Federal Register

Friday,
June 25, 2010

Part II

Department of Commerce

Bureau of Industry and Security

15 CFR Parts 730, 734, 738, et al.

Encryption Export Controls: Revision of License Exception ENC and Mass Market Eligibility, Submission Procedures, Reporting Requirements, License Application Requirements, and Addition of Note 4 to Category 5, Part 2; Interim Final Rule

DEPARTMENT OF COMMERCE

Bureau of Industry and Security

15 CFR Parts 730, 734, 738, 740, 742, 748, 772 and 774

[Docket No. 100309131–0195–02]

RIN 0694–AE89

Encryption Export Controls: Revision of License Exception ENC and Mass Market Eligibility, Submission Procedures, Reporting Requirements, License Application Requirements, and Addition of Note 4 to Category 5, Part 2

AGENCY: Bureau of Industry and Security, Commerce.

ACTION: Interim final rule, with request for comments.

SUMMARY: The Bureau of Industry and Security (BIS) is amending the Export Administration Regulations (EAR or Regulations) to modify the requirements of License Exception ENC, "Encryption Commodities, Software and Technology," and the requirements for qualifying an encryption item as mass market. BIS is also amending specific license requirements for encryption items. With respect to encryption products of lesser national security concern, this rule replaces the requirement to wait 30 days for a technical review before exporting such products and the requirement to file semi-annual post-export sales and distribution reports with a provision that allows immediate authorization to export and reexport these products after electronic submission to BIS of an encryption registration. A condition of this new authorization for less sensitive products is submission of an annual self-classification report on these commodities and software exported under License Exception ENC. With respect to most mass market encryption products, this rule similarly replaces the requirement to wait 30 days for a technical review before exporting and reexporting such products with a provision that allows immediate authorization to export and reexport these products after electronic submission to BIS of an encryption registration, subject to annual self-classification reporting for exported encryption products. Only a few categories of License Exception ENC and mass market encryption products will continue to require submission of a 30-day classification request. Encryption items that are more strictly controlled continue to be authorized for immediate export and reexport to most end-users located in close ally countries upon submission of an encryption registration and classification request to BIS. This rule also eases licensing requirements for the export and reexport of many types of technology necessary for the development and use of encryption products, except to countries subject to export or reexport license requirements for national security reasons or anti-terrorism reasons, or that are subject to embargo or sanctions. This rule also removes the requirement to file separate encryption classification requests (formerly encryption review requests) with both BIS and the ENC Encryption Request Coordinator (Ft. Meade, MD).

BIS is also amending the EAR by implementing the agreements made by the Wassenaar Arrangement at the plenary meeting in December 2009 that pertained to "information security" items. This rule adds an overarching note to exclude particular products that use cryptography from being controlled as "information security" items. The addition of this note focuses "information security" controls on the use of encryption for computing, communications, networking and information security. This rule also makes additional changes throughout the EAR to harmonize it with the new note.

This rule also replaces a note in ECCN 5A002 pertaining to personalized smart cards with a note pertaining to smart cards and smart readers/writers. As a result of this change, a definition is being removed from the EAR.

DATES: This rule is effective: June 25, 2010. Comments must be received by August 24, 2010.

ADDRESSES: You may submit comments, identified by RIN 0694–AE89, by any of the following methods:

- *Federal eRulemaking Portal: http://www.Regulations.gov.* Please follow the instructions for submitting comments.
- *E-mail: publiccomments@bis.doc.gov.* Please include RIN 0694–AE89 in the subject line.
- *Mail or Hand Delivery/Courier:* U.S. Department of Commerce, Bureau of Industry and Security, Regulatory Policy Division, 14th and Pennsylvania Ave., NW., Room H–2705, Washington, DC 20230; or by fax to (202) 482–3355. Please insert "0694–AE89" in the subject line of comments.

Comments regarding the collections of information associated with this rule, including suggestions for reducing the burden, should be sent to OMB Desk Officer, New Executive Office Building, Washington, DC 20503, Attention: Jasmeet Seehra, or by e-mail to *Jasmeet_K._Seehra@omb.eop.gov* or by fax to (202) 395–7285; and to the Office of Administration, Bureau of Industry and Security, Department of Commerce, 14th and Pennsylvania Ave., NW., Room 6883, Washington, DC 20230.

FOR FURTHER INFORMATION CONTACT: For technical questions contact: The Information Technology Division, Office of National Security and Technology Transfer Controls within BIS at 202–482–0707 or by e-mail at *encryption@bis.doc.gov.*

For other questions contact: Sharron Cook, Office of Exporter Services, Bureau of Industry and Security, U.S. Department of Commerce at (202) 482–2440 or by e-mail at *scook@bis.doc.gov.*

SUPPLEMENTARY INFORMATION:

Background

To protect and preserve foreign policy and national security interests, the United States maintains export controls on encryption items. Encryption items may be used to maintain the secrecy of information, and therefore may be used by persons abroad to bring harm to law enforcement, and U.S. foreign policy and national security interests. The U.S. Government has a critical interest in ensuring that the legitimate needs for protecting important and sensitive information of the public and private sectors are met, and that persons opposed to the United States are not able to conceal hostile or criminal activities.

When dual-use encryption items were transferred from the United States Munitions List (USML) to the CCL on December 6, 1996, a foreign policy reason for control, Encryption Items (EI), was imposed on these items. A license is required to export or reexport EI-controlled items classified under Export Control Classification Numbers (ECCNs) 5A002, 5D002 and 5E002 on the CCL to all destinations except Canada. All items controlled for EI reasons are also controlled for National Security (NS) reasons.

This rule enhances national security by focusing encryption export controls and streamlining the collection and analysis of information about encryption products, through reforms that include:

- Removing review requirements for less sensitive encryption items;
- Establishing a company registration requirement for encryption items under License Exception ENC or as mass market encryption items;
- Creating an annual self-classification report requirement for such items pursuant to an encryption registration;

• Making encryption technology eligible for export and reexport under License Exception ENC, except to countries of highest concern;
• Lifting the semi-annual sales reporting for less sensitive encryption items under License Exception ENC;
• Removing the 30-day delay to export and reexport less sensitive encryption items under License Exception ENC; and
• Removing the 30-day delay to make most mass market encryption items eligible for mass market treatment.

BIS is making these amendments to protect national security in the face of an ever-changing global marketplace for encryption items and to ensure continued United States adherence to multilateral regime commitments. The changes in this rule are discussed either topically or by section of the EAR, as applicable. This rule is the first step in the President's effort to reform U.S. encryption export controls to enhance national security by ensuring the continued competitiveness of U.S. encryption products, reducing paperwork requirements for less sensitive encryption items, making the process for submission more efficient, updating the control parameters for controlled encryption items and addressing the impact of export controls on electronic components having encryption functionality. The U.S. Government will also review other issues related to encryption controls, in keeping with national security requirements and multilateral regime commitments.

Review Request vs. Classification Request

This rule replaces the term "review request" with "classification request" in sections 740.17 and 742.15 so that the terminology used in the encryption regulations is consistent with the terminology used for other items on the Commerce Control List (CCL).

Submissions Requirements for Encryption Items

Prior to this rule, the EAR required exporters to submit review requests to both BIS and the ENC Encryption Request Coordinator. This new rule will reduce the paperwork burden on applicants by removing the requirement for applicants to submit requests to the ENC Encryption Request Coordinator when the submission is made via Simplified Network Application Processing system (SNAP–R) for Encryption Registration and Encryption Classification Requests. Upon effectiveness of this rule, BIS will send encryption SNAP–R submissions to the ENC Encryption Request Coordinator. This change will decrease the paperwork burden on the applicants. However, all reports (*i.e.,* the semi-annual sales report and the annual self-classification report) must continue to be submitted to both BIS and the ENC Encryption Request Coordinator.

Supplement No. 1 to Part 730—"Information Collection Requirements Under the Paperwork Reduction Act: OMB Control Numbers"

This supplement is amended by removing the title for collection number 0694–104 and adding in its place "Commercial Encryption Items under Commerce Jurisdiction."

Section 734.4—De Minimis U.S. Content

This rule makes changes to (b)(1)(ii), (b)(1)(iii) and (b)(2) to harmonize with changes to encryption procedures under sections 740.17 and 742.15(b). Paragraph (v) is added to section 734.4(b)(1) to indicate that encryption commodities and software may be considered for *de minimis* treatment if such products were authorized for export under License Exception ENC after submission of an encryption registration pursuant to section 740.17(b)(1) of the EAR.

Section 738.4—Determining Whether a License Is Required

This rule revises the third sentence in paragraph 738.4(a)(2)(ii)(B) of the EAR by replacing "review" with "encryption registration and classification" to harmonize it with the new submission requirements for encryption items.

Section 740.17—License Exception ENC

This rule revises the first sentence in sections 740.17 and 740.17(b)(2) to describe more clearly the types of items eligible for export and reexport under License Exception ENC.

Section 740.17(a)—No Classification Request, Registration or Reporting Required

This rule amends section 740.17(a) by removing references to "review" and by adding references to the encryption registration, classification requests, self-classification reports and sales reports to harmonize it with the new submission requirements for encryption items. This amendment does not change any requirements or eligibility under section 740.17(a) of the EAR.

Immediate Authorization for Less Sensitive Encryption Items and Certain Mass Market Encryption Items With the Submission of an Encryption Registration and Subsequent Self-Classification Annual Report

Prior to this rule, eligibility under section 740.17(b)(3) of License Exception ENC and mass market treatment under section 742.15(b) required prior submission of a review request and 30-day technical review for most encryption items. This system of authorization centered on product-by-product authorizations. The new system of authorization implemented by this rule is based on company authorizations that operate like a bulk license for the company's products. This rule establishes two new procedures—*i.e.,* the company encryption registration and the annual self-classification report—that will allow the export without a 30-day technical review for less sensitive encryption items under License Exception ENC and less sensitive mass market encryption items. The company registration requirement is described in the new Supplement No. 5 to part 742 of the EAR. Special instructions for submitting an encryption registration using SNAP–R are in paragraph (r) of Supplement No. 2 to part 748 of the EAR. Because of this shift from product authorization to company authorization, the information in block 14 (applicant) of the encryption registration screen and the information in Supplement No. 5 to part 742 must pertain to the company that seeks authorization to export and reexport encryption items that are within the scope of this rule. An agent for the exporter, such as a law firm, should not list the agent's name in block 14. The agent may, however submit the encryption registration and list itself in block 15 ("other party authorized to receive license") of the encryption registration screen in SNAP–R. The follow-on self-classification report would be required to be submitted annually to BIS and the ENC Encryption Request Coordinator in February for items exported or reexported the previous calendar year (*i.e.,* January 1 through December 31) pursuant to the encryption registration and applicable sections 740.17(b)(1) or 742.15(b)(1) of the EAR.

An encryption registration is only required for authorization under License Exception ENC sections 740.17(b)(1), 740.17(b)(2) and 740.17(b)(3), and mass market encryption sections 742.15(b)(1) and 742.15(b)(3) of the EAR. Exports and reexports described under sections 740.17(a), 740.17(b)(4), 740.17(c) and

742.15(b)(4) will continue to be authorized without the need for a submission. A company that exports under the authorizations described in this rule only needs to register once and 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. Because exporters of encryption items may not be the producers of those encryption items, they may not know the answers to some of the questions in Supplement No. 5 to part 742, BIS has included instructions in Supplement No. 5 to account for this situation.

When an encryption registration is submitted via SNAP–R, SNAP–R will issue an Encryption Registration Number (ERN), which will start with an "R" and will be followed by 6 digits, *e.g.,* R123456. This ERN authorizes under License Exception ENC exports or reexports of the commodities classified under ECCNs 5A002.a.1, .a.2, .a.5, .a.6, or .a.9, or ECCN 5B002, and equivalent or related software classified under ECCN 5D002, except any such commodities, software or components described in paragraphs (b)(2) or (b)(3) of section 740.17 of the EAR. The ERN also authorizes exports and reexports of commodities and software that are released from "EI" and "NS" controls under section 742.15(b)(1) and are classified under ECCNs 5A992 and 5D992, respectively. These authorizations require submission of a self-classification report to BIS and the ENC Encryption Request Coordinator, in accordance with section 742.15(c) and Supplement No. 8 to part 742 of the EAR. For encryption items authorized after the submission of an encryption registration under sections 740.17(b)(1) or 742.15(b)(1), the filer may be required to provide relevant information about the encryption functionality of the items. BIS may request the filer to provide information described in Supplement No. 6 to part 742.

Prior to this rule, when 30-day technical review and classification by BIS was required for these less sensitive encryption items which may now be self-classified under section 740.17(b) or 742.15(b), many producers of these items made their encryption classifications (CCATS) available for other parties to use when exporting or reexport their products. Under this rule, when an exporter or reexporter relies on the producer's self-classification (pursuant to the producer's encryption registration) or CCATS for an encryption item, the exporter or reexporter is not required to submit a separate encryption registration, classification request or self-classification report to BIS under section 740.17(b) or 742.15(b). Those who submit encryption registrations, classification requests and self-classification reports should either be knowledgeable enough about the encryption functionality to answer relevant questions pertaining to their submissions, or else possess the requisite authority or other means to ensure that such information will be made available to BIS upon request. Only License Exception ENC and mass market encryption authorizations under sections 740.17(b) and 742.15(b) to a company that has fulfilled the requirements of encryption registration (such as the producer of the item) authorize the export and reexport of the company's encryption items by all persons, wherever located, under these sections.

New License Exception ENC Eligibility for Most Encryption Technology, to Non-"Government End-Users" Outside Country Group D:1 or E:1

In section 740.17(b)(2)(iv)(B), encryption technology classified under ECCN 5E002 that are not technology for "cryptanalytic items," "non-standard cryptography," or "open cryptographic interfaces" may now be exported and reexported under License Exception ENC to any non-"government end-user" located in a country not listed in Country Groups D:1 or E:1 of Supplement No. 1 to part 740. This change will eliminate redundant license approvals for expired technology licenses to the same end-users and provide exporters with a more predictable timeframe for authorization, while maintaining U.S. Government review of such technology under License Exception ENC. Previously, all such exports and reexports of ECCN 5E002 encryption technology to end-users other than U.S. subsidiaries and companies located or headquartered in a country listed in Supplement No. 3 to part 740 required a license. This revision will decrease encryption licensing arrangements (ELAs) and other license applications to export or reexport encryption technology by approximately 60%.

Technical Revisions to Sections 740.17(b)(2) and 740.17(b)(3)

This rule updates the License Exception ENC specific list of restricted items in section 740.17(b)(2), and creates a new specific list of additional sensitive items in amended section 740.17(b)(3).

This rule adds a new paragraph section 740.17(b)(2)(i)(A)(*3*) (formerly included in section 740.17(b)(2)(i)) to clarify that network infrastructure software and commodities and components providing satellite communications are included on the list of items subject to section 740.17(b)(2) if they provide transmission over satellite at data rates exceeding 10 Mbps with encryption key lengths exceeding 80 bits for symmetric algorithms. The 10 Mbps parameter (formerly described in paragraph (b)(2)(i)(D)(*1*)) is included in paragraph (b)(2)(i)(A)(*5*) in this rule, for air-interface coverage at operating ranges beyond 1,000 meters.

