What The New Encryption Rules Mean For U.S. Exporters

This article first appeared in *International Trade Law360*, July 1, 2010.

by Sanjay Jose Mullick

Sanjay Jose Mullick
International Trade
+1.202.663.8786
sanjay.mullick@pillsburylaw.com

Sanjay Mullick is a Washington-based member of Pillsbury's International Trade practice, where he advises clients on export issues concerning encryption software and technology and on designing and implementing export control compliance programs.

The Obama administration has taken the first step in export control reform by easing the pathway for U.S. companies to export certain encryption items.

The First Export Control Reform

On June 25, the U.S. Department of Commerce's Bureau of Industry and Security issued new regulations governing export controls on encryption. This rulemaking represents the first formal example of the president's initiative to reform U.S. export controls by concentrating regulation on the most sensitive items.

The new regulations reflect a recognition that encryption is ubiquitous in today's high-tech world and cannot be completely regulated. These rules also attempt to address the need for U.S. companies to be able to get to market quickly, to foster the competitiveness of U.S. industry. However, they do not accomplish a complete de-control of encryption, and the prior system will remain in place for many products.

Although the regulations have been published as an interim final rule with a request for comments, they likely reflect the prevailing framework for regulating encryption exports going forward. Let's take a look at some of the key elements of the new rules and how they will impact exporters.

Company-Based Framework

The new rules move away from a regulatory approach based on disclosure of the technical characteristics of the product to be exported to one focused on the profile of the company that will be making the exports.

Encryption Registration

When President Obama first announced the export control reform initiative, he stated that he wanted to change the export authorization process for encryption items "from 30 days to 30 minutes" and the new rules accomplish that. Specifically, for "less sensitive" encryption items, and for mass market items, the prior requirement to submit a technical questionnaire to BIS for it to conduct a product review has been replaced with one whereby the exporting company submits an online "encryption registration." The encryption registration consists of contact information, an overview of the company and an identification of what categories apply to the company's products.

Once the registration is submitted to BIS, the agency immediately issues a

registration number, and the company becomes authorized to export encryption products such as local area network products, small routers and mass market items. For these products, companies no longer have to submit a technical questionnaire response with information about the product's encryption algorithms and no longer have to wait 30 days to obtain authorization to export to key markets such as China and India.

Under the prior rules, it was often a good business practice for companies to make available to their customers, distributors and other business partners the classifications BIS issued pursuant to ENC review requests. This was because when BIS classified a product, other companies could rely on that classification as authority to make their own exports of the product, even if that company had not submitted the classification. Under the new rules, BIS has indicated that an exporter may rely on a producer's encryption registration (to export that producer's encryption product) without itself having to file a distinct encryption registration.

Classification Report

The company registration requirement is coupled with a requirement for the company to file an annual self-classification report. The report consists of a listing of the encryption items the company has self-classified and exported. Specifically, the report consists of the following six elements: (i) product name; (ii) model/series/part number; (iii) primary manufacturer; (iv) export control classification number; (v) encryption authorization type, e.g., ENC; and (vi) item type selector, e.g., gateway, modem or virtual private network. The report can be filed by e-mail.

One aspect of License Exception ENC many companies have disliked has been the requirement to file semi-annual reports. Although not a requirement that impinged export authorization, that reporting requirement could pose an administrative burden because it required capturing several information fields for all the applicable transactions, and doing so in a way that they could be retrieved and converted into a spreadsheet. For certain encryption items, that reporting requirement no longer applies and has been replaced with the more streamlined annual self-classification report.

Two Key Developments

Although the general easing of export controls on encryption items is important, there are two developments that are particularly key because they extend the useful scope of License Exception ENC and entirely de-control a class of items, respectively.

Encryption Technology Included

One of the limitations of License Exception ENC had been that, as to several countries, it did not authorize exports of certain "technology" necessary for manufacturing, development or testing of encryption items. This would be relevant, for example, if a company were co-developing a product with a business partner overseas and needed to exchange certain technical specifications on encryption or engage in related technical discussions. Under the prior rule, the commodity and software could be exported under License Exception ENC, but the related technology had to wait for the longer approval of an export license, delaying product development.

The new rules now grant export authorization to items classified as ECCN 5E002 after submission of a classification request, either immediately or after 30 days, depending on the country. In now extending License Exception ENC to encryption technology, this one form of export authorization is enough to proceed with all tracks of product development, i.e., the commodity itself and now also both the related software and technology. Depending on the country, the authorization may not extend to encryption technology for more sensitive items, such as for cryptanalytic items, those with an open cryptographic interface and for "non-standard cryptography" (discussed further below). Notably, the authorization also does not extend at all to certain countries typically involved in offshore manufacture and software development. For example, although India is included, China and Russia are excluded.

