Latest regulatory changes reduce burden for software and technology companies under US export controls

International Trade Alert

6 April 2021

By: Nate Bolin | Thomas M. deButts | Nicholas Klein | Richard Newcomb

On March 29, 2021, the US Commerce Department's Bureau of Industry and Security (BIS) revised the US Export Administration Regulations (EAR) to implement export control changes agreed to by the United States and other members of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, a group of 42 countries that seeks to harmonize global export licensing policy.

Among the more significant changes, BIS has revised the reporting obligations for the export, reexport, and transfer of encryption software and commodities and revised License Exception Encryption Commodities, Software, and Technology (ENC) in ways that are expected to reduce the regulatory burden on software and hardware developers under export controls. These changes may also impact mandatory filing determinations for foreign investments subject to review by the Committee on Foreign Investment in the United States (CFIUS).

Changes to encryption reporting requirements

The EAR impose controls on the export, reexport, and transfer of software and commodities that incorporate

encryption, which includes nearly all software produced, developed, or hosted in the United States as well as many non-US software and hardware products. In most cases, companies can rely upon License Exception ENC to export, reexport, or transfer encryption products without seeking authorization from BIS.

Most encryption products (including both software and hardware) may be self-classified as Export Control Classification Number (ECCN) 5A002 (hardware) or 5D002 (software). Commodity encryption products that are generally available to the public at retail (or similar sales channels) and meet other criteria may be self-classified as "mass market" or ECCN 5A992 (hardware) or 5D992 (software). In these cases, companies have until now been required to submit an annual self-classification report to BIS and the National Security Agency listing all self-classified products that they exported or reexported during the previous year.

For more advanced or sensitive products – including network infrastructure items, non-public encryption source code, customized, non-standard, or open interface encryption, quantum cryptography, network penetration tools, network vulnerability/digital forensics items, public safety/first responder radios, ultra-wideband and spread spectrum items, and cryptanalytic items – companies must obtain a formal classification determination (known as a Commodity Classification Automated Tracking System or CCATS request) from BIS in addition to submitting semi-annual sales reports.

BIS has now reduced or eliminated these requirements for many mass market hardware and software products, as described below:

- ***Elimination of most mass market annual self-classification reports –*** The latest amendments to the EAR eliminate the need to file an annual self-classification report for the export, reexport and transfer of most "mass market" encryption items under License Exception ENC (15 C.F.R. § 740.17(b)(1)). Annual self-classification reports will now only be required for a limited subset of mass market encryption components and their "executable software" (ie, software in executable form from a covered hardware component, but not complete binary images of software) as specified in Section 740.17(e)(3) of the EAR.
- ***Certain encryption products no longer require formal classification by BIS –*** Companies previously were required to submit a CCATS request and obtain a formal classification determination from BIS prior to the export, reexport or transfer of certain mass market encryption items identified in License Exception ENC (b)(3) – including hardware components (eg, chips, chipsets, electronic assemblies, and field programmable logic devices), executable software, toolsets, and toolkits. The latest amendments eliminate the requirement to submit a CCATS request to BIS for these items. Companies instead must file annual encryption self-classification reports, significantly reducing the regulatory burden for the export of these products. Classification requests, however, are still required for such components and executable software that use non-standard cryptography and for certain cryptographic libraries and modules.
- ***Removal of notification requirement for publicly available encryption source code –*** BIS has eliminated the requirement to submit an email notification to BIS and the National Security Agency's "ENC Encryption Request Coordinator" when making encryption source code and beta test encryption software available for unrestricted download (such as through an open-source license arrangement). Once made publicly available, such encryption source code and beta test encryption software are no longer subject to export controls under the EAR. The requirement to notify BIS and the NSA is still in place, however, for publicly available encryption source code and beta test encryption software that use "non-standard cryptography" [1] such as new or novel encryption algorithms.