This rule amends the lists of items formerly at section 740.17(b)(2)(iii)(A) and adds items to the new specific list in section 740.17(b)(3). These amendments are consistent with determinations that, for national security reasons, encryption commodities and software that provide penetration capabilities that can be used to attack, deny, disrupt or otherwise impair the use of cyber infrastructure or networks require a license in order to be exported to "government end users" in countries other than countries listed in Supplement No. 3 to part 740. This change is implemented in new paragraph section 740.17(b)(2)(i)(F).

In addition, for national security reasons, classification requests with a 30-day review period continue to be required for items that are not described in the updated section 740.17(b)(2) and that provide or perform vulnerability analysis, network forensics, or computer forensics characterized by any of the following: automated network analysis, visualization, or packet inspection for profiling network flow, network user or client behavior, or network structure/topology and adapting in real-time to the operating environment; or investigation of data leakage, network breaches, and other malicious intrusion activities through triage of captured digital forensic data for law enforcement purposes or in a similarly rigorous evidentiary manner. Therefore, this rule includes these items in the new specific list of items in section 740.17(b)(3)(iii).

To clarify the previous provision related to "public safety radio," this rule creates a new and expanded paragraph for public safety/first responder radios with the addition of section 740.17(b)(2)(G). Former section 740.17(b)(2)(iii)(A) is removed by this rule. The new subparagraph (G) gives two examples of public safety/first responder radio—Terrestrial Trunked Radio (TETRA) and "P25" standards. This is a clarification and does not change the license requirements or license exception eligibility for public safety/first responder radios.

Revisions for Harmonization Purposes

For national security reasons, this rule maintains all existing licensing requirements for exports and reexports of "cryptanalytic items" (*i.e.,* cryptanalytic commodities, software, and technology.) This rule adds new note 3 to the introductory paragraph of section 740.17(b)(2) and new section 740.17(b)(2)(ii) (formerly § 740.17(b)(2)(iv)) to clarify that exports and reexports of "cryptanalytic items" require encryption registration and encryption classification requests, with no wait, to be eligible for License Exception ENC to non-"government end-users" located or headquartered in countries listed in Supplement No. 3 to part 740, and that the export or reexport of cryptanalytic commodities and software (listed in new section 740.17(b)(2)(ii)) require submission of an encryption registration and a 30-day classification request before being eligible for License Exception ENC to non-"government end-users" located or headquartered in a country not listed in Supplement No. 3 to part 740 of the EAR. On account of the utmost sensitivity of cryptanalytic technology transfers, cryptanalytic "technology" classified under ECCN 5E002 is only License Exception ENC eligible to non-"government end-users" located or headquartered in Supplement No. 3 to part 740 countries.

This rule adds a new section 740.17(b)(2)(iv) to describe specific encryption technology. Prior to this rule, all encryption technology under ECCN 5E002 required an encryption review, with no wait, for exports under License Exception ENC to any end-users located or headquartered in countries listed in Supplement No. 3 to part 740. These provisions are maintained in Notes 1 and 3 to the introductory paragraph of section (b)(2). New section 740.17(b)(2)(iv) differentiates between "non-standard cryptography" and other encryption technology. Section 740.17(b)(2)(iv)(A) maintains the authorization for "non-standard cryptography" classified under ECCN 5E002 to be exported under License Exception ENC upon submission (*i.e.,* no wait) of an encryption classification request, including the submission of the answers to questions contained in Supplement No. 5 and Supplement No. 6 to part 742, to any end-user located or headquartered in a country listed in Supplement No. 3 to part 740 of the EAR. Section 740.17(b)(2)(iv)(B) authorizes the use of License Exception ENC for the export of technology other than technology for "cryptanalytic items," "non-standard cryptography" or "open cryptographic interfaces" to any non-"government end-user" located in a country not listed in Country Group D:1 or E:1 of Supplement No. 1 to part 740, 30-days after submission of an encryption registration and an encryption classification request.

This rule also moves paragraphs in section 742.15 to align them with related paragraphs in section 740.17. For example, provisions for encryption components may be found in sections 740.17(b)(3)(i) and 742.15(b)(3)(i).

"Encryption Components" and "Non-Standard Cryptography"—Sections 740.17(b)(3) and 742.15(b)(3)

The requirement for submission of an encryption classification request and information described in Supplement No. 6 to part 742, and a 30-day wait, while BIS performs its review of these submissions remains in effect for all "encryption components," including mass market "encryption components," and for encryption commodities, software and components not described in section 740.17(b)(2) that provide or perform "non-standard cryptography," including mass market encryption commodities, software and components. "Encryption components" are defined in part 772, and this rule adds a new definition of "non-standard cryptography" in part 772. "Encryption components" are chips, chipsets, electronic assemblies and field programmable logic devices, cryptographic libraries, modules, development kits and toolkits, including for operating systems and cryptographic service providers and application-specific hardware or software development kits implementing cryptography. The requirements that these items continue to be subject to the 30-day encryption classification requests are set forth in sections 740.17(b)(3) and 742.15(b)(3). BIS and other agencies continue to study and discuss the impact of export controls on encryption components, including system software libraries, toolkits and electronic components having encryption functionality.

Cryptographic Enabling Commodities, Software and Components

This rule maintains the 30-day technical review requirement for commodities, software and components that activate or enable cryptographic functionality in encryption products which would otherwise remain disabled. Commodities, software and components for the cryptographic activation of most encryption products eligible for License Exception ENC (*i.e.,* §§ 740.17(b)(1), 740.17(b)(3)(ii) or 740.17(b)(3)(iii)) or mass market treatment (*i.e.,* §§ 742.15(b)(1) or 742.15(b)(3)(ii)) are covered in sections 740.17(b)(3)(iv) and 742.15(b)(3)(iv), respectively. Cryptographic activation items associated with restricted encryption commodities, software and components are covered under section 740.17(b)(2), as further explained by a note to paragraph (b)(2). Meanwhile, items described under sections 740.17(b)(3)(i) or 742.15(b)(3)(i) (including certain activation components and software) are covered by those sections as applicable.

Section 740.17(b)(4)—Exclusions From Classification Request and Encryption Registration Requirements

This rule removes all references to "ancillary cryptography" by removing the last sentence in paragraph (b)(4)(i) and removing paragraph (b)(4)(iv). This rule also removes the empty placeholder paragraph (b)(4)(iii). Items that were covered by the "ancillary cryptography" provisions are now excluded from control under Category 5 part 2 of the CCL with the addition of Note 4. An explanation of the changes to Note 4 are described in more detail below under the heading "Note 4 to Category 5, Part 2."

Reporting Requirements Under License Exception ENC

Prior to this rule, semi-annual (post-export) sales reporting was required for exports of most encryption commodities, software and components previously described in section 740.17(b)(3) to all destinations other than Canada, and for reexports from Canada, under License Exception ENC. This rule narrows the scope of this requirement to only apply to certain digital forensics items described under new section 740.17(b)(3)(iii). Therefore, this rule removes some of the exclusions from reporting requirement paragraphs that were formerly in paragraphs (A), (C), (H), (I) and (J) of section 740.17(e)(iii), because they are no longer necessary. When sales reporting is not required under License Exception ENC, companies need only maintain records as required by the EAR that can be reviewed by appropriate agencies of the U.S. Government upon request. The requirement for semi-annual sales reporting to BIS and the ENC Encryption Request Coordinator of encryption items described in section 740.17(b)(2) is maintained. As a result of these changes, BIS expects that the number of semi-annual reports submitted to BIS annually will be reduced from 400 to less than 100 submissions per year.

Section 742.15—Encryption Items

This rule removes all references to "ancillary cryptography" by removing the last sentence formerly in paragraph (b)(3)(i) and removing paragraph (b)(3)(iii). This rule also removes the empty placeholder formerly in paragraph (b)(3)(ii). With the new harmonization of paragraphs between sections 740.17 and 742.15, paragraph (b)(3)(i) is redesignated as paragraph (b)(4)(i).

This rule adds a new paragraph (b)(4)(ii) to exclude submission requirements under section 742.15 for reexports of US-origin mass market encryption commodities and software subject to the EAR or foreign origin products developed with or incorporating U.S.-origin mass market encryption source code, components or toolkits subject to the EAR, that have met the submission requirements in section 742.15. This paragraph is exactly the same as the paragraph in section 740.17(b)(4)(ii), which excludes submission requirements for reexports of US-origin encryption items subject to the EAR or foreign products developed with or incorporating U.S.-origin encryption source code, components or toolkits subject to the EAR, that have met the submission requirements in License Exception ENC under section 740.17.

Supplement No. 5 to Part 742

This rule removes all text of Supplement No. 5 to part 742 and replaces it with seven (7) questions of the "Encryption Registration." As discussed above under the topic heading "Immediate authorization for less sensitive encryption items and certain mass market encryption items with the submission of an encryption registration and subsequent self-classification annual report," an encryption registration is required for most exports under License Exception ENC, and to be eligible for mass market treatment under section 742.15(b)(1). The questions in Supplement No. 5 to part 742 ask for information about:

(1) The point of contact information;

(2) The company that exports the encryption items;

(3) The categories of the company's products;

(4) Whether the products incorporate or use proprietary, unpublished or non-standard 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.

If the registrant is not the principal producer of encryption items, the registrant may answer questions 4 and 7 as "not applicable." For all other questions, an answer must be given, or if the registrant is unsure of the answer, the registrant may state that it is unsure and explain why it is unsure of the answer to the question.

Supplement No. 6 to Part 742

This rule reduces the instances when exporters are required to submit the information requested in Supplement No. 6 to part 742. Prior to this rule, exporters were required to submit the information in Supplement No. 6 to part 742 for every review request for License Exception ENC and mass market encryption products. With the publication of this rule, submission of the information in Supplement No. 6 to part 742 is now only required in support of a 30-day encryption classification request for specified items under License Exception ENC and mass market commodities, software and components (*i.e.,* restricted § 740.17(b)(2) items, specified components and digital forensics items, products that provide or perform "non-standard cryptography," and cryptographic enabling commodities and software). All other items under License Exception ENC and mass market items may receive immediate authorization with the submission of the encryption registration and annual self-classification report.

The title of Supplement No. 6 to part 742 is renamed "Technical Questionnaire for Encryption Items" (formerly "Guidelines for Submitting Review Requests for Encryption Items"). The text explaining how and where to submit a review request is removed because, as explained earlier in the preamble, this rule modifies submission requirements. This rule also harmonizes the text in Supplement No. 6 to part 742 with the new procedure of only submitting this information to BIS with classification requests, unless BIS specifically requests this information in support of an encryption registration or self-classification report. Paragraph (b) is removed because a duplicate submission to the ENC Encryption Request Coordinator and BIS is no longer necessary. The information now only needs to be submitted to BIS via SNAP–R. Paragraph (f) is removed as a consequence of removing the review request procedure. Therefore, paragraphs (c), (d) and (e) are now redesignated as paragraphs (b), (c) and (d). Also, newly designated paragraph (b)(11) (formerly paragraph (c)(11)) is revised to remove outdated text.

Supplement No. 8 to Part 742—Self-Classification Report

In order to protect the national security of the United States and verify the classification of encryption products exported pursuant to sections 740.17(b)(1) and 742.15(b)(1), this rule adds Supplement No. 8 to part 742 "Self-Classification Report" to collect information about such encryption products. Supplement No. 8 to part 742 sets forth questions that must be answered about each encryption item exported pursuant to sections 740.17(b)(1) and 742.15(b)(1). The information requested is:

(1) Name of product;

(2) Model/series/part number;

(3) Primary manufacturer;

(4) ECCN (5A002, 5B002, 5D002, 5A992 or 5D992);

(5) Encryption authorization (*i.e.,* 'ENC' for License Exception ENC or 'MMKT' for mass market); and

(6) Type descriptor to describe the product (chose one from a list of 49 options).

The self-classification report must be submitted as an attachment to an e-mail to BIS and the ENC Encryption Request Coordinator. Reports to BIS must be submitted to a newly created e-mail address for these reports (*crypt-supp8@bis.doc.gov*). Reports to the ENC Encryption Request Coordinator must be submitted to its existing e-mail address (*enc@nsa.gov*). The report has very specific format requirements outlined in Supplement No. 8 to part 742. The information in the report must be provided in tabular or spreadsheet form, as an electronic file in comma separated values format (.csv), only. No other formats other than .csv will be accepted. In lieu of e-mail, submissions of disks and CDs may be mailed to BIS and the ENC Encryption Request Coordinator as specified in section 742.15(c)(2)(ii). A self-classification report for applicable encryption commodities, software and components exported or reexported during a calendar year (January 1 through December 31) must be received by BIS and the ENC Encryption Request Coordinator no later than February 1 the following year. If no information has changed since the previous report, an e-mail must be sent stating that nothing has changed since the previous report or a copy of the previously submitted report must be submitted. No self-classification report is required if no exports or reexports of applicable items pursuant to an encryption registration were made during the calendar year.

Part 748—Application and Documentation

This rule revises the introductory paragraphs to sections 748.1(a) and (d) to replace references to "encryption review requests" with "encryption registration." The term "encryption review request" is removed and not replaced by "encryption registration" in section 748.1(d)(1)(i) because submitting only one encryption registration per year is not a valid reason for eligibility to submit manual applications to BIS. SNAP–R issues a specific Encryption Registration Number (ERN) for each encryption registration electronically submitted to BIS via SNAP–R, which is used to authorize exports and reexports under sections 740.17(b) and 742.15(b).

Section 748.3 is amended by revising the title and paragraphs (a) and (d) to coincide with the removal of review requests, addition of encryption registrations, and the narrowing of submission requirements.

This rule revises the paragraph entitled "Block 5: Type of Application" in Supplement No. 1 to part 748 by replacing the term "encryption review" with "encryption registration" in two cases. This rule also replaces a reference to "classification request" with "encryption registration" in one case, because encryption registrations will have a newly created screen in SNAP–R.

This rule also revises section 748.8(r) and paragraph (r) in Supplement No. 2 to part 748 to harmonize with the removal of review requests and new submission procedures for encryption registration and self-classification reports.

BIS has created a new SNAP–R screen for encryption registrations. The instructions for submitting an encryption registration is found in paragraph (r)(1) of Supplement No. 2 to part 748. In block 5 (Type of Application) of SNAP–R, selecting "encryption registration" will result in the appearance of the new encryption registration screen. On that screen blocks 1–5, 14, 15, 24, and 25 are to be completed, and a PDF must be attached that provides answers to Supplement No. 5 to part 742.

For classification requests for License Exception ENC or mass market encryption under section 742.15, BIS has added a new check box for block 9 (Special Purpose) on the classification request screen of SNAP–R. The new check box states "Check here if you are submitting information about encryption required by 740.17 or 742.15 of the EAR." When that box is checked, a drop down menu will display the following choices: License Exception ENC, Mass Market Encryption, or Encryption Other. This rule implements new procedures in paragraph (r)(2) of Supplement No. 2 to part 748 to address these changes in SNAP–R, as well as instructions about documents submitted with a classification request. In addition, there is an instruction to insert your most recent Encryption Registration Number (ERN) in Block 24 (Additional Information) of the encryption classification request.

Part 772—Definition of Terms

This rule removes the term "ancillary cryptography," the definition, nota bene, and related footnote from section 772.1 of the EAR, because the newly added Note 4 to Category 5, Part 2 removes the need for this definition.

This rule also removes the definition for "personalized smart card" from section 772.1 because Note (a) of Export Control Classification Number (ECCN) 5A002, which used the term "personalized smart card," has been replaced by new text that does not use the term.

