Export Controls for Tech Companies: The Basics and the Pitfalls of U.S. Encryption Controls

By John R. Shane and Lori E. Scheetz, Wiley Rein LLP

Many technology companies do not realize the far-reaching impact that encryption controls in the U.S. Export Administration Regulations (EAR) can have, particularly if the company’s exit strategy is acquisition. Oftentimes, failure to understand how and when such controls apply can negatively affect valuation and result in burdensome escrow or indemnification requirements, not to mention potential penalties. While the web of obligations and restrictions created by these regulations can at first appear overwhelming, the EAR’s encryption-related controls actually are fairly straightforward and have been relaxed significantly in recent years, thanks largely to efforts to reform such controls to enhance national security by fostering the continued global competitiveness of U.S. encryption products. Nonetheless, the EAR can still present challenges and potential pitfalls for companies engaged in exporting or reexporting software and hardware with encryption functionality. In this primer, we provide a summary of the EAR’s export controls and answer questions about how these controls apply.

Continued on page 8

John R. Shane is a partner at Wiley Rein LLP in Washington, DC. Lori E. Scheetz is an associate at Wiley Rein LLP in Washington, DC. Wiley Rein LLP’s Export Controls group features professionals well-versed in the EAR’s encryption controls. To get started with a question about exporting an encryption product or for further information, please contact Mr. Shane at (202) 719-7222 or jshane@wileyrein.com or Ms. Scheetz at (202) 719-7419 or lscheetz@wileyrein.com. The authors would like to thank Alexandra Landis for her contributions to this primer.
encryption provisions, a sampling of issues commonly faced by U.S. companies, and a brief discussion of the potential consequences of violating U.S. encryption controls.

OVERVIEW OF U.S. ENCRYPTION REGULATIONS

The EAR, which is administered by the U.S. Department of Commerce's Bureau of Industry and Security (BIS), controls the export and reexport (i.e., the shipment, transmission, or release of a U.S. item from one foreign country to another foreign country) of commercial and dual-use commodities, software, and technology. Software and hardware with encryption functionality (along with encryption technology) are subject to special rules under the EAR, and, as a result, can be subject to registration, classification, and reporting requirements.1

Subject to certain exceptions, most software (including source code) with encryption functionality generally will fall under one of two Export Control Classification Numbers (ECCNs):2 5D992 or 5D002. Similarly, hardware with encryption functionality generally will fall under ECCN 5A992 or 5A002.3

PRODUCTS USING ONLY WEAK ENCRYPTION OR ENCRYPTION FOR CERTAIN LIMITED PURPOSES

Software and hardware classified as ECCN 5D992/5A992 include, for example, products that use only weak encryption (i.e., using key length ≤ 56 symmetric/512 asymmetric/112 elliptic curve), and products that use encryption for other certain limited purposes, such as password protection and authentication. These items are subject to a low level of control and typically can be exported without a license (No License Required or NLR) to most destinations except “E:1 countries,” which currently include Cuba, Iran, North Korea, Sudan, and Syria. Exporters of these types of products are not subject to registration or reporting requirements.

MASS MARKET PRODUCTS

Many software and hardware products with encryption functionality qualify as “mass market” items under the EAR. Such items generally are made available to the public by nature of being sold from stock at retail selling points; their price and product information must be available before purchase without requiring the purchaser to consult the supplier. These items can be installed by the user without substantial support by the supplier. Furthermore, the cryptographic functionality of these items cannot be easily changed by the user. Generally, mass market products are those that are of potential interest to a wide range of individuals and businesses (as opposed to software that is only sold business to business). Most mass market items, including some products that contain strong encryption, can be self-classified as ECCN 5D992/5A992 and can be exported to destinations other than “E:1 countries” without a license under the designation NLR.4 However, in order to self-classify and export mass market products, the manufacturer/exporter must first register with BIS. The company also must submit to the U.S. government an annual report of all mass market products that it has self-classified and exported or reexported during the calendar year.

