

US Implements Regulation Changes for Encryption Products, Software and Technology

Skadden

09/29/16

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Jeffrey D. Gerrish

Washington, D.C.
202.371.7381
jeffrey.gerrish@skadden.com

Nathaniel B. Bolin

Washington, D.C.
202.371.7893
nathaniel.bolin@skadden.com

Luke A. Meisner

Washington, D.C.
202.371.7751
luke.meisner@skadden.com

Nicholas A. Klein

Washington, D.C.
202.371.7211
nicholas.klein@skadden.com

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

1440 New York Avenue, N.W.
Washington, D.C. 20005
202.371.7000

Four Times Square
New York, NY 10036
212.735.3000

skadden.com

On September 20, 2016, the Bureau of Industry and Security (BIS) of the U.S. Commerce Department amended the Export Administration Regulations (EAR) and the list of goods, software and technology that are controlled under the Commerce Control List. These latest changes were made as part of ongoing Export Control Reform efforts and to implement changes agreed to late last year by the United States and 40 other countries that are members of the multilateral Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.

Among other things, the amendments to the EAR make a number of changes to the rules governing exports, re-exports and transfers of encryption technology, software and information security items as well as many products that contain or use encryption. U.S. and non-U.S. companies that design, produce, sell or distribute goods, software and technology containing encryption should take appropriate steps to update their compliance policies and practices to account for these changes, the more significant of which are summarized below.

Classification of Encryption Items on the Commerce Control List

Encryption items that were previously classified on the Commerce Control List under various subparagraphs of Export Control Classification Number (ECCN) 5A002 now have been divided into three broad categories under separate ECCNs.

The three categories and their corresponding ECCNs are: (i) cryptographic information security items (ECCN 5A002), (ii) noncryptographic information security items (such as communication cable systems designed to detect wiretapping) (ECCN 5A003), and (iii) items that defeat, weaken or bypass information security (ECCN 5A004). Conforming changes were made to existing ECCNs 5D002 (which covers information security software) and 5E002 (which applies to information security technology).

BIS also has revised the portions of the Commerce Control List that apply to less sensitive encryption items by removing several subcategories from ECCNs 5A992 and 5D992 and making conforming changes to ECCN 5E992. As a result, ECCNs 5A992 and 5D992 now designate only encryption commodities or software that qualify as mass market items under the EAR.

Mass Market Encryption Items and License Exception ENC

BIS has made a number of changes to the portions of the EAR that permit the export, re-export and transfer without a license of mass market and certain other encryption goods, software and technology to most jurisdictions, end uses and end users (with the exception of certain embargoed destinations, end uses involving terrorism, and certain governments and other designated end users).

- License Exception ENC authorizes the export, re-export and transfer without a license of certain encryption goods, software and technology to private sector companies headquartered in countries listed in Supplement No. 3 of Part 740 of the EAR. The list of eligible Supplement No. 3 countries has been expanded to include Croatia, a Wassenaar Arrangement member. As a result, Supplement No. 3 now encompasses Cyprus, Iceland and all of the Wassenaar Arrangement member nations except Argentina, Mexico, South Korea, Russia, South Africa and Ukraine.
- The latest amendments expand the types of transactions that are eligible for License Exception ENC to include transactions involving non-U.S. origin encryption items that transit the United States.

US Implements Regulation Changes for Encryption Products, Software and Technology

- Encryption registration is no longer required for use of License Exception ENC. Instead, individuals and companies must submit an expanded “self-classification report” or request a classification from BIS. The list of information that must be provided in these reports and classification requests has been expanded to include some items that were previously provided as part of the encryption registration process.
- Provided that a classification request has been submitted to BIS, “network infrastructure” encryption items described in paragraph 740.17(b)(2) of the EAR may now be exported to most private sector and “less sensitive” government end users located outside of Supplement No. 3 countries (with the exception of embargoed countries and prohibited end uses and end users). The addition of “less sensitive” government end users is new, and the term is defined in Part 772 of the EAR.¹
- While the encryption registration requirement has been eliminated, companies making use of the License Exception ENC self-classification provisions must continue to file annual self-classification reports. Companies that receive a commodity classification (CCATS) determination from BIS that their product is eligible for self-classification treatment do not need to include that product in their self-classification report. As before, an email must be submitted in lieu of the self-classification report if no new products are made eligible for export or re-export under the self-classification provisions of License Exception ENC during a calendar year. Those companies making use of the provisions of Section 740.17(b)(2) of the EAR must continue to file semiannual reports as before.
- BIS has expanded, revised and reorganized a number of explanatory notes and definitions of terms (such as “network infrastructure”) that are used throughout Section 740.17(b)(2)

¹ A companion definition of “more sensitive” government end users also has been added and is referred to in revised statements of BIS’ licensing policy in Section 742.15(a)(2) of the EAR. The “less sensitive” and “more sensitive” government end user categories are based on BIS’ experience developing worldwide encryption licensing arrangements.

of the EAR. As a result, some of the performance parameters used to define eligible items have changed and certain items (such as some satellite infrastructure items that utilize encryption) are no longer subject to the requirements of Section 740.17(b)(2).

Publicly Available Encryption Source Code

BIS has revised and updated the EAR provisions relating to encryption source code that is made publicly available. The new provisions are found in Section 742.15(b) of the EAR and provide that source code that is made publicly available (such as through posting on the internet) is not subject to the EAR once a notice is submitted to BIS and the National Security Agency’s ENC encryption request coordinator.² Distribution or posting of source code that meets the EAR definition of publicly available is eligible for this treatment even if the commercial production or sale of products developed using the source code requires the payment of a licensing fee or royalty.

Effective Date

The amendments to the EAR went into effect on September 20, 2016. No notice and comment period was provided. However, the amendments do provide for a limited grandfathering of the old rules for items that now require a license but were in transit on September 20, 2016, pursuant to actual orders for exports, re-exports or transfers. Such items can be exported, re-exported or transferred before November 21, 2016. Any such items not actually exported, re-exported or transferred before midnight Eastern Time on November 21, 2016, will require a license in accordance with this rule.

² These notices must be updated when the source code is updated. If the source code is posted on the internet, notices of changes and modifications are not required provided that the internet location of the source code does not change.