Supplement No. 1 to Part 774—Commerce Control List

Note 4 to Category 5, Part 2

This rule adds a new Note 4 to Category 5, Part 2 to exclude certain items incorporating or using "cryptography" from control under Category 5, Part 2. Specifically, the note excludes an item that incorporates or uses "cryptography" from Category 5, Part 2 control if the item's primary function or set of functions is not "information security," computing, communications, storing information, or networking, and if the cryptographic functionality is limited to supporting such primary function or set of functions. The primary function is the obvious, or main, purpose of the item. It is the function which is not there to support other functions. The "communications" and "information storage" primary function does not include items that support entertainment, mass commercial broadcasts, digital rights management or medical records management.

The items excluded from Category 5, Part 2 controls by Note 4 have been determined not to be of national security concern due to their encryption functionality. Items that are covered by Note 4 should be evaluated under other categories of the CCL (Supplement No. 1 to part 774 of the EAR) to determine if any other controls apply. For example, a camera system that incorporates encryption would be evaluated under Category 6 of the CCL; a chemical analysis software program that incorporates encryption would be evaluated under Category 2. If the result of this evaluation is that the item is not controlled under another category of the CCL (*e.g.,* a refrigerator), the item is designated as EAR99.

Note 4 to Category 5, Part 2 covers certain items that were previously excluded from control under ECCN 5A002 by one or more paragraphs of the exclusion Note to ECCN 5A002. Specifically, the scope of Note 4 includes items previously covered in paragraphs (b), (c) and (h) of the Note to ECCN 5A002. The exclusion Note to ECCN 5A002 provides that the items listed in paragraph (a) through (i) to the Note are controlled under ECCN 5A992. With the addition of Note 4 to Category 5, Part 2 upon the effective date of this rule, the items previously covered in paragraphs (b), (c) and (h) of the exclusion Note to ECCN 5A002 are no longer controlled under Category 5, Part 2 (by virtue of the new Note 4, irrespective of the Note to ECCN 5A002), and are therefore classified under another category of the CCL or designated as EAR99.

The scope of Note 4 is coextensive with the scope of the "ancillary cryptography" provisions that were added to the EAR on October 3, 2008. Under that amendment, commodities and software that perform "ancillary cryptography" remained controlled under Category 5, Part 2, but were exempted from review and reporting requirements under License Exception ENC (§ 740.17 of the EAR) and the mass market provisions of section 742.15 of the EAR.

Items that were self-classified or classified by BIS as "ancillary cryptography" items after October 3, 2008 are, upon the effective date of this rule, no longer classified under Category 5, Part 2. In addition, items that were self-classified or classified by BIS under ECCN 5A992 or 5D992 based on former paragraphs (b), (c) or (h) of the note to ECCN 5A002 are, upon the effective date of this rule, no longer classified under Category 5, Part 2. Exporters should re-classify such items under other categories of the CCL or designate as EAR99, as appropriate.

Examples of items that are excluded from Category 5, Part 2 by Note 4 include, but are not limited to, the following: Piracy and theft prevention for software or music; games and gaming; household utilities and appliances; printing, reproduction, imaging and video recording or playback (not videoconferencing); business process modeling and

automation (*e.g.,* supply chain management, inventory, scheduling and delivery); industrial, manufacturing or mechanical systems (*e.g.,* robotics, heavy equipment, facilities systems such as fire alarm, HVAC); automotive, aviation, and other transportation systems; LCD TV, Blu-ray/DVD, video on demand (VoD), cinema, digital video recorders (DVRs)/personal video recorders (PVRs); on-line media guides, commercial content integrity and protection, HDMI and other component interfaces; medical/clinical—including diagnostic applications, patient scheduling, and medical data records confidentiality; academic instruction and testing/on-line training—tools and software; applied geosciences—mining/drilling, atmospheric sampling/weather monitoring, mapping/surveying, dams/hydrology; scientific visualization/simulation/co-simulation (excluding such tools for computing, networking, or cryptanalysis); data synthesis tools for social, economic, and political sciences (*e.g.,* economic, population, global climate change, public opinion polling, forecasting and modeling); software and hardware design IP protection; and computer aided design (CAD) software and other drafting tools.

ECCN 5A002

This rule revises the Related Controls paragraph in ECCN 5A002 to reflect the deletion of paragraphs from the Note in the beginning of the Items paragraph of 5A002. The Note at the beginning of the Items paragraph of 5A002 is amended by: Replacing paragraph (a) to remove from 5A002 control certain smart card readers/writers, and to add definitions for 'personal data' and 'readers/writers;' removing paragraphs (b), (c) and (h) because they are now covered by newly added Note 4 to Category 5, Part 2; deleting "other specially designed" before components, and adding "specially designed for information security" to the end of 5A002.a to clarify the text; and deleting a parenthetical reference to "GPS or GLONASS" in the nota bene, following 5A002.a, to clarify the text.

Supplement No. 3 to Part 774—Statements of Understanding

Because the length of Supplement No. 3 to part 774 is expanding, the need for paragraph designations is necessary. Therefore, this rule adds paragraph designations for each of the statements of understanding. This rule also adds a new statement of understanding that relates to Note 4 of Category 5, Part 2. The new statement of understanding is simply a copy of the text that previously appeared in note (h) of ECCN 5A002, which is removed by this rule, that provides the public a reference of the specific details about portable or mobile radiotelephones and similar client wireless devices that are now encompassed under the new Note 4 of Category 5, Part 2.

Grandfathering

For encryption commodities, software and components described in, or otherwise meeting the specifications of sections 740.17(b) and 742.15(b), effective June 25, 2010, such items reviewed and classified by BIS prior to June 25, 2010 are authorized for export and reexport under the applicable provisions of sections 740.17(b) and 742.15(b), as amended upon publication of this rule, using the CCATS previously issued by BIS, without any encryption registration (*i.e.,* the information described in Supplement No. 5 to this part), new classification by BIS, self-classification reporting (*i.e.,* the information described in Supplement No. 8 to part 742), or semi-annual sales reporting required under section 740.17(e) provided the cryptographic functionality of the item has not changed. These grandfathering provisions do not apply to particular commodities and software previously made eligible for License Exception ENC under former paragraph (b)(3) that are now listed in paragraph (b)(2) and therefore require a license to certain "government end-users" outside the countries listed in Supplement No. 3 to part 740. These grandfathering provisions also do not apply if the encryption functionality has changed since the encryption product was last classified by BIS, as specified in 740.17(d)(1)(iii) and 742.15(b)(7)(i)(C).

Export Administration Act

Since August 21, 2001, the Export Administration Act has been in lapse. However, the President, through Executive Order 13222 of August 17, 2001 (3 CFR 2001 Comp. 783 (2002)), which has been extended by successive Presidential Notices, the most recent being that of August 13, 2009 (74 FR 41325 (August 14, 2009)), has continued the Regulations in effect under the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*).

Rulemaking Requirements

1. This rule has been determined to be significant for purposes of Executive Order 12866.

2. Notwithstanding any other provision of law, no person is required to respond to nor be subject to a penalty for failure to comply with a collection of information, subject to the requirements of the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*) (PRA), unless that collection of information displays a currently valid Office of Management and Budget (OMB) Control Number. This rule involves a collection of information that has been approved by the OMB under control number 0694–0088, "Multi-Purpose Application," which carries a burden hour estimate of 58 minutes to prepare and submit form BIS–748. Miscellaneous and recordkeeping activities account for 12 minutes per submission. This rule amends a collection that has been approved by the Office of Management and Budget under control number 0694–0104, "Commercial Encryption Items Under the Jurisdiction of the Department of Commerce" by adding two new submissions: "Encryption registration" and "self-classification report." Although the changes in this rule increase the number of collections under 0694–0104, the burden hour estimate is decreased from 7 hours to 1.9 hours per submission (manual or electronic). Send comments regarding these burden estimates or any other aspect of these collections of information, including suggestions for reducing the burden, to Jasmeet Seehra, OMB Desk Officer, by e-mail at *Jasmeet_K._Seehra@omb.eop.gov* or by fax to (202) 395–7285; and to the Regulatory Policy Division, Bureau of Industry and Security, Department of Commerce, 14th and Pennsylvania Ave., NW., Room 2705, Washington, DC 20230.

3. This rule does not contain policies with Federalism implications as that term is defined under Executive Order 13132.

4. Pursuant to 5 U.S.C. 553(a)(1), the provisions of this rule amending the Commerce Control List (Note 4 to Category 5 part 2), the Statements of Understanding (Supplement No. 3 to Part 774), and the definitions provisions (Part 772) of the EAR are exempt from the provision of the Administrative Procedure Act (5 U.S.C. 553) (APA) requiring notice and an opportunity for public comment because this regulation involves a military and foreign affairs function of the United States. Immediate implementation of these amendments fulfills the United States' international obligation to the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual Use Goods and Technologies (Wassenaar Arrangement or WA). The Wassenaar Arrangement contributes to international security and regional stability by promoting greater responsibility in transfers of

conventional arms and dual use goods and technologies, thus preventing destabilizing accumulations of such items. The Wassenaar Arrangement consists of 40 member countries that act on a consensus basis and this change was approved at the 2009 plenary session of the WA. Since the United States is a significant exporter of encryption items, implementation of this provision is necessary for the WA to achieve its purpose. Any delay in implementation will create a disruption in the movement of affected items globally because of the disharmony between export control regulations, resulting in tension between member countries. Export controls work best when all countries implement the same export controls in a timely manner. Any delay in implementation would injure the credibility of the United States in this and other multilateral regimes. If notice and comment precedes, rather than follows, the promulgation of this rule, the delays associated with soliciting comments will result in the inability of the United States to fulfill its commitment to the WA.

For the other provisions of this rule, the Department has determined that there is good cause under 5 U.S.C. 553(b)(B) to waive the provisions of the Administrative Procedure Act requiring notice and the opportunity for public comment when doing so is contrary to the public interest. This rule expedites the process for eligibility for use of a license exception for the export of encryption items, while maintaining the effectiveness of authorizations previously issued. If this rule is delayed to allow for prior notice and opportunity for public comment, U.S. industry would continue to be subject to a more burdensome licensing process than necessary for the export of encryption items. Because this rule will ensure the competitiveness of U.S. industry, delaying the effectiveness of this rule is contrary to the public interest.

For the reasons listed above, good cause exists to waive the 30-day delay in effectiveness otherwise required by the APA. Further, no other law requires that a notice of proposed rulemaking and an opportunity for public comment be given for this interim final rule. Accordingly, no regulatory flexibility analysis is required and none has been prepared. Although notice and opportunity for comment are not required, BIS is issuing this rule in interim final form and is seeking public comments on these revisions.

The period for submission of comments will close August 24, 2010. BIS will consider all comments received before the close of the comment period in developing a final rule. Comments received after the end of the comment period will be considered if possible, but their consideration cannot be assured. BIS will not accept public comments accompanied by a request that a part or all of the material be treated confidentially because of its business proprietary nature or for any other reason. BIS will return such comments and materials to the persons submitting the comments and will not consider them in the development of the final rule. All public comments on this interim rule must be in writing (including fax or e-mail) and will be a matter of public record, available for public inspection and copying. The Office of Administration, Bureau of Industry and Security, U.S. Department of Commerce, displays these public comments on BIS's Freedom of Information Act (FOIA) Web site at *http://www.bis.doc.gov/foia.* This office does not maintain a separate public inspection facility. If you have technical difficulties accessing this Web site, please call BIS's Office of Administration at (202) 482–0953 for assistance.

List of Subjects

15 CFR Part 730

Administrative practice and procedure, Advisory committees, Exports, Reporting and recordkeeping requirements, Strategic and critical materials.

15 CFR Part 734

Administrative practice and procedure, Exports, Inventions and patents, Research Science and technology.

15 CFR Parts 738 and 772

Exports.

15 CFR Parts 740 and 748

Administrative practice and procedure, Exports, Reporting and recordkeeping requirements.

15 CFR Part 742

Exports, Terrorism.

15 CFR Part 774

Exports, Reporting and recordkeeping requirements.

■ Accordingly, Parts 730, 734, 738, 740, 742, 748, 772 and 774 of the EAR (15 CFR Parts 730–774) are amended as follows:

PART 730—[AMENDED]

■ 1. The authority citation for part 730 continues to read as follows:

Authority: 50 U.S.C. app. 2401 *et seq.;* 50 U.S.C. 1701 *et seq.;* 10 U.S.C. 7420; 10 U.S.C. 7430(e); 22 U.S.C. 287c; 22 U.S.C. 2151 note; 22 U.S.C. 3201 *et seq.;* 22 U.S.C. 6004; 30 U.S.C. 185(s), 185(u); 42 U.S.C. 2139a; 42 U.S.C. 6212; 43 U.S.C. 1354; 15 U.S.C. 1824a; 50 U.S.C. app. 5; 22 U.S.C. 7201 *et seq.;* 22 U.S.C. 7210; E.O. 11912, 41 FR 15825, 3 CFR, 1976 Comp., p. 114; E.O. 12002, 42 FR 35623, 3 CFR, 1977 Comp., p. 133; E.O. 12058, 43 FR 20947, 3 CFR, 1978 Comp., p. 179; E.O. 12214, 45 FR 29783, 3 CFR, 1980 Comp., p. 256; E.O. 12851, 58 FR 33181, 3 CFR, 1993 Comp., p. 608; E.O. 12854, 58 FR 36587, 3 CFR, 1993 Comp., p. 179; E.O. 12918, 59 FR 28205, 3 CFR, 1994 Comp., p. 899; E.O. 12938, 59 FR 59099, 3 CFR, 1994 Comp., p. 950; E.O. 12947, 60 FR 5079, 3 CFR, 1995 Comp., p. 356; E.O. 12981, 60 FR 62981, 3 CFR, 1995 Comp., p. 419; E.O. 13020, 61 FR 54079, 3 CFR, 1996 Comp., p. 219; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; E.O. 13099, 63 FR 45167, 3 CFR, 1998 Comp., p. 208; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783; E.O. 13224, 66 FR 49079, 3 CFR, 2001 Comp., p. 786; E.O. 13338, 69 FR 26751, May 13, 2004; Notice of August 13, 2009, 74 FR 41325 (August 14, 2009); Notice of November 6, 2009, 74 FR 58187 (November 10, 2009).

■ 2. Supplement No. 1 is amended by removing the title for collection number 0694–0104 and adding in its place "Commercial Encryption Items under Commerce Jurisdiction."

PART 734—[AMENDED]

■ 3. The authority citation for part 734 continues to read as follows:

Authority: 50 U.S.C. app. 2401 *et seq.;* 50 U.S.C. 1701 *et seq.;* E.O. 12938, 59 FR 59099, 3 CFR, 1994 Comp., p. 950; E.O. 13020, 61 FR 54079, 3 CFR, 1996 Comp., p. 219; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783; Notice of August 13, 2009, 74 FR 41325 (August 14, 2009); Notice of November 6, 2009, 74 FR 58187 (November 10, 2009).

■ 4. Section 734.4 is amended by revising paragraph (b)(1)(ii), (b)(1)(iii), and (b)(1)(iv), and adding a new paragraph (b)(1)(v), to read as follows:

§ 734.4 De minimis U.S. content.