PRODUCTS USING STRONG ENCRYPTION FOR PROTECTION OF DATA AND/OR SECURING COMMUNICATIONS OR WEB TRAFFIC

Software and hardware classified as ECCN 5D002/5A002 include products that use strong encryption for purposes such as protecting data and/or securing communications or Web traffic. These products are subject to a higher level of control, but typically may be self-classified by the manufacturer/exporter and exported to most destinations without a license (except “E:1 countries”) using License Exception ENC. A license exception allows a company to export a product without applying for a license from the U.S. government. Importantly, and like the requirements for most mass market products, this license exception (and the ability to self-classify these products) generally is available only after the company registers with BIS as a manufacturer/exporter of encryption products.
Registered companies also must submit an annual report listing all self-classified products exported or reexported during the calendar year.5 Importantly, certain products that fall within ECCN 5D002/5A002 and have more advanced capabilities, including certain network infrastructure products, are eligible for use of License Exception ENC-Restricted only after submission of a formal commodity classification request to BIS.6 Network infrastructure products, for example, are eligible for export to those close allies of the United States listed in Supplement No. 3 to Part 740 of the EAR (License Exception ENC Favorable Treatment Countries) immediately after submission of the classification request. Thirty days after submission of the request, the company can export such products to non-government end users located or headquartered in a non-Supplement No. 3 country. However, exports to government end users in non-Supplement No. 3 countries require a BIS-approved individual export license or an Encryption Licensing Arrangement. Companies must submit detailed semi-annual reports on exports to all destinations other than Canada and reexports from Canada under License Exception ENC-Restricted.

**PRACTICAL ISSUES FACED BY U.S. COMPANIES**

There are several practical issues that U.S. companies face when navigating the EAR's encryption controls. For example, what, precisely, comprises an “export” transaction? Moreover, what products trigger U.S. encryption controls? The answers to these questions cover an unexpectedly wide range of activities and products. The ability to recognize and address the common pitfalls described below can help a company better protect itself from the risk of violations of the EAR when engaging in the export or reexport of its encryption products.

**DOWNLOADING ENCRYPTION SOFTWARE TO A LOCATION OUTSIDE OF THE UNITED STATES CONSTITUTES AN “EXPORT”**

One common area of confusion, particularly for companies that do not ship software overseas, is the range of activities that are considered exports under U.S. law. The EAR controls more than just the physical shipment or transmission of items out of the United States. Downloading or causing the download of encryption software, or otherwise making such software available for transfer outside the United States both qualify as “exporting” the software.11 To this end, many producers make trial versions or other limited versions of software available for download; when such software is downloaded abroad, it is viewed as an export. Even software that is accessed remotely can trigger U.S. export controls issues if the person accessing the software receives any code—whether in source code or object code form—subject to the EAR or any controlled information, such as controlled technology.12
ENCRYPTION FUNCTIONALITY IS DEFINED BROADLY

As is true of the definition of “export,” encryption items are defined broadly. Regulated items can include, for example, the following types of items:

1. Items where the encryption actually is performed by the operating system, an external library, a third-party product, or a cryptographic processor;
2. Items that call, access, or otherwise implement encryption, even if such encryption is not shipped with or incorporated into the product;
3. Items that include but do not use encryption functionality; and
4. Items that direct communications over encrypted channels.

EVEN SOFTWARE PRODUCTS THAT INCORPORATE ONLY OPEN SOURCE AND/OR THIRD-PARTY ENCRYPTION ARE SUBJECT TO BIS’S ENCRYPTION REGULATIONS

Many software products with encryption functionality incorporate only open source and/or third-party encryption software, not proprietary encryption software. Nonetheless, such products are still subject to BIS’s registration, classification, and reporting requirements. This is one of the most misunderstood aspects of BIS’s encryption regulations and, as a result, is a common pitfall for companies.

Indeed, although publicly available encryption source code is eligible for export or reexport under License Exception TSU in the EAR, this exception is not available for an encryption product that simply incorporates publicly available encryption source code if the source code for the entire product itself is not publicly available. Because many software products incorporate or call out to publicly available encryption products, this area of the regulations is one of the prime areas for missteps.

USING FOREIGN CONSULTANTS OR CONTRACTORS CAN REQUIRE AUTHORIZATION FROM BIS

Many U.S. companies engage foreign consultants or contractors to help develop and/or test new encryption products. As noted above, exports of encryption source code or object code to private sector end users headquartered in Supplement No. 3 countries (for development or production of new products), U.S. subsidiaries (for internal company use), and foreign nationals who are employees, contractors, or interns of a U.S. company or its subsidiaries (for internal company use) are authorized by License Exception ENC without the need to register, classify the items, or file reports to BIS. However, other exports to foreign consultants or contractors require either compliance with BIS’s registration, classification,
and reporting requirements or an approved license from BIS.

Notably, while BIS permits exports to “contractors” of U.S. companies and subsidiaries without the need to comply with its usual requirements for encryption products, generally it has taken the position that “contractor,” in this context, means a contract employee (i.e., a human person), not a contracted company. Accordingly, providing encryption items to a contracted company abroad may require an export license, depending on what will be provided to the company and where the company is headquartered. Furthermore, any items produced or developed with encryption software, components, or technology exported pursuant to License Exception ENC are subject to the EAR and may require registration and classification before being sold, reexported, or transferred.

