sensitive industries.[4]

- Certain very basic commercial software that does not qualify as "publicly available" may be classified as EAR99 (when, for instance, the encryption is less than 64-bit key level for a symmetric algorithm), meaning no license is required to export to most countries and end-users. Think software used to play your online music collection.

As noted, software containing enhanced encryption receives special attention. In fact, until recently, most software containing encryption required a license from BIS for export to many country destinations. In 2010, BIS adopted new rules allowing most software to be exported without a license under MMKT (Mass Market) or License Exception ENC (Encryption).[5]

Under License Exception ENC, for example, certain encryption software may be exported without review or reporting if exported to private sector companies for use in the development or production of other end products, or if used by the exporter's U.S. subsidiaries wherever located for internal development use. Other software, however, involving network infrastructure, cryptanalytics and certain wireless functionality, may require the exporter to register with BIS by obtaining an encryption registration number, then submit a classification request prior to export.

KEEPING SYSTEMS RUNNING: BEST PRACTICES FOR SOFTWARE COMPANIES

Any software company that has exported overseas, or is considering moving parts of its operation overseas,

should take into account the potential impact of U.S. export controls. For some companies, the nature of their software may raise few, if any, export concerns, especially if the export qualifies for MMKT treatment or License Exception ENC. For others, developing software overseas, including sharing source code and other sensitive information, may present complex licensing requirements. The best way for a company to get a handle on these issues is to conduct a comprehensive review of operations and to implement appropriate compliance policies and procedures.[6]

Develop an export compliance policy and procedures

Designing and implementing an effective program is not a one-size-fits-all endeavor. Companies should design their programs taking into account their size, operating structure and business risks. At a minimum, however, an export policy should set forth a company's commitment to export compliance and associated procedures and provide guidance to employees. The policy should include an overview of applicable laws and a summary of the company's products and services and related export controls, prohibited activities, employee responsibilities and implementation of BIS-mandated recordkeeping requirements for a period of five years from the date of the export/re-export.

It bears emphasizing that an export compliance policy is effective only if understood and followed by employees and officers. Training should be done on a regular cycle to ensure employees receive updates on developments in the area and learn from each other's experiences over the course of time, and to ensure all new employees are brought into the system on a reasonably timely basis.

The very tools that allow teams of developers in different countries to collaborate on designing software can create challenges for export compliance.

A compliance program should also include an audit function by the company's independent auditor. Reviewing the program as part of an annual cycle shows employees the importance of the program and underlines the seriousness senior management attaches to sound business practices in this area. If a potential violation arises, the company should immediately stop the conduct in question and mitigate risks, including reporting the potential violation to the company's compliance officer or legal counsel.

Conduct due diligence on each transaction and all parties involved

Another standard practice is to require the people involved in every transaction that crosses a border to complete an export control checklist.[7] Consider developing a database that matches your company's products and services to potential export licensing requirements. Employees can use this database to check each export transaction for licensing requirements. In addition, companies susceptible to potential deemed exports should develop a list of all non-U.S. employees engaged in the company's activities, wherever located.

Additional due diligence practices include:

- Require information on intermediate destination(s) and final destination for any applicable restrictions or sanctions.

- Examine end use for each transaction.

- Identify and screen every supplier, service provider, counterparty, customer, etc., against the U.S. government's Consolidated Screening List.[8] This list consolidates a number of "prohibited" party lists maintained by the U.S. government, including by BIS, OFAC and the State Department.

Beware of red flags

Finally, conducting due diligence on each transaction is of limited value if the information obtained is not reviewed for export risk. The following is a list of example red-flags that must be considered when handling an export transaction:

- The customer or purchasing agent is reluctant to offer information about the end use (or end-user) of a product.

- The customer has little or no business background.

- The customer is willing to pay cash for a very expensive item when the terms of the sale call for financing.

- A freight forwarding firm or foreign trade zone is listed as the product's final destination.

- The shipping route is abnormal for the product and destination.

- When questioned, the buyer is evasive or unclear about whether the purchased product is for domestic use, export or re-export.

- The customer uses only a P.O. box address or has facilities that appear inappropriate for the items ordered.

- The customer is known to have, or is suspected of having, unauthorized dealings with embargoed countries.

Once controlled technology or source code is shared or released to a foreign national (wherever located, even in the U.S. or over the phone), the rules consider this a "deemed export."

CONCLUSION

U.S. software companies looking to save money or taxes by offshoring their business operations would be wise to review their planned (or current) operations to ensure they comply with applicable U.S. export controls.

NOTES

[1] Steven D. Jones, *Software Firms Find Tax Advantages,* WALL ST. J. (Jan. 28, 2013), http://online.wsj.com/article/SB10001424127887324329204578270142806806574.html.

[2] An item is subject to the EAR, for example, if it was produced or originated in the U.S; is a foreign-made product that contains more than a specified percentage of U.S.-controlled content; or is a foreign-made product based on certain U.S.-origin technology or software and is intended for shipment to specified destinations.

[3] The EAR does not cover the export of certain types of publicly available software or technology that are related to fundamental research, are educational or are included in patent applications (under certain conditions).

[4] *E.g.,* ECCV 5A002, 5D002, or 5D992.

[5] Exports eligible for License Exception ENC have certain semiannual reporting requirements for most destinations, as described in Section 740.17(e) of the EAR. For exports eligible for License Exception MMKT, BIS created a registration and annual self-classification reporting procedure.

[6] Failure to comply with BIS' export requirements can result in fines of up to $250,000 per violation or twice the transaction amount for civil violations, $1 million for companies and individuals for criminal violations, and/or up to 20 years in prison for individuals.

[7] "Transaction," in this context, means any cross-border activity, not just the purchase or sale of software. Each type of cross-border movement of software should be reviewed for compliance with regulatory requirements.

[8] The consolidated export screening list is *available at* http://export.gov/ecr/eg_main_023148.asp.

D.E. Wilson (L) is a partner in the Washington office of **Venable LLP** and a former U.S. Treasury official. He can be reached at dwilson@venable.com. **Andrew Bigart** (R) is an associate in Venable's Washington office specializing in international trade and related regulatory areas. He can be reached at abigart@venable.com.