* * * * *

(b) * * *

(1) * * *

(ii) Authorized for License Exception ENC by BIS after classification pursuant to § 740.17(b)(3) of the EAR;

(iii) Authorized for License Exception ENC by BIS after classification pursuant to § 740.17(b)(2) of the EAR, and the foreign made product will not be sent to any destination in Country Group E:1 in Supplement No. 1 to part 740 of the EAR;

(iv) Authorized for License Exception ENC pursuant to § 740.17(b)(4) of the EAR; or

(v) Authorized for License Exception ENC after submission of an encryption registration pursuant to § 740.17(b)(1) of the EAR.

* * * * *

PART 738—[AMENDED]

■ 5. The authority citation for part 738 continues to read as follows:

Authority: 50 U.S.C. app. 2401 *et seq.;* 50 U.S.C. 1701 *et seq.;* 10 U.S.C. 7420; 10 U.S.C. 7430(e); 22 U.S.C. 287c; 22 U.S.C. 3201 *et seq.;* 22 U.S.C. 6004; 30 U.S.C. 185(s), 185(u); 42 U.S.C. 2139a; 42 U.S.C. 6212; 43 U.S.C. 1354; 15 U.S.C. 1824a; 50 U.S.C. app. 5; 22 U.S.C. 7201 *et seq.;* 22 U.S.C. 7210; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783; Notice of August 13, 2009, 74 FR 41325 (August 14, 2009).

■ 6. Section 738.4 is amended by revising the third and fourth sentences in paragraph (a)(2)(ii)(B) to read as follows:

§ 738.4 Determining whether a license is required.

(a) * * *

(2) * * *

(ii) * * *

(B) * * * For example, any applicable encryption registration and classification requirements described in § 742.15(b) of the EAR must be met for certain mass market encryption items to effect your shipment using the symbol "NLR." Proceed to parts 758 and 762 of the EAR for information on export clearance procedures and recordkeeping requirements. * * *

* * * * *

PART 740—[AMENDED]

■ 7. The authority citation for part 740 continues to read as follows:

Authority: 50 U.S.C. app. 2401 *et seq.;* 50 U.S.C. 1701 *et seq.;* 22 U.S.C. 7201 *et seq.;* E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783; Notice of August 13, 2009, 74 FR 41325 (August 14, 2009).

■ 8. Section 740.17 is revised to read as follows:

§ 740.17 Encryption commodities, software and technology (ENC).

License Exception ENC authorizes export and reexport of systems, equipment, commodities and components therefor that are classified under ECCNs 5A002.a.1, a.2, a.5, a.6 or a.9, systems, equipment and components therefor classified under ECCN 5B002, and equivalent or related software and technology classified under ECCNs 5D002 or 5E002. This License Exception ENC does not authorize export or reexport to, or provision of any service in any country listed in Country Group E:1 in Supplement No. 1 to part 740 of the EAR, or release of source code or technology to any national of a country listed in Country Group E:1. Reexports and transfers under License Exception ENC are subject to the criteria set forth in paragraph (c) of this section. Paragraphs (b) and (d) of this section set forth information about encryption registrations and classifications required by this section. Paragraph (e) sets forth reporting required by this section. For items exported under paragraphs (b)(1), (b)(3)(i), (b)(3)(ii) or (b)(3)(iv) of this section and therefore excluded from paragraph (e) reporting requirements, exporters are reminded of the recordkeeping requirements in part 762 of the EAR and that they may be required to make such records available upon request. All classification requests, registrations, and reports submitted to BIS pursuant to this section for encryption items will be reviewed by the ENC Encryption Request Coordinator, Ft. Meade, MD.

(a) *No classification request, registration or reporting required.*

(1) *Internal "development" or "production" of new products.* License Exception ENC authorizes exports and reexports of items described in paragraph (a)(1)(i) of this section, to end-users described in paragraph (a)(1)(ii) of this section, for the intended end-use described in paragraph (a)(1)(iii) of this section without submission of encryption registration, classification request, self-classification report or sales report to BIS.

(i) *Eligible items.* Eligible items are those classified under ECCNs 5A002.a.1, .a.2, .a.5, .a.6, or .a.9, ECCN 5B002, and equivalent or related software and technology classified under ECCNs 5D002 or 5E002.

(ii) *Eligible End-users.* Eligible end-users are "private sector end-users" wherever located that are headquartered in a country listed in Supplement No. 3 of this part.

Note to paragraph (a)(1)(ii): A "private sector end-user" is:

(1) An individual who is not acting on behalf of any foreign government; or

(2) A commercial firm (including its subsidiary and parent firms, and other subsidiaries of the same parent) that is not wholly owned by, or otherwise controlled by or acting on behalf of, any foreign government.

(iii) *Eligible End-use.* The eligible end-use is internal "development" or "production" of new products by those end-users.

Note to paragraph (a)(1)(iii): All items produced or developed with items exported or reexported under this paragraph (a)(1) are subject to the EAR. These items may require the submission of a classification request or encryption registration before sale, reexport or transfer, unless otherwise authorized by license or license exception.

(2) *Exports and reexports to "U.S. Subsidiaries."* License Exception ENC authorizes export and reexport of systems, equipment, commodities and components therefor classified under ECCNs 5A002.a.1, .a.2, .a.5, .a.6, or .a.9, systems, equipment, and components therefor classified under ECCN 5B002, and equivalent or related software and technology classified under ECCNs 5D002 or 5E002, to any "U.S. subsidiary," wherever located without submission of an encryption registration, classification request, self-classification report or sales report to BIS. License Exception ENC also authorizes export or reexport of such items by a U.S. company and its subsidiaries to foreign nationals who are employees, contractors or interns of a U.S. company or its subsidiaries if the items are for internal company use, including the "development" or "production" of new products, without prior review by the U.S. Government.

Note to paragraph (a)(2): All items produced or developed with items exported or reexported under this paragraph (a)(2) are subject to the EAR. These items may require the submission of a classification request or encryption registration before sale, reexport or transfer to non-"U.S. subsidiaries," unless otherwise authorized by license or license exception.

(b) *Encryption registration required, with classification request or self-classification report.* Exports and reexports authorized under paragraphs (b)(1), (b)(2) and (b)(3) of License Exception ENC require submission of an encryption registration in accordance with paragraph (d) of this section and the specific instructions of paragraph (r)(1) of Supplement No. 2 to part 748 of the EAR. In addition: for paragraph (b)(1) of this section a self-classification report in accordance with § 742.15(c) of the EAR is also required from specified exporters and reexporters; for paragraphs (b)(2) and (b)(3) of this section, a thirty-day (30-day) classification request is required in accordance with paragraph (d) of this section. *See* paragraph (f) of this section for grandfathering provisions applicable to certain encryption items reviewed and classified by BIS under this license exception prior to June 25, 2010. Only License Exception ENC authorizations under this paragraph (b) to a company that has fulfilled the requirements of encryption registration (such as the producer of the item) authorize the

export and reexport of the company's encryption items by all persons, wherever located, under this license exception. When an exporter or reexporter relies on the producer's self-classification (pursuant to the producer's encryption registration) or CCATS for an encryption item eligible for export or reexport under License Exception ENC under paragraph (b)(1), (b)(2), or (b)(3) of this section, it is not required to submit an encryption registration, classification request or self-classification report. Exporters are still required to comply with semi-annual sales reporting requirements under paragraph (e) of this section, even if relying on a CCATS issued to a producer for specified encryption items described in paragraphs (b)(2) and (b)(3)(iii) of this section.

(1) *Immediate authorization.* Once an encryption registration is submitted to BIS in accordance with paragraph (d) of this section and an Encryption Registration Number (ERN) has been issued, this paragraph (b)(1) authorizes the exports or reexports of the associated commodities classified under ECCNs 5A002.a.1, .a.2, .a.5, .a.6, or .a.9, or ECCN 5B002, and equivalent or related software classified under ECCN 5D002, except any such commodities, software or components described in (b)(2) or (b)(3) of this section, subject to submission of a self-classification report in accordance with § 742.15(c) of the EAR.

(2) *Classification request required.* Thirty (30) days after the submission of a classification request with BIS in accordance with paragraph (d) of this section and subject to the reporting requirements in paragraph (e) of this section, this paragraph under License Exception ENC authorizes certain exports or reexports of the items submitted for classification, as further described in paragraphs (b)(2)(i), (b)(2)(ii) and (b)(2)(iv)(B) of this section.

Note to introductory text of paragraph (b)(2): Immediately after the classification request is submitted to BIS in accordance with paragraph (d) of this section and subject to the reporting requirements in paragraph (e) of this section, this paragraph also authorizes exports or reexports of:

1. All submitted encryption items described in this paragraph (b)(2), except "cryptanalytic items," to any end-user located or headquartered in a country listed in Supplement No. 3 to this part;

2. Encryption source code as described in paragraph (b)(2)(i)(B) to non-"government end-users" in any country;

3. "Cryptanalytic items" to non-"government end-users", only, located or headquartered in a country listed in Supplement No. 3 to this part; and

4. Items described in paragraphs (b)(2)(iii) and (b)(2)(iv)(A) of this section, to specified destinations and end-users.

(i) *Cryptographic commodities, software and components.* The following items to non-"government end-users" located or headquartered in a country not listed in Supplement No. 3 to this part:

(A) Network infrastructure software and commodities and components thereof (including commodities and software necessary to activate or enable cryptographic functionality in network infrastructure products) providing secure Wide Area Network (WAN), Metropolitan Area Network (MAN), Virtual Private Network (VPN), satellite, digital packet telephony/media (voice, video, data) over Internet protocol, cellular or trunked communications meeting any of the following with key lengths exceeding 80-bits for symmetric algorithms:

(*1*) Aggregate encrypted WAN, MAN, VPN or backhaul throughput (including communications through wireless network elements such as gateways, mobile switches, and controllers) greater than 90 Mbps;

(*2*) Wire (line), cable or fiber-optic WAN, MAN or VPN single-channel input data rate exceeding 154 Mbps;

(*3*) Transmission over satellite at data rates exceeding 10 Mbps;

(*4*) Media (voice/video/data) encryption or centralized key management supporting more than 250 concurrent encrypted data channels, or encrypted signaling to more than 1,000 endpoints, for digital packet telephony/media (voice/video/data) over Internet protocol communications; or

(*5*) Air-interface coverage (*e.g.,* through base stations, access points to mesh networks, and bridges) exceeding 1,000 meters, where any of the following applies:

(*i*) Maximum transmission data rates exceeding 10 Mbps (at operating ranges beyond 1,000 meters);

(*ii*) Maximum number of concurrent full-duplex voice channels exceeding 30; or

(*iii*) Substantial support is required for installation or use;

(B) Encryption source code that would not be eligible for export or reexport under License Exception TSU because it is not publicly available as that term is used in § 740.13(e)(1) of the EAR;

(C) Encryption software, commodities and components therefor, that have any of the following:

(*1*) Been designed, modified, adapted or customized for "government end-user(s)";

(*2*) Cryptographic functionality that has been modified or customized to customer specification; or

(*3*) Cryptographic functionality or "encryption component" (except encryption software that would be considered publicly available, as that term is used in § 740.13(e)(1) of the EAR) that is user-accessible and can be easily changed by the user;

(D) Encryption commodities and software that provide functions necessary for quantum cryptography, as defined in ECCN 5A002 of the Commerce Control List;

(E) Encryption commodities and software that have been modified or customized for computers classified under ECCN 4A003;

(F) Encryption commodities and software that provide penetration capabilities that are capable of attacking, denying, disrupting or otherwise impairing the use of cyber infrastructure or networks;

(G) Public safety/first responder radio (*e.g.,* implementing Terrestrial Trunked Radio (TETRA) and/or Association of Public-Safety Communications Officials International (APCO) Project 25 (P25) standards);

(ii) *Cryptanalytic commodities and software.* Commodities and software classified as "cryptanalytic items" to non-"government end-users" located or headquartered in countries not listed in Supplement No. 3 to this part;

(iii) "*Open cryptographic interface*" *items.* Items that provide an "open cryptographic interface", to any end-user located or headquartered in a country listed in Supplement No. 3 to this part.

(iv) *Specific encryption technology.* Specific encryption technology as follows:

(A) *Technology for* "*non-standard cryptography.*" Encryption technology classified under ECCN 5E002 for "non-standard cryptography," to any end-user located or headquartered in a country listed in Supplement No. 3 to this part;

(B) *Other technology.* Encryption technology classified under ECCN 5E002 except technology for "cryptanalytic items," "non-standard cryptography" or any "open cryptographic interface," to any non-"government end-user" located in a country not listed in Country Group D:1 or E:1 of Supplement No. 1 to part 740 of the EAR.

Note to paragraph (b)(2): Commodities, software, and components that allow the end-user to activate or enable cryptographic functionality in encryption products which would otherwise remain disabled, are controlled according to the functionality of the activated encryption product.

(3) *Classification request required for specified commodities, software and components.* Thirty (30) days after a classification request is submitted to BIS in accordance with paragraph (d) of this section and subject to the reporting requirements in paragraph (e) of this section, this paragraph authorizes exports or reexports of the items submitted for classification, as further described in this paragraph (b)(3), to any end-user, provided the item does not perform the functions, or otherwise meet the specifications, of any item described in paragraph (b)(2) of this section.

Note to introductory text of paragraph (b)(3): Immediately after the classification request is submitted to BIS in accordance with paragraph (d) of this section and subject to the reporting requirements in paragraph (e) of this section, this paragraph also authorizes exports or reexports of the items described in this paragraph (b)(3) to any end-user located or headquartered in a country listed in Supplement No. 3 to this part.

(i) Specified components classified under ECCN 5A002.a.1, .a.5 or .a.6 and equivalent or related software classified under ECCN 5D002 not described by paragraph (b)(2) of this section, as follows:

(A) Chips, chipsets, electronic assemblies and field programmable logic devices;

(B) Cryptographic libraries, modules, development kits and toolkits, including for operating systems and cryptographic service providers (CSPs);

(C) Application-specific hardware or software development kits implementing cryptography.

(ii) Encryption commodities, software and components not described by paragraph (b)(2) of this section, that provide or perform "non-standard cryptography" as defined in part 772 of the EAR.

(iii) Encryption commodities and software not described by paragraph (b)(2) of this section, that provide or perform vulnerability analysis, network forensics, or computer forensics functions characterized by any of the following:

(A) Automated network analysis, visualization, or packet inspection for profiling network flow, network user or client behavior, or network structure/topology and adapting in real-time to the operating environment; or

(B) Investigation of data leakage, network breaches, and other malicious intrusion activities through triage of captured digital forensic data for law enforcement purposes or in a similarly rigorous evidentiary manner.

(iv) *Cryptographic enabling commodities and software.* Commodities and software and components that activate or enable cryptographic functionality in encryption products which would otherwise remain disabled, where the product or cryptographic functionality is not otherwise described in paragraphs (b)(2) or (b)(3)(i) of this section.

(4) *Exclusions from classification request, encryption registration and self-classification reporting requirements.* License Exception ENC authorizes the export and reexport of the commodities and software described in this paragraph (b)(4) without the submission of a classification request, encryption registration or self-classification report to BIS, except that paragraph (b)(4)(ii) of this section does not authorize exports from the United States of foreign products developed with or incorporating U.S.-origin encryption source code, components, or toolkits.

(i) *Short-range wireless encryption functions.* Commodities and software that are not otherwise controlled in Category 5, but are nonetheless classified under ECCN 5A002, 5B002 or 5D002 only because they incorporate components or software that provide short-range wireless encryption functions (*e.g.,* with a nominal operating range not exceeding 100 meters according to the manufacturer's specifications, designed to comply with the Institute of Electrical and Electronic Engineers (IEEE) 802.11 wireless LAN standard or the IEEE 802.15.1 standard).