Ancillary Encryption De-Controlled

The new rules also entirely release from the encryption controls items where "the primary function or set of functions" is neither (i) information security, (ii) computing, (iii) information storage or transmission, nor (iv) networking, and where the cryptographic functionality is limited to supporting the primary function or set of functions. Such items now include gaming, household appliances, fire alarm systems, inventory management software and business

process automation. Exporters should review the entire list carefully to see if it applies to their business.

BIS took a sizable step in this direction in October 2008 when it created the exception for items that perform only "ancillary cryptography." Although that allowed those products to escape the review requirement, it was somewhat confusing because the products still were classified, e.g., under ECCN 5A002 and required License Exception ENC for export. The new rule allows such products to be classified as EAR99, so long as any other aspect of their functionality does not trigger a specific ECCN.

Limitations of the Changes

Alas, the new rules do not ease the regulatory burden on all encryption products. Upon a closer review, chip manufacturers and software developers may conclude the amended regulations do not provide the benefits they may seem to offer at first glance.

Encryption Components

Still subject to the traditional requirement to submit a one-time product review (now termed a classification request) and to file semi-annual product export reports are certain "encryption components" and "equivalent or related software," including (i) chips, chipsets, electronic assemblies and field programmable logic devices; (ii) cryptographic libraries, modules, development kits and toolkits; and (iii) application-specific hardware or software development kits.

Depending on the encryption algorithm and key length, this means those involved in supplying OEMs with the encryption elements of even consumer-type items, as well as companies engaged in cross-border development of their own products, generally will still likely have to follow the prior procedure. As before, whether exports are authorized to commence upon registration of the classification request or are subject to the 30-day waiting period will depend on the countries involved.

BIS has also been reluctant to grant mass market treatment to components of mass market end-items, e.g., the chip going into a consumer smartphone as opposed to the smartphone itself. This is because such components may not necessarily be sold in the same way as the final product and, until incorporated into it, they theoretically could be used in other applications.

In the future, perhaps BIS might consider extending mass market treatment to such components and software upon a clear demonstration that they are specially designed to be used exclusively with mass market end-items. For now, however, the new regulations re-affirm that generally encryption components will themselves have to satisfy the tests of large sales volume and general retail availability to be able to qualify for mass market treatment.

Non-Standard Cryptography

Also still subject to the prior review and reporting requirement are encryption commodities, software and components that provide or perform "non-standard cryptography." That term is defined as "any implementation of 'cryptography' involving the incorporation or use of proprietary or unpublished cryptographic functionality, including encryption algorithms or protocols that have not been adopted or approved by a recognized international standards body... and have not otherwise been published."

Carving out use of encryption that is published is a fairly significant policy development, but it does not go as far as it may seem.

Previously, a fairly common stumbling block for industry was using publicly available algorithms like Advanced Encryption Standard without recognizing that their incorporation or implementation into proprietary products was deemed to create a new and distinct encryption product requiring ENC review. Focusing controls on "non-standard cryptography" may go a long way toward exempting those end-products from classification and waiting period requirements.

However, use of such algorithms and protocols can still be considered nonstandard cryptography if—though standard themselves—they are being modified or customized in a particular way. Companies will likely have to conduct careful internal review of how they are using encryption before concluding they are not using "nonstandard cryptography."

These are concepts that are new even to the regulators, so at this stage the full range of their scope and applicability is not entirely clear. Instead, sorting out exactly what fits this criteria can be expected to be a focus of discussion over the coming months.

Restricted Items

License Exception ENC continues to contain a subsection previously called "ENC Restricted," which covers items such as network infrastructure software, commodities and components. BIS has revised and updated that list and it should be reviewed carefully. It also imposes classification, waiting period and reporting requirements. This subcategory of encryption items is significant because, for certain countries, an export license is required in order to export to governmental customers.

New Regulatory Architecture

In issuing the new encryption regulations, BIS indicated it would continue to review the rules, and certainly the real process of export control reform has only just begun. What these regulations do accomplish is the creation of a new architecture for regulating encryption that recognizes the reality that today encryption is a pervasive technology.

U.S. companies have to be able to develop products, consult with partners and service customers abroad swiftly to be able to compete effectively in a globalized world. At the same time, the speed at which technology can be deployed across borders places a greater strain on the systems that help safeguard national security.

As BIS consults with industry, this new framework should enable it to respond more quickly to market trends by more readily shifting items from a category of greater control to one of lesser control, calibrating the focus of export control resources on higher priority areas.