  This change to the email notification requirement is important for industry because many common encryption source code and beta test software files are publicly-released through an open-source license or without a license. In the past, incorporating such source code into a new, similarly open-source software program would also often trigger the email notification requirement. That requirement has now been eliminated for publicly available software that uses standard encryption. BIS estimates that this change will reduce the overall number of required email notifications by approximately 80 percent.

- ***Encryption changes for software development –*** BIS has made two changes that should reduce licensing burdens on companies engaged in software development in global consortia or with cross-border development teams. Specifically, BIS has added digital forensics software to a class of items that can be more readily considered to be "de minimis" when determining whether a non-US made product that contains US content is

subject to the EAR.BIS has also reduced the notification requirements for the use of License Exception Temporary Imports, Exports, Reexports, and Transfers (In-Country) (TMP) (15 C.F.R. § 740.9) to temporarily export beta test encryption software that does not use non-standard cryptography.

Impacts on business operations and investments

On their own, each of the above changes to the EAR regulations governing encryption items represent an incremental, although still significant, reduction in reporting burdens for industry. Collectively, however, these changes promise to significantly reduce regulatory burdens for some technology companies that regularly make use of License Exception ENC. The monitoring and preparation of these reports and CCATS requests proved to be a time consuming and costly process for many companies. With the latest updates issued by BIS, companies should see the volume of their CCATS requests and self-classification reports decline substantially. Indeed, BIS estimates that these latest changes will reduce the number of encryption self-classification reports that are filed under License Exception ENC by approximately 60 percent.

These changes will also have an important impact on the CFIUS laws governing foreign investment in software and technology companies. As explained in more detail here, a filing with CFIUS for a covered foreign investment is mandatory where the US business is engaged with "critical technologies" (which includes encryption items under ECCN 5A002 (hardware) and 5D002 (software)) that are subject to export licensing requirements to export to the country of the foreign investor. However, recent changes to the CFIUS regulations eliminated the requirement to file a mandatory declaration with CFIUS if, inter alia, the "critical technology" of the US business is eligible for export to the country of the foreign investor under Subsection (b) of License Exception ENC (15 C.F.R. § 740.17(b)). Anecdotal evidence suggests that this exception had resulted in a substantial increase in the number of CCATS ruling requests and related filings with BIS. With the latest changes to the EAR making it easier to use License Exception ENC without filing CCATS requests or self-classification reports, a greater number of investment transactions involving software and technology companies should now be exempt from CFIUS mandatory declaration filings.

As the above discussion illustrates, the relationship between the classification of software and technology under the US export control regulations and the requirements of the CFIUS regulations is complex. Companies and investors are well advised to carefully consider the application of these regulations to their portfolios and current and future investment plans. Software and technology companies that develop or otherwise engage with encryption hardware or software products should carefully review how these changes impact their reporting obligations.

Learn more about the implications of these regulatory changes for your business by contacting any of the authors.

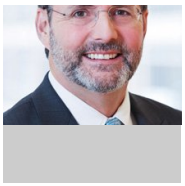
---

[1] Non-standard cryptography generally includes proprietary or unpublished cryptographic functionality, including encryption algorithms or protocols that have not been adopted or approved by a duly recognized international standards body, such as IEEE, IETF, ISO, ITU, ETSI, 3GPP, TIA, and GSMA and that have not otherwise been published.

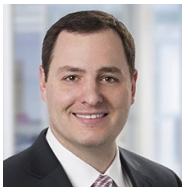
AUTHORS

Nate Bolin
Partner
Washington, DC | T: +1 202 799 4000
nate.bolin@dlapiper.com

Thomas M. deButts
Partner



Washington, DC | T: +1 202 799 4000
thomas.debutts@dlapiper.com



Nicholas Klein
Of Counsel
Washington, DC | T: +1 202 799 4000
nicholas.klein@dlapiper.com

Richard Newcomb
Partner
Washington, DC | T: +1 202 799 4000
richard.newcomb@dlapiper.com