Note to paragraph (b)(4)(i): An example of what this paragraph authorizes for export without classification, registration or self-classification reporting is a laptop computer that without encryption would be classified under ECCN 4A994, and the Category 5, Part 2-controlled components of the laptop only implement short-range wireless encryption functionality. On the other hand, this paragraph (b)(4)(i) does not apply to any commodities or software that would still be classified under an ECCN in Category 5 even if the short-range wireless encryption functionality were removed. For example, certain access points, gateways and bridges are classified under ECCN 5A991 without encryption functionality, and components for mobile communication equipment are classified under ECCN 5A991.g without encryption functionality. Such items, when implementing cryptographic functionality controlled by Category 5, Part 2 are not excluded from encryption classification, registration or self-classification reporting by this paragraph.

(ii) *Foreign products developed with or incorporating U.S.-origin encryption source code, components, or toolkits.* Foreign products developed with or incorporating U.S.-origin encryption source code, components or toolkits that are subject to the EAR, provided that the U.S.-origin encryption items have previously been classified or registered and authorized by BIS and the cryptographic functionality has not been changed. Such products include foreign-developed products that are designed to operate with U.S. products through a cryptographic interface.

(c) *Reexport and transfer.* U.S. or foreign distributors, resellers or other entities who are not original manufacturers of encryption commodities and software are permitted to use License Exception ENC only in instances where the export or reexport meets the applicable terms and conditions of this section. Transfers of encryption items listed in paragraph (b)(2) of this section to "government end-users," or for government end-uses, within the same country are prohibited, unless otherwise authorized by license or license exception.

(d) *Encryption registration and classification request procedures.*

(1) *Submission requirements and instructions.* To submit an encryption registration or classification request to BIS, you must submit an application to BIS in accordance with the procedures described in §§ 748.1 and 748.3 of the EAR and the instructions in paragraph (r) of Supplement No. 2 to part 748 "Unique Application and Submission Requirements," along with other required information as follows:

(i) *Encryption registrations in support of encryption classification requests and self-classification reports.* You must submit the applicable information as described in Supplement No. 5 to part 742 of the EAR and follow the specific instructions of paragraph (r)(1) of Supplement No. 2 to part 748 of the EAR, if any of the following apply:

(A) This is your first time submitting an encryption classification request under paragraphs (b)(2) or (b)(3) of this section since August 24, 2010;

(B) You are making an encryption item eligible for export and reexport (including as defined for encryption software in § 734.2(b)(9) of the EAR) under paragraph (b)(1) of this section for the first time since August 24, 2010; or

(C) If you have not otherwise provided BIS the information described in Supplement No. 5 to part 742 during the current calendar year and your answers to the questions in Supplement No. 5 to part 742 have changed since the last time you provided answers to the questions.

(ii) *Technical information submission requirements.* In addition to the encryption registration requirements of paragraph (d)(1)(i) of this section, for all submissions of encryption classification requests for items described under

paragraph (b)(2) or (b)(3) of this section, you must also provide BIS the applicable information described in paragraphs (a) through (d) of Supplement No. 6 to part 742 of the EAR (Technical Questionnaire for Encryption Items). For items authorized after submission of an encryption registration under paragraph (b)(1) of this section, you may be required to provide BIS this Supplement No. 6 to part 742 information on an as-needed basis, upon request by BIS.

(iii) *Changes in encryption functionality following a previous classification.* A new product encryption classification request (under paragraphs (b)(2) or (b)(3) of this section) or self-classification report (under paragraph (b)(1) of this section) is required if a change is made to the cryptographic functionality (*e.g.,* algorithms) or other technical characteristics affecting License Exception ENC eligibility (*e.g.,* encrypted throughput) of the originally classified product. However, a new product classification request or self-classification report is not required when a change involves: The subsequent bundling, patches, upgrades or releases of a product; name changes; or changes to a previously reviewed encryption product where the change is limited to updates of encryption software components where the product is otherwise unchanged.

(2) *Action by BIS.*

(i) *Encryption registrations for paragraph (b) of this section.* Upon submission to BIS of an encryption registration in accordance with paragraph (d)(1) of this section and acceptance of the application by SNAP–R, BIS will issue the Encryption Registration Number (ERN) via SNAP–R, which will constitute authorization for exports and reexports of eligible items under paragraph (b)(1) of this license exception.

(ii) *For items requiring classification by BIS under paragraphs (b)(2) and (b)(3) of this section.*

(A) For classifications that require a thirty (30) day waiting period, if BIS has not, within thirty-days (30-days) from registration in SNAP–R of your complete classification request, informed you that your item is not authorized for License Exception ENC, you may export or reexport under the applicable provisions of License Exception ENC.

(B) Upon completion of its classification, BIS will issue a Commodity Classification Automated Tracking System (CCATS) to you.

(C) *Hold Without Action (HWA) for classification requests.* BIS may hold your classification request without action if necessary to obtain additional information or for any other reason necessary to ensure an accurate classification. Time on such "hold without action" status shall not be counted towards fulfilling the thirty-day (30-day) processing period specified in this paragraph.

(iii) BIS may require you to supply additional relevant technical information about your encryption item(s) or information that pertains to their eligibility for License Exception ENC at any time, before or after the expiration of the thirty-day (30-day) processing period specified in this paragraph and in paragraphs (b)(2) and (b)(3) of this section, or after any registrations as required in paragraph (b)(1) of this section. If you do not supply such information within 14 days after receiving a request for it from BIS, BIS may return your classification request(s) without action or otherwise suspend or revoke your eligibility to use License Exception ENC for that item(s). At your request, BIS may grant you up to an additional 14 days to provide the requested information. Any request for such an additional number of days must be made prior to the date by which the information was otherwise due to be provided to BIS, and may be approved if BIS concludes that additional time is necessary.

(e) *Reporting requirements.*

(1) *Semi-annual reporting requirement.* Semi-annual reporting is required for exports to all destinations other than Canada, and for reexports from Canada for items described under paragraphs (b)(2) and (b)(3)(iii) of this section. Certain encryption items and transactions are excluded from this reporting requirement, *see* paragraph (e)(1)(iii) of this section. For information about what must be included in the report and submission requirements, *see* paragraphs (e)(1)(i) and (e)(1)(ii) of this section respectively.

(i) *Information required.* Exporters must include for each item, the Commodity Classification Automated Tracking System (CCATS) number and the name of the item(s) exported (or reexported from Canada), and the following information in their reports:

(A) *Distributors or resellers.* For items exported (or reexported from Canada) to a distributor or other reseller, including subsidiaries of U.S. firms, the name and address of the distributor or reseller, the item and the quantity exported or reexported and, if collected by the exporter as part of the distribution process, the end-user's name and address;

(B) *Direct Sales.* For items exported (or reexported from Canada) through direct sale, the name and address of the recipient, the item, and the quantity exported; or

(C) *Foreign manufacturers and products that use encryption items.* For exports (*i.e.,* from the United States) or direct transfers (*e.g.,* by a "U.S. subsidiary" located outside the United States) of encryption components, source code, general purpose toolkits, equipment controlled under ECCN 5B002, technology, or items that provide an "open cryptographic interface," to a foreign developer or manufacturer headquartered in a country not listed in Supplement No. 3 to this part when intended for use in foreign products developed for commercial sale, the names and addresses of the manufacturers using these encryption items and, if known, when the product is made available for commercial sale, a non-proprietary technical description of the foreign products for which these encryption items are being used (*e.g.,* brochures, other documentation, descriptions or other identifiers of the final foreign product; the algorithm and key lengths used; general programming interfaces to the product, if known; any standards or protocols that the foreign product adheres to; and source code, if available).

(ii) *Submission requirements.* For exports occurring between January 1 and June 30, a report is due no later than August 1 of that year. For exports occurring between July 1 and December 31, a report is due no later than February 1 the following year. These reports must be provided in electronic form. Recommended file formats for electronic submission include spreadsheets, tabular text or structured text. Exporters may request other reporting arrangements with BIS to better reflect their business models. Reports may be sent electronically to BIS at *crypt@bis.doc.gov* and to the ENC Encryption Request Coordinator at *enc@nsa.gov,* or disks and CDs containing the reports may be sent to the following addresses:

(A) Department of Commerce, Bureau of Industry and Security, Office of National Security and Technology Transfer Controls, 14th Street and Pennsylvania Ave., NW., Room 2705, Washington, DC 20230, Attn: Encryption Reports, and

(B) Attn: ENC Encryption Request Coordinator, 9800 Savage Road, Suite 6940, Ft. Meade, MD 20755–6000.

(iii) *Exclusions from reporting requirement.* Reporting is not required for the following items and transactions:

(A) [Reserved]

(B) Encryption commodities or software with a symmetric key length not exceeding 64 bits;

(C) Encryption items exported (or reexported from Canada) via free and anonymous download;

(D) Encryption items from or to a U.S. bank, financial institution or its subsidiaries, affiliates, customers or contractors for banking or financial operations;

(E) Items listed in paragraph (b)(4) of this section, unless it is a foreign item described in paragraph (b)(4)(ii) of this section that has entered the United States;

(F) Foreign products developed by bundling or compiling of source code;

(2) *Key length increases.* Reporting is required for commodities and software that, after having been classified and authorized for License Exception ENC in accordance with paragraphs (b)(2) or (b)(3) of this section, are modified only to upgrade the key length used for confidentiality or key exchange algorithms. Such items may be exported or reexported under the previously authorized provision of License Exception ENC without a classification resubmission.

(i) *Information required.*

(A) A certification that no change to the encryption functionality has been made other than to upgrade the key length for confidentiality or key exchange algorithms.

(B) The original Commodity Classification Automated Tracking System (CCATS) authorization number issued by BIS and the date of issuance.

(C) The new key length.

(ii) *Submission requirements.*

(A) The report must be received by BIS and the ENC Encryption Request Coordinator before the export or reexport of the upgraded product; and

(B) The report must be e-mailed to *crypt@bis.doc.gov* and *enc@nsa.gov.*

(f) *Grandfathering.* The following provisions apply to encryption items reviewed and classified by BIS under this license exception prior to June 25, 2010:

(1) *Items described in paragraphs (b)(1) or (b)(3) of this section.* For encryption commodities, software and components described in (or otherwise meeting the specifications of) paragraphs (b)(1) or (b)(3) of this section effective June 25, 2010, such items reviewed and classified by BIS prior to June 25, 2010 are authorized for export and reexport to eligible end-users and destinations under the applicable paragraph (b)(1) or (b)(3) of this license exception using the CCATS previously issued by BIS, without any encryption registration (*i.e.,* the information described in Supplement No. 5 to part 742 of the EAR), new classification by BIS, self-classification reporting (*i.e.,* the information described in Supplement No. 8 to part 742 of the EAR), or semi-annual sales reporting required under section 740.17(e) provided the cryptographic functionality of the item has not changed. *See* paragraph (d)(1)(iii) of this section regarding changes in encryption functionality following a previous classification.

(2) *Items described in paragraph (b)(2) of this section.*

(i) *Commodities, software and components described in paragraph (b)(2)(i) of this section.* For encryption commodities, software and components described in (or otherwise meeting the specifications of) paragraph (b)(2)(i) of this section effective June 25, 2010, such items reviewed and classified by BIS prior to June 25, 2010 are authorized for export and reexport to eligible end-users and destinations under paragraph (b)(2) of this license exception using the CCATS previously issued by BIS, without any encryption registration (*i.e.,* the information described in Supplement No. 5 to part 742 of the EAR) and new classification by BIS, provided the previous CCATS established License Exception ENC § 740.17(b)(2) treatment for the item and the cryptographic functionality of the item has not changed. *See* paragraph (d)(1)(iii) of this section regarding changes in encryption functionality following a previous classification. An encryption registration and updated classification must be submitted to BIS for items described in paragraph (b)(2)(i) of this section effective June 25, 2010 if the items were not previously classified under § 740.17(b)(2), even if the cryptographic functionality has not changed.

(ii) *Cryptoanalytic items, open cryptographic interface items, and encryption technology.* For items described in (or otherwise meeting the specifications of) paragraphs (b)(2)(ii), (b)(2)(iii) or (b)(2)(iv) of this section effective June 25, 2010, such items reviewed and classified by BIS prior to June 25, 2010 are authorized for export and reexport to eligible end-users and destinations under paragraph (b)(2) of this license exception using the CCATS previously issued by BIS, without any encryption registration (*i.e.,* the information described in Supplement No. 5 to part 742 of the EAR), new classification by BIS, or self-classification reporting (*i.e.,* the information described in Supplement No. 8 to part 742 of the EAR), provided the cryptographic functionality of the item has not changed. *See* paragraph (d)(1)(iii) of this section regarding changes in encryption functionality following a previous classification.

PART 742—[AMENDED]

■ 9. The authority citation for part 742 continues to read as follows:

Authority: 50 U.S.C. app. 2401 *et seq.;* 50 U.S.C. 1701 *et seq.;* 22 U.S.C. 3201 *et seq.;* 42 U.S.C. 2139a; 22 U.S.C. 7201 *et seq.;* 22 U.S.C. 7210; Sec. 1503, Pub. L. 108–11, 117 Stat. 559; E.O. 12058, 43 FR 20947, 3 CFR, 1978 Comp., p. 179; E.O. 12851, 58 FR 33181, 3 CFR, 1993 Comp., p. 608; E.O. 12938, 59 FR 59099, 3 CFR, 1994 Comp., p. 950; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783; Presidential Determination 2003–23 of May 7, 2003, 68 FR 26459, May 16, 2003; Notice of August 13, 2009, 74 FR 41325 (August 14, 2009); Notice of November 6, 2009, 74 FR 58187 (November 10, 2009).

■ 10. Section 742.15 is amended by revising the Note to paragraph (a), revising paragraph (b), and adding paragraphs (c) and (d) to read as follows:

§ 742.15 Encryption Items.

* * * * *

(a) * * *

Note to paragraph (a): Pursuant to Note 3 to Category 5 Part 2 of the Commerce Control List in Supplement No. 1 to Part 774, mass market encryption commodities and software may be released from "EI" and "NS" controls by submitting an encryption registration in accord with § 742.15(b) of the EAR. Once an encryption registration has been submitted to BIS and accepted in SNAP–R as indicated by the issuance of an Encryption Registration Number (ERN), then the commodities and software are classified under ECCNs 5A992 and 5D992 respectively and are no longer subject to "EI" and "NS" controls.

