BIS Takes First Step in Export Control Reform Process by Making Significant Changes to Encryption Export Controls

By Douglas N. Jacobson, Esq.*

The U.S. Department of Commerce's Bureau of Industry and Security (BIS) took the first step in the export control reform process by publishing an interim final rule in the June 25, 2010 *Federal Register* (75 Fed. Reg. 36,481) making significant changes to the regulations governing the export of hardware and software containing encryption algorithms and functions.

The interim final rule, which took effect on the publication date, implements the President's announcement in a speech at the Export-Import Bank's annual conference in March 2010 that the current review-and-wait and semi-annual sales reporting requirements would be replaced with a "more efficient" one-time notification-and-ship process.

Developers, manufacturers and exporters of software and hardware containing encryption functionality should be aware that, while the new regulation eliminates the 30 day technical review and waiting requirement for most software and hardware currently eligible for license exception ENC and "mass market" treatment, it also establishes a new encryption registration requirement.

The new encryption rule also revises Note 4 to Category 5, Part 2 of the Commerce Control List (CCL) to exclude from the scope of encryption export controls items where the cryptography's primary function is not related to communications, networking, computing or "information security." This change, which will remove a number of currently controlled items from the scope of U.S. export controls, was a result of changes to multi-lateral encryption export controls made at the Wassenaar Arrangement's December 2009 plenary session.

In a press release issued by BIS, Assistant Secretary of Commerce for Export Administration Kevin Wolf said that the "Administration will continue to review the encryption rules to further enhance national security and ensure the continued competitiveness of U.S. encryption products. This effort will include a review of the current controls on publicly available encryption software, integrated circuits with encryption functionality, high-speed routers, and other types of restricted encryption products."

The following is a summary of the key aspects of the reforms made to U.S. export controls on software and hardware containing encryption functionality:

A. Changes Made to Encryption Review and Reporting Requirements

* Doug Jacobson is a Washington, DC-based export controls, sanctions and international trade attorney. Doug can be reached at 202-431-2407 and dnj@djacobsonlaw.com. Doug is the editor of the International Trade Law News blog (www.tradelawnews.com).

Three types encryption items had previously been subject to a 30-day technical review before they could be exported from the U.S.:

(1) mass market encryption hardware and software (classified as ECCNs 5A992.c and 5D992.c);
(2) certain less sensitive encryption hardware and software (classified as ECCNs 5A992 and 5D992) that can be exported pursuant to License Exception ENC to government and non-government end-users in destinations other than the designated terrorism-supporting countries; and
(3) sensitive encryption items (classified as ECCNs 5A002 and 5D002) that are eligible for License Exception ENC to non-government end-users in destinations other than the designated terrorism-supporting countries (Country Group E).

The June 25, 2010 encryption reform rule removes the 30 day technical review requirement for most mass market and license exception ENC unrestricted items, including Local Area Network (LAN) products, small routers, and most items that meet the multilateral Wassenaar Arrangement “mass market” criteria.

As a result of the new regulation, developers and manufacturers of encryption hardware and software may now self-classify their products and export them following the submission of a company encryption registration to BIS, which is discussed in more detail below.

The new regulation specifies that certain mass market and unrestricted items will remain subject to the 30-day technical review and semi-annual reporting requirements. These items include: encryption components; items that provide or perform non-standard cryptography; certain items providing or performing vulnerability analysis, network forensics or computer forensics; and cryptographic enabling commodities and software.

In addition, certain “restricted items”, such as network infrastructure items that exceed certain technical performance parameters, such as routers and 3G wireless base stations, will also remain subject to the 30-day technical review and semi-annual sales reporting requirements.

BIS’s encryption reform regulation also extends the scope of License Exception ENC eligibility to most encryption technology necessary for manufacturing, development or testing of encryption items to all countries, except those of national security concern or subject to anti-terrorism controls, after the submission of a 30-day review to BIS.