COMPANIES THAT HAVE NOT COMPLIED WITH APPLICABLE REGISTRATION, CLASSIFICATION, AND REPORTING REQUIREMENTS GENERALLY ARE PROHIBITED FROM SERVICING PREVIOUSLY EXPORTED PRODUCTS

General Prohibition 10 and Section 764.2(e) of the EAR prohibit servicing items with knowledge that a violation of the EAR has occurred. Practically speaking, once a company knows that it has not complied with BIS’s encryption regulations, it cannot service or maintain past exports that violated the EAR unless and until BIS provides authorization to do so. Although there is a process whereby companies can request such authorization, this issue can be particularly troublesome for customer relations because services should be put on hold until the BIS authorization is obtained.

REAL-WORLD IMPACT OF VIOLATING U.S. ENCRYPTION REGULATIONS

In 2010, BIS removed or eased encryption-related controls on many items. However, this easing of regulatory controls and requirements has not reduced the importance of compliance with those controls that remain. The consequences for non-compliance can be severe, sometimes including monetary penalties or serious impact on a company’s value in the acquisition context.

Each violation of the EAR, such as an unauthorized export of encryption software, may render a company subject to civil penalties that can range up to the greater of either $250,000 per violation or twice the value of the transaction at issue. Criminal penalties, which generally are imposed only for willful violations, can include up to $1 million per violation in fines and/or imprisonment for up to 20 years. BIS also can deny a company export privileges, which is a significant penalty for any company with international sales operations. While voluntarily disclosing potential violations to BIS and instituting remedial measures tend to result in a substantial mitigation of penalties, BIS nonetheless has broad enforcement discretion. However, companies generally are not subject to the most severe penalties for encryption issues unless they have compromised U.S. national security or intentionally disregarded export controls in a manner that jeopardizes national security or foreign policy interests.

Violations can have other business consequences as well. Export controls compliance typically is a key due diligence issue in the mergers and acquisitions context. Potential violations of U.S. encryption regulations can result in significant added investigative costs, along with costs associated with implementing remedial measures. Some acquiring companies require that the target company indemnify them for any losses resulting from export controls violations, while others require that significant funds be held in escrow until all potential violations are resolved by the U.S. government. Indemnification and escrow requirements can be particularly burdensome for small or start-up software companies. Just as importantly, if a company is being acquired or going public, export controls violations can negatively affect valuation.

CONCLUSION

Many potential stumbling blocks related to U.S. encryption controls—and the resulting consequences of being non-compliant with the EAR—can be avoided through strong compliance policies and procedures and employee training. Adoption of such compliance
measures also demonstrates to the government that the company takes export controls compliance seriously, and that can be an additional substantial mitigating factor in the event of a potential violation.

NOTES

1. Note that hardware or software specially designed for medical end-use, products where the encryption functionality is limited to intellectual property or copyright protection functions, certain publicly available software, and products meeting the requirements of Note 4 of Category 5, Part 2 of the Commerce Control List (CCL) are not controlled as encryption items under Category 5, Part 2 of the CCL.

2. ECCNs are entries on the EAR’s CCL designated by five characters that describe the technical parameters and characteristics of dual-use items controlled for export purposes. An ECCN generally categorizes items based on product type (e.g., electronics, information security, etc.) and general product group (e.g., systems and equipment, software, technology, etc.).

3. Technology required for the development, production, or use of encryption likely is classified as 5E992 or 5E002.

4. 15 C.F.R. § 742.15(b)(1). Note that certain mass market items require submission of a formal commodity classification request to BIS. Id. § 742.15(b)(3).

5. Id. § 740.17(b)(1). Certain short-range wireless encryption commodities or software are exempt from BIS’s registration, classification, and reporting requirements. Id. §§ 740.17(b)(4), 742.15(b)(4).

6. Id. § 740.17(b)(2). Some other encryption products, such as items that contain “non-standard cryptography”; items that perform vulnerability analysis; and network forensic products require registration, submission of a commodity classification request, a 30-day wait period to ship to certain end users, and, in certain cases, the filing of semi-annual reports. Id. § 740.17(b)(3).

7. As noted below, BIS generally has taken the position that “contractor” means a contract employee (i.e., a human person), not a contracted company.

8. 15 C.F.R. § 740.17(a).

9. Id. § 740.13(e).

10. Id. § 740.9(c).

11. Id. §§ 734.2(b)(1) & (9).


17. 15 C.F.R. § 740.17(a).

18. Id. §§ 736.2(b)(10), 764.2(e).