(b) *Encryption registration required, with classification request or self-classification report, for mass market encryption commodities, software and components with encryption exceeding 64 bits.* To be eligible for export and reexport under this paragraph (b), encryption commodities, software and components must qualify for mass market treatment under the criteria in the Cryptography Note (Note 3) of Category 5, Part 2 ("Information Security"), of the Commerce Control List (Supplement No. 1 to part 774 of the EAR), and employ a key length greater than 64 bits for the symmetric algorithm (or, for commodities and software not implementing any symmetric algorithms, employing a key length greater than 768 bits for asymmetric algorithms or greater than 128 bits for elliptic curve algorithms). Encryption items that are described in §§ 740.17(b)(2) or (b)(3)(iii) of the EAR do not qualify for mass market

treatment. This paragraph (b) does not authorize export or reexport to, or provision of any service in any country listed in Country Group E:1 in Supplement No. 1 to part 740 of the EAR. Exports and reexports authorized under paragraphs (b)(1) and (b)(3) of this section must be supported by an encryption registration in accordance with paragraph (b)(7) of this section and the specific instructions of paragraph (r)(1) of Supplement No. 2 to part 748 of the EAR. In addition, paragraphs (b)(1) and (b)(3) of this section set forth requirements pertaining to the classification of mass market encryption commodities and software. *See* paragraph (d) of this section for grandfathering provisions applicable to certain encryption items reviewed and classified by BIS under this section prior to June 25, 2010. All classification requests, registrations, and reports submitted to BIS pursuant to this section for encryption items will be reviewed by the ENC Encryption Request Coordinator, Ft. Meade, MD. Only mass market encryption authorizations under this paragraph (b) to a company that has fulfilled the requirements of encryption registration (such as the producer of the item) authorize the export and reexport of the company's encryption items by all persons, wherever located, under this section. When an exporter or reexporter relies on the producer's self-classification (pursuant to the producer's encryption registration) or CCATS for a mass market encryption item, it is not required to submit an encryption registration, classification request or self-classification report.

(1) *Immediate mass market authorization.* Once an encryption registration is submitted to BIS in accordance with paragraph (b)(7) of this section and an Encryption Registration Number (ERN) has been issued, this paragraph (b)(1) authorizes the exports or reexports of the associated mass market encryption commodities and software classified under ECCNs 5A992 or 5D992 using the symbol "NLR", except any such commodities, software or components described in (b)(3) of this section, subject to submission a self-classification report in accordance with paragraph (c) of this section.

(2) [Reserved]

(3) *Classification request required for specified mass market commodities, software and components.* Thirty-days (30-days) after the submission of a classification request to BIS in accordance with paragraph (b)(7) of this section, this paragraph (b)(3) authorizes exports and reexports of the mass market items submitted for classification, using the symbol "NLR", provided the items qualify for mass market treatment as described in paragraph (b) of this section and are classified by BIS under ECCNs 5A992 or 5D992:

Note to introductory text of paragraph (b)(3): Once a mass market classification request is accepted in SNAP–R, you may export and reexport the encryption commodity or software under License Exception ENC as ECCN 5A002 or 5D002, whichever is applicable, to any end-user located or headquartered in a country listed in Supplement No. 3 to part 740 as authorized by § 740.17(b) of the EAR, while the mass market classification request is pending review with BIS.

(i) Specified mass market encryption components as follows:

(A) Chips, chipsets, electronic assemblies and field programmable logic devices;

(B) Cryptographic libraries, modules, development kits and toolkits, including for operating systems and cryptographic service providers (CSPs);

(C) Application-specific hardware or software development kits implementing cryptography.

(ii) Mass market encryption commodities, software and components that provide or perform "non-standard cryptography" as defined in part 772 of the EAR.

(iii) [Reserved]

(iv) *Mass market cryptographic enabling commodities and software.* Commodities and software and components that themselves qualify for mass market treatment, and activate or enable cryptographic functionality in mass market encryption products which would otherwise remain disabled, where the product or cryptographic functionality is not otherwise described in paragraph (b)(3)(i) of this section.

(4) *Exclusions from mass market classification request, encryption registration and self-classification reporting requirements.* The following commodities and software do not require a submission of an encryption registration, classification request or self-classification report to BIS for export or reexport as mass market products:

(i) *Short-range wireless encryption functions.* Commodities and software that are not otherwise controlled in Category 5, but are nonetheless classified under ECCN 5A992 or 5D992 only because they incorporate components or software that provide short-range wireless encryption functions (*e.g.,* with a nominal operating range not exceeding 100 meters according to the manufacturer's specifications, designed to comply with the Institute of Electrical and Electronic Engineers (IEEE) 802.11 wireless LAN standard or the IEEE 802.15.1 standard).

Note to paragraph (b)(4)(i): An example of what this paragraph authorizes for export without classification, registration or self-classification reporting is a laptop computer that without encryption would be classified under ECCN 4A994, and the Category 5, Part 2-controlled components of the laptop only implement short-range wireless encryption functionality. On the other hand, this paragraph (b)(4)(i) does not apply to any commodities or software that would still be classified under an ECCN in Category 5 even if the short-range wireless encryption functionality were removed. For example, certain access points, gateways and bridges are classified under ECCN 5A991 without encryption functionality, and components for mobile communication equipment are classified under ECCN 5A991.g without encryption functionality. Such items, when implementing cryptographic functionality controlled by Category 5, Part 2 are not excluded from encryption classification, registration or self-classification reporting by this paragraph.

(ii) *Foreign products developed with or incorporating U.S.-origin encryption source code, components, or toolkits.* Foreign products developed with or incorporating U.S.-origin encryption source code, components or toolkits that are subject to the EAR, provided that the U.S.-origin encryption items have previously been classified or registered and authorized by BIS and the cryptographic functionality has not been changed. Such products include foreign-developed products that are designed to operate with U.S. products through a cryptographic interface.

(5) [Reserved]

(6) *Examples of mass market encryption products.* Subject to the requirements of the Cryptography Note (Note 3) in Category 5, Part 2, of the Commerce Control List, mass market encryption products include, but are not limited to, general purpose operating systems and desktop applications (*e.g.,* e-mail, browsers, games, word processing, database, financial applications or utilities) designed for use with computers classified as ECCN 4A994 or designated as EAR99, laptops, or hand-held devices; commodities and software for client Internet appliances and client wireless LAN devices; home use networking commodities and software (*e.g.,* personal firewalls, cable modems for personal computers, and consumer set top boxes); and portable or mobile civil telecommunications commodities and software (*e.g.,* personal data assistants (PDAs), radios, or cellular products).

(7) *Mass market encryption registration and classification request procedures.*

(i) *Submission requirements and instructions.* To submit an encryption registration or classification request to BIS for certain mass market encryption items under this paragraph (b), you must submit an application to BIS in accordance with the procedures described in §§ 748.1 and 748.3 of the EAR and the instructions in paragraph (r) of Supplement No. 2 to part 748 "Unique Application and Submission Requirements", along with other required information as follows:

(A) *Encryption registration in support of mass market encryption classification requests and self-classification reports.* You must submit the applicable information as described in Supplement No. 5 to this part and follow the specific instructions of paragraph (r)(1) of Supplement No. 2 to part 748 of the EAR, if any of the following apply:

(*1*) This is your first time submitting an encryption classification request under paragraph (b)(3) of this section since August 24, 2010;

(*2*) You are making a mass market encryption product eligible for export and reexport (including as defined for encryption software in § 734.2(b)(9) of the EAR) under paragraph (b)(1) of this section for the first time since August 24, 2010; or

(*3*) If you have not otherwise provided BIS the information described in Supplement No. 5 to this part during the current calendar year and your answers to the questions in Supplement No. 5 to this part have changed since the last time you provided answers to the questions.

(B) *Technical information submission requirements.* In addition to the registration requirements of paragraph (b)(7)(i)(A) of this section, for all submissions of encryption classification requests for mass market products described under paragraph (b)(3) of this section, you must also provide BIS the applicable information described in paragraphs (a) through (d) of Supplement No. 6 to this part (Technical Questionnaire for Encryption Items). For mass market products authorized after the submission of an encryption registration under paragraph (b)(1) of this section, you may be required to provide BIS this information described in Supplement No. 6 to this part on an as-needed basis, upon request by BIS.

(C) *Changes in encryption functionality following a previous classification.* A new mass market encryption classification request (under paragraph (b)(3) of this section) or self-classification (under paragraph (b)(1) of this section) is required if a change is made to the cryptographic functionality (*e.g.,* algorithms) or other technical characteristics affecting mass market eligibility (*e.g.,* performance enhancements to provide network infrastructure services, or customizations to end-user specifications) of the originally classified product. However, a new product classification request or self-classification is not required when a change involves: the subsequent bundling, patches, upgrades or releases of a product; name changes; or changes to a previously reviewed encryption product where the change is limited to updates of encryption software components where the product is otherwise unchanged.

(ii) *Action by BIS.*

(A) *Encryption registrations for mass market encryption items.* Upon submission to BIS of an encryption registration in accordance with paragraph (b)(7)(i) of this section and acceptance of the application by SNAP–R, BIS will issue the Encryption Registration Number (ERN) via SNAP–R, which will constitute authorization under this paragraph (b). Immediately upon receiving your ERN from BIS, you may export and reexport mass market encryption products described in paragraph (b)(1) of this section using the symbol "NLR".

(B) *For mass market items requiring classification by BIS under paragraph (b)(3) of this section.*

(*1*) For mass market encryption classifications that require a thirty (30)-day waiting period, if BIS has not, within thirty (30) days from acceptance in SNAP–R of your complete classification request, informed you that your item is not authorized as a mass market item, you may export and reexport under the applicable provisions of this paragraph (b). If, during the course of its review, BIS determines that your encryption items do not qualify for mass market treatment under the EAR, or are otherwise classified under ECCN 5A002, 5B002, 5D002 or 5E002, BIS will notify you and will review your items for eligibility under License Exception ENC (*see* § 740.17 of the EAR for review and reporting requirements for encryption items under License Exception ENC).

(*2*) Upon completion of its review, BIS will issue a Commodity Classification Automated Tracking System (CCATS) to you.

(*3*) *Hold Without Action (HWA) for mass market classification requests.* BIS may hold your mass market classification request without action if necessary to obtain additional information or for any other reason necessary to ensure an accurate classification. Time on such "hold without action" status shall not be counted towards fulfilling the thirty-day (30-day) processing period specified in this paragraph.

(C) BIS may require you to supply additional relevant technical information about your encryption item(s) or information that pertains to their eligibility as mass market products at any time, before or after the expiration of the thirty-day (30-day) processing period specified in this paragraph and in paragraph (b)(3) of this section, or after any registrations as required in paragraph (b)(1) of this section. If you do not supply such information within 14 days after receiving a request from BIS, BIS may return your classification request without action or otherwise suspend or revoke your eligibility to use mass market authorization for that item. At your request, BIS may grant you up to an additional 14 days to provide the requested information. Any request for such an additional number of days must be made prior to the date by which the information was otherwise due to be provided to BIS and may be approved if BIS concludes that additional time is necessary.

(c) *Self-classification reporting for certain encryption commodities, software and components.* This paragraph (c) sets forth requirements for self-classification reporting to BIS and the ENC Encryption Request Coordinator (Ft. Meade, MD) of encryption commodities, software and components exported or reexported pursuant to encryption registration under §§ 740.17(b)(1) or 742.15(b)(1) of the EAR. Reporting is required, effective June 25, 2010.

(1) *When to report.* Your self-classification report for applicable encryption commodities, software and components exported or reexported during a calendar year (January 1 through December 31) must be received by BIS and the ENC Encryption Request Coordinator no later than February 1 the following year.

(2) *How to report.* Encryption self-classification reports must be sent to BIS and the ENC Encryption Request Coordinator via e-mail or regular mail. In your submission, specify the export timeframe that your report spans and identify points of contact to whom questions or other inquiries pertaining to the report should be directed. Follow these instructions for your submissions:

(i) *Submissions via e-mail.* Submit your encryption self-classification report electronically to BIS at *crypt-supp8@bis.doc.gov* and to the ENC Encryption Request Coordinator at

enc@nsa.gov, as an attachment to an e-mail. Identify your e-mail with subject "Self-classification report for ERN R######", using your most recent ERN in the subject line (so as to correspond your encryption self-classification report to your most recent encryption registration ERN).

(ii) *Submissions on disks and CDs.* The self-classification report may be sent to the following addresses, in lieu of e-mail:

(A) Department of Commerce, Bureau of Industry and Security, Office of National Security and Technology Transfer Controls, 14th Street and Pennsylvania Ave., NW., Room 2705, Washington, DC 20230, Attn: Encryption Reports, and

(B) Attn: ENC Encryption Request Coordinator, 9800 Savage Road, Suite 6940, Ft. Meade, MD 20755–6000.

(3) *Information to report.* Your encryption self-classification report must include the information described in paragraph (a) of Supplement No. 8 to this part for each applicable encryption commodity, software and component exported or reexported pursuant to an encryption registration under §§ 740.17(b)(1) or 742.15(b)(1) of the EAR. If no information has changed since the previously submitted report, you must either send an e-mail stating that nothing has changed since the previous report or submit a copy of the previously submitted report.

(4) *File format requirements.* The information described in paragraph (a) of Supplement No. 8 to this part must be provided to BIS and the ENC Encryption Request Coordinator in tabular or spreadsheet form, as an electronic file in comma separated values format (.csv) adhering to the specifications set forth in paragraph (b) of Supplement No. 8 to this part.

(d) *Grandfathering.* For mass market encryption commodities, software and components described in (or otherwise meeting the specifications of) paragraph (b) of this section effective June 25, 2010, such items reviewed and classified by BIS as mass market products prior to June 25, 2010 are authorized for export and reexport under paragraph (b) of this section using the CCATS previously issued by BIS, without any encryption registration (*i.e.,* the information described in Supplement No. 5 to this part), new classification by BIS, or self-classification reporting (*i.e.,* the information described in Supplement No. 8 to this part), provided the cryptographic functionality of the item has not changed. *See* paragraph (b)(7)(i)(C) of this section regarding changes in encryption functionality following a previous classification.

■ 11. Supplement No. 5 is revised to read as follows:

Supplement No. 5 to Part 742—Encryption Registration

Certain classification requests and self-classification reports for encryption items must be supported by an encryption registration, *i.e.,* the information as described in this Supplement, submitted as a support documentation attachment to an application in accordance with the procedures described in §§ 740.17(b), 740.17(d), 742.15(b), 748.1, 748.3 and Supplement No. 2 to part 748 of the EAR.

(1) Point of Contact Information
(a) Contact Person
(b) Telephone Number
(c) Fax Number
(d) E-mail address
(e) Mailing Address

(2) Company Overview (approximately 100 words).

(3) Identify which of the following categories apply to your company's technology/families of products:
(a) Wireless
(i) 3G cellular
(ii) 4G cellular/WiMax/LTE
(iii) Short-range wireless/WLAN
(iv) Satellite
(v) Radios
(vi) Mobile communications, n.e.s.
(b) Mobile applications
(c) Computing platforms
(d) Multimedia over IP
(e) Trusted computing
(f) Network infrastructure
(g) Link layer encryption
(h) Smartcards or other identity management
(i) Computer or network forensics
(j) Software
(i) Operating systems
(ii) Applications
(k) Toolkits/ASICs/components
(l) Information security including secure storage
(m) Gaming
(n) Cryptanalytic tools
(o) "Open cryptographic interface" (or other support for user-supplied or non-standard cryptography)
(p) Other (identify any not listed above)
(q) Not Applicable (Not a producer of encryption or information technology items)

(4) Describe whether the products incorporate or use proprietary, unpublished or non-standard cryptographic functionality, including encryption algorithms or protocols that have not been adopted or approved by a duly recognized international standards body. (If unsure, please explain.)

(5) Will your company be exporting "encryption source code"?

(6) Do the products incorporate encryption components produced or furnished by non-U.S. sources or vendors? (If unsure, please explain.)

(7) With respect to your company's encryption products, are any of them manufactured outside the United States? If yes, provide manufacturing locations. (Insert "not applicable", if you are not the principal producer of encryption products.)