The June 25, 2010 regulation makes a number of important and useful changes to the export of “mass market” products that contain encryption functionality. Mass market encryption products include hardware and software that are sold in large quantities and are generally available to the public through common retail methods, such as retail stores or internet sales. As a result of the changes made by the new regulation,

exporters and manufacturers of mass market encryption products may now self-classify their products and export them after submission of a company encryption registration to BIS. An annual self-classification report will also be required to be submitted to BIS.

BIS estimates that the changes made by the encryption reform regulation should decrease technical review submissions by approximately 70% and semi-annual reporting by up to 85%.

B. Changes Made to Items Incorporating "Ancillary Cryptography"

At the December 2009 plenary meeting, the Wassenaar Arrangement's member countries agreed to decontrol items meeting the "ancillary cryptography" criteria. BIS's June 25, 2010 rule implements those changes by adding Note 4 to Category 5, Part 2, of the CCL and by removing all references to "ancillary cryptography" from the EAR. The new Note 4 to Category 5, Part 2, reads as follows:

> **Note 4:** Category 5, Part 2 does not apply to items incorporating or using "cryptography" and meeting all of the following:
> a. The primary function or set of functions is not any of the following:
> 1. "Information security";
> 2. A computer, including operating systems, parts and components therefor;
> 3. Sending, receiving or storing information (except in support of entertainment, mass commercial broadcasts, digital rights management or medical records management); or
> 4. Networking (includes operation, administration, management and provisioning);
> b. The cryptographic functionality is limited to supporting their primary function or set of functions; and
> c. When necessary, details of the items are accessible and will be provided, upon request, to the appropriate authority in the exporter's country in order to ascertain compliance with conditions described in paragraphs a. and b. above.

As a result of these changes, hardware and software incorporating or using "cryptography" will no longer be classified under Category 5, Part 2 if their primary function is not communications, networking, computing or "information security" and the cryptographic functionality is limited to supporting the primary function. Examples of such items include robotics, household appliances, fire alarm systems, inventory management software and transportation systems. Such items may be classified under another category of the CCL or as EAR99.

The change to Note 4 is a significant one, as many items previously classified in Category 5, Part 2 of the CCL will now be classified as EAR99 and will no longer require an encryption review or encryption registration to be exported or reexported.

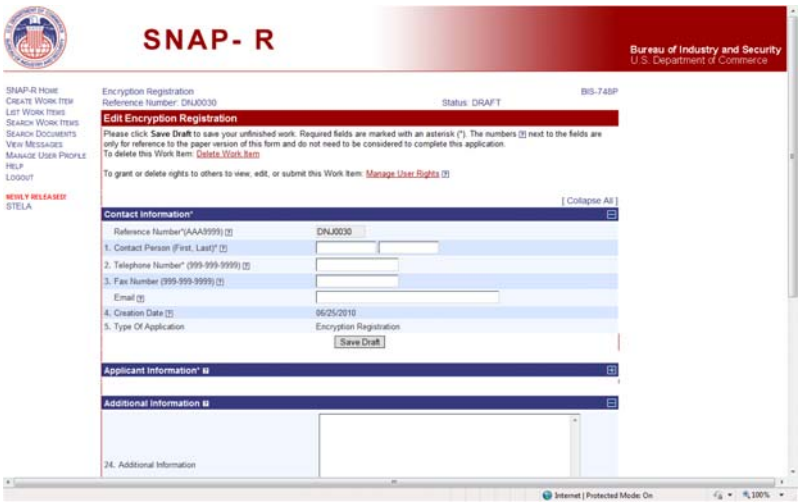
C. New Encryption Registration Process and Annual Report

In lieu of the previous technical review process required for certain hardware and software products eligible for license exception ENC and mass market treatment BIS has established a new encryption registration process in SNAP-R (https://snapr.bis.doc.gov/snapr), BIS's online licensing and classification system. Once an encryption registration is submitted to BIS in SNAP-R, BIS will issue the applicant an Encryption Registration Number (ERN), which will start with an "R" and will be followed by 6 digits, e.g., R123456.

