wiley

ALERT

Commerce Eases Encryption Export Controls, Reporting Requirements

March 29, 2021

On March 29, 2021, the Department of Commerce's Bureau of Industry and Security (BIS) issued a final rule implementing certain changes in the Export Administration Regulations (EAR) agreed upon in December 2019 by governments participating in the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (Wassenaar Arrangement), a multilateral export control regime. In addition to these clarifications and modifications, the rule eases BIS's encryption controls, including eliminating certain reporting requirements for mass market products. These encryption-related changes follow the U.S. government's trend of slowly and steadily loosening controls on encryption products and reducing the regulatory burden for encryption exporters.

Background

The EAR controls the export, reexport, and in-country transfer of commercial and dual-use commodities, software, and technology. Items with encryption functionality are subject to special rules under the EAR, including export classification and reporting requirements.

Under the existing regime, exporters can self-classify most products that use encryption for data confidentiality as Export Control Classification Number (ECCN) 5A002 (hardware) or 5D002 (software). These products are known as "(b)(1)" products, and they generally can be exported to non-sanctioned destinations without a license under License Exception ENC. To rely on this exception, exporters must submit an annual report to the U.S. government listing all self-classified products exported or reexported during the prior calendar year.

Authors

Lori E. Scheetz
Partner
202.719.7419
lscheetz@wiley.law

John R. Shane
Partner
202.719.7222
jshane@wiley.law

Practice Areas

Export Controls and Economic Sanctions
International Trade
National Security

Additionally, most mass market products—*i.e.*, those products that are generally available and of interest to the public—can be self-classified as ECCN 5A992 (hardware) or 5D992 (software) and exported to all destinations other than sanctioned countries without a license. Historically, the annual reporting requirement also applied for these products.

Certain more advanced or sensitive products, such as network infrastructure items, non-public source code, encryption technology, and quantum cryptography, are considered License Exception ENC "(b)(2)" products. Other items, including encryption components such as chips and chipsets, non-standard cryptography, digital forensics products, and cryptographic activation items, are considered ENC "(b)(3)" products. These (b)(2) and (b)(3) products are generally only eligible for export under License Exception ENC after submission of a formal commodity classification request to BIS; semi-annual reporting and additional licensing requirements also apply under certain circumstances.

Changes Under the New Rule

The new rule makes a number of changes to BIS's encryption rules, including the elimination of the annual self-classification reporting requirement for most mass market products. The changes are summarized below:

- **Removal of certain mass market items from paragraph "(b)(3)" of License Exception ENC:** This rule moves mass market components (*e.g.*, chips, chipsets, electronic assemblies, and field programmable logic devices), executable software, toolsets, and toolkits—with the exception of those using non-standard cryptography—out of paragraph (b)(3) and into paragraph (b)(1) of License Exception ENC, making them eligible for self-classification. BIS noted that most cryptographic libraries and modules will remain (b)(3) items because they will not meet the requirements for mass market treatment.

- **Elimination of most mass market self-classification reporting obligations:** In a fairly significant change, BIS is no longer requiring exporters to include most mass market products in their annual self-classification reports. There is a special authorization in BIS's mass market controls that allows for mass market treatment of components and executable software that do not meet the traditional mass market criteria (*e.g.*, generally available to the public, etc.) but that are incorporated in existing mass market items. These are the only mass market items that will still require reporting in the annual submission.
- **Elimination of the notification requirements for most publicly available encryption source code and beta test software:** Formerly, BIS required exporters to submit email notifications to the U.S. government with the Internet location of publicly available encryption source code, before such source code could be released from the EAR's controls. BIS required similar notifications before permitting exports of best test encryption software.

  BIS has eliminated the email notification requirement for publicly available encryption source code, as well as beta test encryption software, as long as the source code and beta test software do not implement non-standard cryptography. (Note that non-standard cryptography generally involves incorporation or use of proprietary or unpublished cryptographic functionality, including encryption algorithms or protocols that have not been adopted or approved by a duly recognized international

standards body, *e.g.*, IEEE, IETF, ISO, ITU, ETSI, 3GPP, TIA, and GSMA, and that have not otherwise been published.)

- **Other encryption changes:** BIS's rule also expands an exclusion in the encryption controls for wireless personal area network functionality by removing the limitations on range (30 meters, or, for equipment that cannot interconnect with more than seven devices, 100 meters). As such, any item using only published or commercial cryptographic standards, where the information security functionality is limited to personal area network functionality, now falls outside of BIS's encryption controls, including related classification and reporting requirements.

  The rule also adds gateways to an existing carve-out from the encryption controls for certain items (*e.g.*, routers, switches, relays) that are limited to the tasks of Operations, Administration or Maintenance (OAM).

Apart from these encryption changes, as noted above, BIS clarified and modified several ECCNs in Categories 0, 1, 2, 3, 6, and 9 of the EAR's Commerce Control List (CCL) to align with decisions made at the Wassenaar plenary meeting in 2019. These changes follow BIS's October 2020 rule implementing revisions to the EAR related to emerging technologies, which also were agreed upon at the December 2019 plenary meeting. Companies that manufacture or engage in export transactions involving products and technologies classified in the modified CCL Categories should carefully review BIS's changes and make any necessary updates to their export classifications.

Wiley has unparalleled experience assisting clients to navigate BIS's encryption controls. Should you have any questions, please do not hesitate to contact one of the attorneys listed on this alert.

Nicole Hager, a Law Clerk at Wiley Rein LLP, contributed to this alert.