■ 12. Supplement No. 6 is revised to read as follows;

Supplement No. 6 to Part 742—Technical Questionnaire for Encryption Items

(a) For all encryption items:

(1) State the name(s) of each product being submitted for classification or other consideration (as a result of a request by BIS) and provide a brief non-technical description of the type of product (*e.g.,* routers, disk drives, cell phones, and chips) being submitted, and provide brochures, data sheets, technical specifications or other information that describes the item(s).

(2) Indicate whether there have been any prior classifications or registrations of the product(s), if they are applicable to the current submission. For products with minor changes in encryption functionality, you must include a cover sheet with complete reference to the previous review (Commodity Classification Automated Tracking System (CCATS) number, Encryption Registration Number (ERN), Export Control Classification Number (ECCN), authorization paragraph) along with a clear description of the changes.

(3) Describe how encryption is used in the product and the categories of encrypted data (*e.g.,* stored data, communications, management data, and internal data).

(4) For 'mass market' encryption products, describe specifically to whom and how the product is being marketed and state how this method of marketing and other relevant information (*e.g.,* cost of product and volume of sales) are described by the Cryptography Note (Note 3 to Category 5, Part 2).

(5) Is any "encryption source code" being provided (shipped or bundled) as part of this offering? If yes, is this source code publicly available source code, unchanged from the code obtained from an open source Web site, or is it proprietary "encryption source code?"

(b) For classification requests and other submissions for an encryption

commodity or software, provide the following information:

(1) Description of all the symmetric and asymmetric encryption algorithms and key lengths and how the algorithms are used, including relevant parameters, inputs and settings. Specify which encryption modes are supported (*e.g.,* cipher feedback mode or cipher block chaining mode).

(2) State the key management algorithms, including modulus sizes that are supported.

(3) For products with proprietary algorithms, include a textual description and the source code of the algorithm.

(4) Describe the pre-processing methods (*e.g.,* data compression or data interleaving) that are applied to the plaintext data prior to encryption.

(5) Describe the post-processing methods (*e.g.,* packetization, encapsulation) that are applied to the cipher text data after encryption.

(6) State all communication protocols (*e.g.,* X.25, Telnet, TCP, IEEE 802.11, IEEE 802.16, SIP * * *) and cryptographic protocols and methods (*e.g.,* SSL, TLS, SSH, IPSEC, IKE, SRTP, ECC, MD5, SHA, X.509, PKCS standards * * *) that are supported and describe how they are used.

(7) Describe the encryption-related Application Programming Interfaces (APIs) that are implemented and/or supported. Explain which interfaces are for internal (private) and/or external (public) use.

(8) Describe the cryptographic functionality that is provided by third-party hardware or software encryption components (if any). Identify the manufacturers of the hardware or software components, including specific part numbers and version information as needed to describe the product. Describe whether the encryption software components (if any) are statically or dynamically linked.

(9) For commodities or software using Java byte code, describe the techniques (including obfuscation, private access modifiers or final classes) that are used to protect against decompilation and misuse.

(10) State how the product is written to preclude user modification of the encryption algorithms, key management and key space.

(11) Describe whether the product meets any of the § 740.17(b)(2) criteria. Provide specific data for each of the parameters listed, as applicable (*e.g.,* maximum aggregate encrypted user data throughput, maximum number of concurrent encrypted channels, and operating range for wireless products).

(12) For products which incorporate an "open cryptographic interface" as defined in part 772 of the EAR, describe the cryptographic interface.

(c) For classification requests for hardware or software "encryption components" other than source code (*i.e.,* chips, toolkits, executable or linkable modules intended for use in or production of another encryption item) provide the following additional information:

(1) Reference the application for which the components are used in, if known;

(2) State if there is a general programming interface to the component;

(3) State whether the component is constrained by function; and

(4) Identify the encryption component and include the name of the manufacturer, component model number or other identifier.

(d) For classification requests for "encryption source code" provide the following information:

(1) If applicable, reference the executable (object code) product that was previously classified by BIS or included in an encryption registration to BIS;

(2) Include whether the source code has been modified, and the technical details on how the source code was modified; and

(3) Upon request, include a copy of the sections of the source code that contain the encryption algorithm, key management routines and their related calls.

■ 13. Supplement No. 8 is added to read as follows:

Supplement No. 8 to Part 742—Self-Classification Report for Encryption Items

This supplement provides certain instructions and requirements for self-classification reporting to BIS and the ENC Encryption Request Coordinator (Ft. Meade, MD) of encryption commodities, software and components exported or reexported pursuant to encryption registration under License Exception ENC (§ 740.17(b)(1) only) or "mass market" (§ 742.15(b)(1) only) provisions of the EAR. *See* § 742.15(c) of the EAR for additional instructions and requirements pertaining to this supplement, including when to report and how to report.

(a) *Information to report.* The following information is required in the file format as described in paragraph (b) of this supplement, for each encryption item subject to the requirements of this supplement and §§ 740.17(b)(1) and 742.15(b)(1) of the EAR:

(1) Name of product (50 characters or less).

(2) Model/series/part number (50 characters or less.) If necessary, enter 'NONE' or 'N/A'.

(3) Primary manufacturer (50 characters or less). Enter 'SELF' if you are the primary manufacturer of the item. If there are multiple manufacturers for the item but none is clearly primary, either enter the name of one of the manufacturers or else enter 'MULTIPLE'. If necessary, enter 'NONE' or 'N/A'.

(4) Export Control Classification Number (ECCN), selected from *one* of the following:

(i) 5A002
(ii) 5B002
(iii) 5D002
(iv) 5A992
(v) 5D992

(5) Encryption authorization type identifier, selected from *one* of the following, which denote eligibility under License Exception ENC (§ 740.17(b)(1), only) or as 'mass market' (§ 742.15(b)(1), only):

(i) ENC
(ii) MMKT

(6) Item type descriptor, selected from *one* of the following:

(i) Access point
(ii) Cellular
(iii) Computer
(iv) Computer forensics
(v) Cryptographic accelerator
(vi) Data backup and recovery
(vii) Database
(viii) Disk/drive encryption
(ix) Distributed computing
(x) E-mail communications
(xi) Fax communications
(xii) File encryption
(xiii) Firewall
(xiv) Gateway
(xv) Intrusion detection
(xvi) Key exchange
(xvii) Key management
(xviii) Key storage
(xix) Link encryption
(xx) Local area networking (LAN)
(xxi) Metropolitan area networking (MAN)
(xxii) Modem
(xxiii) Network convergence or infrastructure n.e.s.
(xxiv) Network forensics
(xxv) Network intelligence
(xxvi) Network or systems management (OAM/OAM&P)
(xxvii) Network security monitoring
(xxviii) Network vulnerability and penetration testing
(xxix) Operating system
(xxx) Optical networking
(xxxi) Radio communications
(xxxii) Router
(xxxiii) Satellite communications
(xxxiv) Short-range wireless n.e.s.

(xxxv) Storage area networking (SAN)
(xxxvi) 3G/4G/LTE/WiMAX
(xxxvii) Trusted computing
(xxxviii) Videoconferencing
(xxxix) Virtual private networking (VPN)
(xl) Voice communications n.e.s.
(xli) Voice over Internet protocol (VoIP)
(xlii) Wide area networking (WAN)
(xliii) Wireless local area networking (WLAN)
(xliv) Wireless personal area networking (WPAN)
(xlv) Commodities n.e.s.
(xlvi) Components n.e.s.
(xlvii) Software n.e.s.
(xlviii) Test equipment n.e.s.
(xlix) OTHER

(b) *File format requirements.*

(1) The information described in paragraph (a) of this supplement must be provided in tabular or spreadsheet form, as an electronic file in comma separated values format (.csv), only. No file formats other than .csv will be accepted, as your encryption self-classification report must be directly convertible to tabular or spreadsheet format, where each row (and all entries within a row) properly correspond to the appropriate encryption item.

Note to paragraph (b)(1): An encryption self-classification report data table created and stored in spreadsheet format (*e.g.,* file extension .xls, .numbers, .qpw, .wb*, .wrk, and .wks) can be converted and saved into a comma delimited file format directly from the spreadsheet program. This .csv file is then ready for submission.

(2) Each line of your encryption self-classification report (.csv file) must consist of six entries as further described in this supplement.

(3) The first line of the .csv file must consist of the following six entries (*i.e.,* match the following) without alteration or variation: PRODUCT NAME, MODEL NUMBER, MANUFACTURER, ECCN, AUTHORIZATION TYPE, ITEM TYPE.

Note to paragraph (b)(3): These first six entries (*i.e.,* first line) of a encryption self-classification report in .csv format correspond to the six column headers (*i.e.,* first row) of a spreadsheet data file.

(4) Each subsequent line of the .csv file must correspond to a single encryption item (or a distinguished series of products) as described in paragraph (c) of this supplement.

(5) Each line must consist of six entries as described in paragraph (a)(1), (a)(2), (a)(3), (a)(4), (a)(5), and (a)(6) of this supplement. No entries may be left blank. Each entry must be separated by a comma (,). Certain additional instructions are as follows:

(i) Line entries (a)(1) ('PRODUCT NAME') and (a)(4) ('ECCN') must be completed with relevant information.

(ii) For entries (a)(2) ('MODEL NUMBER') and (a)(3) ('MANUFACTURER'), if these entries do not apply to your item or situation you may enter 'NONE' or 'N/A'.

(iii) For entries (a)(5) ('AUTHORIZATION TYPE'), if none of the provided choices apply to your situation, you may enter 'OTHER'.

(6) Because of .csv file format requirements, the only permitted use of a comma is as the necessary separator between line entries. You may not use a comma for any other reason in your encryption self-classification report.

(c) *Other instructions.*

(1) The information provided in accordance with this supplement and §§ 740.17(b)(1), 742.15(b)(1) and 742.15(c) of the EAR must identify product offerings as they are typically distinguished in inventory, catalogs, marketing brochures and other promotional materials.

(2) For families of products where all the information described in paragraph (a) of this supplement is identical except for the model/series/part number (entry (a)(2)), you may list and describe these products with a single line in your .csv file using an appropriate model/series/part number identifier (*e.g.,* '300' or '3xx') for entry (a)(2), provided each line in your .csv file corresponds to a single product series (or product type) within an overall product family.

(3) For example, if Company A produces, markets and sells both a '100' ('1xx') and a '300' ('3xx') series of product, in its encryption self-classification report (.csv file) Company A must list the '100' product series in one line (with entry (a)(2) completed as '100' or '1xx') and the '300' product series in another line (with entry (a)(2) completed as '300' or '3xx'), even if the other required information is common to all products in the '100' and '300' series.

PART 748—[AMENDED]

■ 14. The authority citations for part 748 continue to read as follows:

Authority: 50 U.S.C. app. 2401 *et seq.;* 50 U.S.C. 1701 *et seq.;* E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783; Notice of August 13, 2009, 74 FR 41325 (August 14, 2009).

■ 15. Section 748.1 is amended by:

■ a. Revising the first two sentences of the introductory text to paragraph (a);

■ b. Revising introductory text to paragraph (d); and

■ c. Revising paragraph (d)(1)(i), to read as follows:

§ 748.1 General provisions.

(a) *Scope.* In this part, references to the Export Administration Regulations or EAR are references to 15 CFR chapter VII, subchapter C. The provisions of this part involve requests for classifications and advisory opinions, export license applications, encryption registration, reexport license applications, and certain license exception notices subject to the EAR. * * *

* * * * *

(d) *Electronic Filing Required.* All export and reexport license applications (other than Special Comprehensive License or Special Iraq Reconstruction License applications), encryption registrations, license exception AGR notifications, and classification requests and their accompanying documents must be filed via BIS's Simplified Network Application Processing system (SNAP–R), unless BIS authorizes submission via the paper forms BIS 748–P (Multipurpose Application Form), BIS–748P–A (Item Appendix) and BIS–748P–B, (End-User Appendix). Only original paper forms may be used. Facsimiles or reproductions are not acceptable.

(1) * * *

(i) BIS has received no more than one submission (*i.e.* the total number of export license applications, reexport license applications, license exception AGR notifications, *and* classification requests) from that party in the twelve months immediately preceding its receipt of the current submission;

* * * * *

■ 16. Section 748.3 is amended by revising the section heading and paragraphs (a) and (d) to read as follows:

§ 748.3 Classification requests, advisory opinions, and encryption registrations.

* * * * *

(a) *Introduction.* You may ask BIS to provide you with the correct Export Control Classification Number down to the paragraph (or subparagraph) level, if appropriate. BIS will advise you whether or not your item is subject to the EAR and, if applicable, the appropriate ECCN. This type of request is commonly referred to as a "Classification Request." If requested, for a given end-use, end-user, and/or destination, BIS will advise you whether a license is required, or likely to be granted, for a particular transaction. Note that these responses do not bind BIS to issuing a license in the future. This type of request, along with requests for guidance regarding other interpretations of the EAR, is commonly referred to as an "Advisory Opinion." The encryption provisions in

the EAR require the submission of an encryption registration or classification request in accordance with § 740.17(d) of the EAR in order for certain items to be eligible for export and reexport under License Exception ENC (*see* § 740.17 of the EAR) or to be released from "EI" controls (*see* §§ 742.15(b)(1) and 742.15(b)(3) of the EAR).

* * * * *

(d) *Classification requests and encryption registration for encryption items.* A classification request or encryption registration associated with encryption items transferred from the U.S. Munitions List consistent with Executive Order 13026 of November 15, 1996 (3 CFR, 1996 Comp., p. 228) and pursuant to the Presidential Memorandum of that date may be required to determine eligibility under License Exception ENC or for release from "EI" controls. Refer to Supplement No. 5 to part 742 of the EAR for information that must be included in the encryption registration, which must be submitted in support of certain encryption classification requests and self-classification reports. Refer to Supplement No. 6 to part 742 of the EAR for a complete list of technical information that is required for encryption classification requests. Refer to § 742.15(c) and Supplement No. 8 to part 742 of the EAR for information that is required to be submitted in a self-classification report. Refer to § 742.15(b) of the EAR for instructions regarding mass market encryption commodities and software, including encryption registration, self-classifications and classification requests. Refer to § 740.17 of the EAR for the provisions of License Exception ENC, including encryption registration, self-classifications, classification requests and sales reporting. All classification requests, registrations, and reports submitted to BIS pursuant to §§ 740.17 and 742.15(b) of the EAR for encryption items will be reviewed by the ENC Encryption Request Coordinator, Ft. Meade, MD.

■ 17. Section 748.8 is amended by removing from paragraph (r) the phrase "Encryption review requests." and adding in its place "Encryption classification requests and encryption registrations."

■ 18. Supplement No. 1 is amended by revising the paragraph for block 5 to read as follows:

Supplement No. 1 to Part 748—BIS–748P, BIS–748P–A: Item Appendix, and BIS–748P–B: End-User Appendix; Multipurpose Application Instructions

* * * * *

Block 5: Type of Application. *Export.* If the items are located within the United States, and you wish to export those items, mark the Box labeled "Export" with an (X). *Reexport.* If the items are located outside the United States, mark the Box labeled "Reexport" with an (X). *Classification.* If you are requesting BIS to classify your item against the Commerce Control List (CCL), mark the Box labeled "Classification Request" with an (X). *Encryption Registration.* If you are requesting encryption registration under License Exception ENC (§ 740.17 of the EAR) or "mass market" encryption provisions (§ 742.15(b) of the EAR), mark the Box labeled "Encryption Registration" with an (X). *Special Comprehensive License.* If you are submitting a Special Comprehensive License application in accordance with the procedures described in part 752 of the EAR, mark the Box labeled "Special Comprehensive License" with an (X).