In order to obtain an ERN, the applicant will have to provide certain information about the company and provide a PDF document containing the answers to seven questions that are contained in new Supplement No. 5 to part 742 of the EAR. The information that will need to be provided to BIS for purposes of obtaining an encryption registration includes:

(1) Company point of contact information;
(2) Name of company that exports the encryption items;
(3) The categories of the company's products (e.g., wireless, mobile, computing, network infrastructure, information security, gaming);
(4) Whether the products incorporate or use proprietary, unpublished or nonstandard cryptographic functionality;
(5) Whether the exporting company will export encryption source code;
(6) Whether the products incorporate encryption components produced or furnished by non-U.S. sources or vendors; and
(7) Whether the products are manufactured outside the United States.

The following is a screenshot of the new Encryption Registration function in SNAP-R:



Upon submission of all of the required information in SNAP-R, the applicant will receive an ERN within a few minutes to an hour. Once the ERN is received the manufacturer's encryption items become eligible for export and reexport under the applicable provision

of license exception ENC (section 740.17(b) of the EAR) and mass market (section 742.15(b) of the EAR), subject to the conditions and restriction of those sections.

A company that exports under the ERN does not need to resubmit its encryption registration unless the answers to the questions in Supplement No. 5 to Part 742 changed during the previous calendar year.

BIS expects developers and manufacturers of encryption hardware and software to provide their ERNs to their customers. However, if the manufacturer will not share its ERN, has not filed for an ERN, or the customer cannot determine the manufacturer's ERN, then the exporter (non-producer) should obtain their own ERN via SNAP-R.

For those companies submitting encryption registrations, the new regulation requires companies to submit an annual self-classification report. The purpose of the report is to allow BIS and the National Security Agency to verify the classification of encryption products exported under the new self-classification provisions. The annual report has very specific format requirements that are set forth in new Supplement No. 8 to Part 742of the EAR. The information in the report must be provided in tabular or spreadsheet form, as an electronic file in comma separated values format (CSV), and submitted as an attachment to an e-mail to BIS and the ENC Encryption Request Coordinator at Fort Meade, Maryland no later than February 1 of the year following the calendar year in which the encryption items are exported.

D. Other Changes Made to Encryption Export Controls

BIS's encryption reform regulation made a number of other changes to the regulations governing encryption export controls, including:

- Replacing the term "review request" with "classification request."
- Elimination of requirement to file separate encryption classification requests (formerly known as encryption review requests) with BIS and the ENC Encryption Request Coordinator at Fort Meade when classification submission is made via SNAP-R (however, all reports must continue to be submitted to both BIS and the ENC Encryption Request Coordinator).
- Reduction in the number of situations where exporters are required to submit the detailed information in Supplement No. 6 to Part 742 of the EAR and renames Supplement No. 6 as the "Technical Questionnaire for Encryption Items."
- Eliminates definition of "personalized smart card" since that term is no longer used.

With respect to encryption items that have been subject to previous encryption reviews and classifications, the June 25, 2010 regulation contains a provision grandfathering most items previously reviewed and classified for export under the previous requirement and such items will not be subject to the new encryption registration or reporting requirements, as long as the encryption functionality has not changed.

Pending technical review requests, including requests for items eligible for self-classification pursuant to the June 25, 2010 rule, will continue to be processed and BIS will issue a CCATS under the amended provisions of the EAR. In addition, BIS has advised that an Encryption Registration is not required to be submitted for pending requests since they are considered grandfathered under the old regulations.

D. Conclusion

While the June 25, 2010 regulation is only the first step in the export control reform process, the regulation is a major step in the right direction and should decrease the time and expense necessary for manufacturers and exporters of encryption hardware and software to comply with U.S. export control requirements.

However, this regulation is far from perfect. For example, the new encryption registration process and use of the Encryption Registration Number is bound to raise a number of practical issues, particularly from exporters and distributors of software and hardware products who are not themselves developers and manufacturers and must rely upon their suppliers to obtain ERNs. In addition, this regulation does not make any changes to a number of important encryption-related issues, including open source and publicly available encryption software, integrated circuits with encryption functionality and other types of restricted encryption products.

As a result, manufacturers, developers and exporters of encryption hardware and software should take advantage of the opportunity to submit comments on the scope and other aspects of the new regulation within the 60-day comment period.