* * * * *

■ 19. Supplement No. 2 is amended by revising paragraph (r) to read as follows:

Supplement No. 2 to Part 748—Unique Application and Submission Requirements

* * * * *

(r) *Encryption registrations and classification requests.* Failure to follow the instructions in this paragraph may delay consideration of your encryption classification request or encryption registration.

(1) *Encryption registration.* Fill out blocks 1–4, 14, 15, 24, and 25 pursuant to the instructions in Supplement No. 1 to this Part. Leave blocks 6, 7, 8, 9–13, and 16–23 blank. In Block 5 (Type of Application), place an "X" in the box marked "Encryption Registration".

(2) *Classification Requests.* Fill out blocks 1–4, 14, 15, 22, and 25 pursuant to the instructions in Supplement No. 1 to this Part. Leave blocks 6, 7, 8, 10–13, 18–21, and 23 blank. Follow the directions specified for the blocks indicated below.

(i) In Block 5 (Type of Application), place an "X" in the box marked "classification" or "commodity classification" if submitting electronically for classification requests.

(ii) In Block 9 (Special Purpose).

(A) If submitting via SNAP–R, check the box "check here if you are submitting information about encryption required by 740.17 or 742.15 of the EAR."

(B) From the drop down menu in SNAP–R, choose:

(*1*) "License Exception ENC" if you are submitting an encryption classification request for specified License Exception ENC provisions (§§ 740.17(b)(2) or (b)(3) of the EAR);

(*2*) "Mass Market Encryption" if you are submitting an encryption classification request for certain mass market encryption items (§ 742.15(b)(3) of the EAR).

(*3*) "Encryption—other" if you are submitting an encryption classification, for another reason.

(iii) In Block 24 (Additional Information), insert your most recent Encryption Registration Number (ERN).

* * * * *

PART 772—[AMENDED]

■ 20. The authority citation for part 772 continues to read as follows:

Authority: 50 U.S.C. app. 2401 *et seq.;* 50 U.S.C. 1701 *et seq.;* E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783; Notice of August 13, 2009, 74 FR 41325 (August 14, 2009).

■ 21. Section 772.1 is amended by:

■ a. Removing the definition, nota bene and footnote No. 1 for "ancillary cryptography";

■ b. Removing the definition for "personalized smart card"; and

■ c. Adding in alphabetical order the definition for "non-standard cryptography", to read as follows:

§ 772.1 Definitions of Terms.

* * * * *

Non-standard cryptography. Means 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 duly recognized international standards body (*e.g.,* IEEE, IETF, ISO, ITU, ETSI, 3GPP, TIA, and GSMA) and have not otherwise been published.

* * * * *

PART 774—[AMENDED]

■ 22. The authority citation for part 774 continues to read as follows:

Authority: 50 U.S.C. app. 2401 *et seq.;* 50 U.S.C. 1701 *et seq.;* 10 U.S.C. 7420; 10 U.S.C. 7430(e); 22 U.S.C. 287c, 22 U.S.C. 3201 *et seq.,* 22 U.S.C. 6004; 30 U.S.C. 185(s), 185(u); 42 U.S.C. 2139a; 42 U.S.C. 6212; 43 U.S.C. 1354; 15 U.S.C. 1824a; 50 U.S.C. app. 5; 22 U.S.C. 7201 *et seq.;* 22 U.S.C. 7210; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783; Notice of August 13, 2009, 74 FR 41325 (August 14, 2009).

■ 23. In Supplement No. 1 to part 774 (the Commerce Control List), Category 5 Telecommunications and "Information Security", Part II Information Security is amended by:

■ a. Revising the Nota Bene to the Note 3 (Cryptography Note); and

■ b. Adding a new Note 4 to the beginning of Category 5 part II, to read as follows:

Supplement No. 1 to Part 774—The Commerce Control List

* * * * *

CATEGORY 5—TELECOMMUNICATIONS AND "INFORMATION SECURITY" Part II. "INFORMATION SECURITY"

* * * * *

N.B. to Note 3 (Cryptography Note): You must submit a classification request or encryption registration to BIS for mass market encryption commodities and software eligible for the Cryptography Note employing a key length greater than 64 bits for the symmetric algorithm (or, for commodities and software not implementing any symmetric algorithms, employing a key length greater than 768 bits for asymmetric algorithms or greater than 128 bits for elliptic curve algorithms) in accordance with the requirements of § 742.15(b) of the EAR in order to be released from the "EI" and "NS" controls of ECCN 5A002 or 5D002.

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.

* * * * *

■ 24. In Supplement No. 1 to part 774 (the Commerce Control List), Category 5 Telecommunications and "Information Security", Part 2 Information Security, ECCN 5A002 is amended by revising the Related Controls and the Items paragraph of the List of Items Controlled section, to read as follows:

5A002 "Information security" systems, equipment and components therefor, as follows (see List of Items Controlled).

* * * * *

List of Items Controlled

Unit: * * *

Related Controls: (1) 5A002 does not control the commodities listed in paragraphs (a), (d), (e), (f), (g) and (i) in the Note in the items paragraph of this entry. These commodities are instead classified under ECCN 5A992, and related software and technology are classified under ECCNs 5D992 and 5E992 respectively. (2) After encryption registration to or classification by BIS, mass market encryption commodities that meet eligibility requirements are released from "EI" and "NS" controls. These commodities are classified under ECCN 5A992.c. *See* § 742.15(b) of the EAR.

Related Definitions: * * *

Items:

Note: 5A002 does not control any of the following. However, these items are instead controlled under 5A992:

(a) Smart cards and smart card 'readers/writers' as follows:

(1) A smart card or an electronically readable personal document (*e.g.,* token coin, e-passport) that meets any of the following:

a. The cryptographic capability is restricted for use in equipment or systems excluded from 5A002 by Note 4 in Category 5—Part 2 or entries (b) to (i) of this Note, and cannot be reprogrammed for any other use; *or*

b. Having all of the following:

1. It is specially designed and limited to allow protection of 'personal data' stored within;

2. Has been, or can only be, personalized for public or commercial transactions or individual identification; *and*

3. Where the cryptographic capability is not user-accessible;

Technical Note: 'Personal data' includes any data specific to a particular person or entity, such as the amount of money stored and data necessary for authentication.

(2) 'Readers/writers' specially designed or modified, and limited, for items specified by (a)(1) of this Note.

Technical Note: 'Readers/writers' include equipment that communicates with smart cards or electronically readable documents through a network.

(b) [Reserved]

N.B.: See Note 4 in Category 5—Part 2 for items previously specified in 5A002 Note (b).

(c) [Reserved]

N.B.: See Note 4 in Category 5—Part 2 for items previously specified in 5A002 Note (c).

(d) Cryptographic equipment specially designed and limited for banking use or 'money transactions';

Technical Note: The term 'money transactions' includes the collection and settlement of fares or credit functions.

(e) Portable or mobile radiotelephones for civil use (*e.g.,* for use with commercial civil cellular radio communication systems) that are not capable of transmitting encrypted data directly to another radiotelephone or equipment (other than Radio Access Network (RAN) equipment), nor of passing encrypted data through RAN equipment (*e.g.,* Radio Network Controller (RNC) or Base Station Controller (BSC));

(f) Cordless telephone equipment not capable of end-to-end encryption where the maximum effective range of unboosted cordless operation (*i.e.,* a single, unrelayed hop between terminal and home base station) is less than 400 meters according to the manufacturer's specifications;

(g) Portable or mobile radiotelephones and similar client wireless devices for civil use, that implement only published or commercial cryptographic standards (except for anti-piracy functions, which may be non-published) and also meet the provisions of paragraphs b. to d. of the Cryptography Note (Note 3 in Category 5—Part 2), that have been customized for a specific civil industry application with features that do not affect the cryptographic functionality of these original non-customized devices; *or*

(h) [Reserved]

N.B.: See Note 4 in Category 5—Part 2 for items previously specified in 5A002 Note (h).

(i) Wireless "personal area network" equipment that implement only published or commercial cryptographic standards and where the cryptographic capability is limited to a nominal operating range not exceeding 30 meters according to the manufacturer's specifications.

a. Systems, equipment, application specific "electronic assemblies", modules and integrated circuits for "information security", as follows, and components therefor specially designed for "information security":

N.B.: For the control of Global Navigation Satellite Systems (GNSS) receiving equipment containing or employing decryption, *see* ECCN 7A005.

a.1. Designed or modified to use "cryptography" employing digital techniques performing any cryptographic function other than authentication or digital signature and having any of the following:

Technical Notes: 1. Authentication and digital signature functions include their associated key management function.

2. Authentication includes all aspects of access control where there is no encryption of files or text except as directly related to the protection of passwords, Personal Identification Numbers (PINs) or similar data to prevent unauthorized access.

3. "Cryptography" does not include "fixed" data compression or coding techniques.

Note: 5A002.a.1 includes equipment designed or modified to use "cryptography" employing analog principles when implemented with digital techniques.

a.1.a. A "symmetric algorithm" employing a key length in excess of 56-bits; *or*

a.1.b. An "asymmetric algorithm" where the security of the algorithm is based on any of the following:

a.1.b.1. Factorization of integers in excess of 512 bits (*e.g.,* RSA);

a.1.b.2. Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (*e.g.,* Diffie-Hellman over Z/pZ); *or*

a.1.b.3. Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2 in excess of 112 bits (*e.g.,* Diffie-Hellman over an elliptic curve);

a.2. Designed or modified to perform cryptanalytic functions;

a.3. [Reserved]

a.4. Specially designed or modified to reduce the compromising emanations of information-bearing signals beyond what is necessary for health, safety or electromagnetic interference standards;

a.5. Designed or modified to use cryptographic techniques to generate the spreading code for "spread spectrum" systems, not controlled in 5A002.a.6., including the hopping code for "frequency hopping" systems;

a.6. Designed or modified to use cryptographic techniques to generate channelizing codes, scrambling codes or network identification codes, for systems using ultra-wideband modulation techniques and having any of the following:

a.6.a. A bandwidth exceeding 500 MHz; *or*

a.6.b. A "fractional bandwidth" of 20% or more;

a.7. Non-cryptographic information and communications technology (ICT) security systems and devices evaluated to an assurance level exceeding class EAL–6 (evaluation assurance level) of the Common Criteria (CC) or equivalent;

a.8. Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion;

a.9. Designed or modified to use 'quantum cryptography.'

Technical Notes: 1. 'Quantum cryptography' A family of techniques for the establishment of a shared key for "cryptography" by measuring the quantum-mechanical properties of a physical system (including those physical properties explicitly governed by quantum optics, quantum field theory, or quantum electrodynamics).

2. 'Quantum cryptography' is also known as Quantum Key Distribution (QKD).

■ 25. In Supplement No. 1 to part 774 (the Commerce Control List), Category 5 Telecommunications and "Information Security", Part 2 Information Security, ECCN 5A992 is amended by revising paragraph c. in the items paragraph of the List of Items Controlled section, to read as follows:

5A992 Equipment not controlled by 5A002.

* * * * *

List of Items Controlled

* * * * *

Items:

* * * * *

c. Commodities that BIS has received an encryption registration or that have been classified as mass market encryption commodities in accordance with § 742.15(b) of the EAR.

* * * * *

■ 26. In Supplement No. 1 to part 774 (the Commerce Control List), Category 5 Telecommunications and "Information Security", Part 2 "Information Security", ECCN 5D002 is amended by revising the Related Controls paragraph in the List of Items Controlled section, to read as follows:

"**5D002 "Software" as follows (see List of Items Controlled).**

* * * * *

List of Items Controlled

* * * * *

Related Controls: (1) This entry does not control "software" "required" for the "use" of equipment excluded from control under the Related Controls paragraph or the Technical Notes in ECCN 5A002 or "software" providing any of the functions of equipment excluded from control under ECCN 5A002. This software is classified as ECCN 5D992. (2) After an encryption registration has been submitted to BIS or classification by BIS, mass market encryption software that meet eligibility requirements are released from "EI" and "NS" controls. This software is classified under ECCN 5D992.c. *See* § 742.15(b) of the EAR.

* * * * *

■ 27. In Supplement No. 1 to part 774 (the Commerce Control List), Category 5 Telecommunications and "Information Security", Part 2 Information Security, ECCN 5D992 is amended by revising paragraph c. of the Items paragraph of the List of Items Controlled section, to read as follows:

5D992 "Information Security" "software" not controlled by 5D002.

* * * * *

List of Items Controlled

* * * * *

Items:

* * * * *

c. "Software" that BIS has received an encryption registration or that have been classified as mass market encryption software in accordance with § 742.15(b) of the EAR.

* * * * *

■ 28. Supplement No. 3 is revised to read as follows:

Supplement No. 3 to Part 774—Statements of Understanding

(a) Statement of Understanding—medical equipment. Commodities that are "specially designed for medical end-use" that "incorporate" commodities or software on the Commerce Control List (Supplement No. 1 to part 774 of the EAR) that do not have a reason for control of Nuclear Nonproliferation (NP), Missile Technology (MT), or Chemical & Biological Weapons (CB) are designated by the number EAR99 (*i.e.,* are not elsewhere specified on the Commerce Control List).

Notes to paragraph a: (1) "Specially designed for medical end-use" means designed for medical treatment or the practice of medicine (does not include medical research).

(2) Commodities or software are considered "incorporated" if the commodity or software is: Essential to the functioning of the medical equipment; customarily included in the sale of the medical equipment; and exported or reexported with the medical equipment.

(3) Except for such software that is made publicly available consistent with § 734.3(b)(3) of the EAR, commodities and software "specially designed for medical end-use" remain subject to the EAR.

(4) *See also* § 770.2(b) interpretation 2, for other types of equipment that incorporate items on the Commerce Control List that are subject to the EAR.

(5) For computers used with medical equipment, *see also* ECCN 4A003 note 2 regarding the "principal element" rule.

(6) For commodities and software specially designed for medical end-use that incorporate an encryption or other "information security" item subject to the EAR, *see also* Note 1 to Category 5, Part II of the Commerce Control List.

(b) *Statement of Understanding—Source Code.* For the purpose of national security controlled items, "source code" items are controlled either by "software" or by "software" and "technology" controls, except when such "source code" items are explicitly decontrolled.

(c) *Category 5—Part 2—Note 4 Statement of Understanding.* All items previously described by Notes (b), (c) and (h) to 5A002 are now described by Note 4 to Category 5—Part 2. Note (h) to 5A002 prior to June 25, 2010 stated that the following was not controlled by 5A002:

Equipment specially designed for the servicing of portable or mobile radiotelephones and similar client wireless devices that meet all the

provisions of the Cryptography Note (Note 3 in Category 5, Part 2), where the servicing equipment meets all of the following:

(1) The cryptographic functionality of the servicing equipment cannot easily be changed by the user of the equipment;

(2) The servicing equipment is designed for installation without further substantial support by the supplier; *and*

(3) The servicing equipment cannot change the cryptographic functionality of the device being serviced.

Dated: June 17, 2010.

Kevin J. Wolf,

Assistant Secretary for Export Administration.

[FR Doc. 2010–15072 Filed 6–24–10; 8:45 am]

BILLING CODE 3510–33–P