RECORD OF PUBLIC COMMENTS

INTERIM FINAL RULE, WITH REQUEST FOR COMMENTS: 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

Publication in the Federal Register: June 25, 2010 (75 FR 36481)
Comments due August 24, 2010

	SOURCE	SIGNER(S) OF COMMENT	DATE	NUMBER OF PAGES
1.	Bill Root	Bill Root	07/05/10	6
2.	Cisco	Steve Bird	08/20/10	3
3.	TechAmerica	Ken Montgomery	08/24/10	14
4.	Semiconductor Industry Association (SIA)	Cynthia Johnson & David Rose	08/24/10	32
5.	Alliance for Network Security	Roszel C. Thomsen II	08/24/10	20
6.	eCrypt technologies Inc	Brad Lever	08/30/10	2

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

July 5, 2010

To: Publiccomments@bis.doc.gov
From: Bill Root

Subject: Encryption June 25, 2010, regulation RIN 0694-AE89

1. 730 Supplement No. 1:

The term "Commercial Encryption Items under Commerce Jurisdiction" implies, probably unintentionally, that
(a) there are also non-"Commercial" items under Commerce jurisdiction; and
(b) OMB has assigned to BIS information collection requirements for the Patent and Trademark Office in the Department of Commerce (see 730 Supp. 3).
Part 772.1 does not define "Commercial." It does define "Encryption items" to include "all encryption commodities, software, and technology that contain encryption features and are subject to the EAR."

It is recommended that the term in 730 Supp. 1 be changed to either "Encryption Items" (in quotation marks) or Encryption Items Subject to the EAR.

2. 734.4(b)(1):

This section, as amended on June 25 and on June 28, 2010, defines encryption item U.S.-origin commodities or software *de minimis* eligibility , "if controlled under ECCNs 5A002.a.1, a.2, a.5, a.6, or a.9 or 5D002," as those meeting not only paragraphs (c) or (d) but also paragraphs (b)(1)(i, ii, iii, iv, or v).

(a) Paragraphs (b)(1)(ii) and (iii) limit eligibility for those ECCNs to those "Authorized for License Exception ENC by BIS after classification pursuant to Sec. (740.17 (b)(3) or (b)(2))." However, 740.17(b)(3) and (b)(2) authorize License Exception ENC after submitting a classification request whether or not BIS has completed its classification. For those instances where the authorization is to export or reexport immediately after submission of the classification request, BIS could not have completed its classification. For the remainder instances where the exporter or reexporter must wait 30 days, BIS may, or may not, have completed its classification within 30 days.

It is recommended that "by BIS after classification" in (b)(1)(ii) and (iii) be changed to "after submission of a classification request."

(b) Paragraph (b)(1)(iii) does not apply if the foreign-made product will be sent to an E:1 country. This implies that (b)(1)(i ii, iv, and v) are not limited in this fashion. However, neither the 740.13(e) portion of TSU nor entire ENC applies to E:1. Per 734.3(a)(3), foreign-made products with uncontrolled U.S.-origin content are not subject to the EAR. Therefore, the only effect of *de minimis* for items eligible for TSU or ENC is to E:1 countries.

It is recommended that (b)(1)(i, ii, iv, and v) be revised to apply explicitly to E:1 and that, if, as a policy matter, 740.17(b)(2) must not be eligible for *de minimis* to E:1, that be so stated in 734.4(a)(2) and 734.4(b)(1)(iii) be deleted.

(c) It is unclear whether, in 734.4(b)(1), 5D002 is intended to mean all of 5D002 or only the EI portion (5D002.a, or .c.1 for 5A002.a,1 a.2, a.5, a.6, or a.9).

It is recommended that, in 734.4(b)(1), either "all of" be inserted before 5D002 or that "5D002" be changed to "5D002.a, or .c.1 for 5A002.a,1 a.2, a.5, a.6, or a.9"

(d) Per 734.4(b)(2), 5A992, 5D992, and 5E992 are eligible for *de minimis* with no special requirements. However, 734.4(b) applies only to "special requirements." If it is necessary to expressly authorize de *miniimis* for those encryption items for which there are no special requirements, eligibility for 5A002.a.4, a.7, a.8 and 5B002 should also be mentioned.

It is recommended that either 734.4(b)(2) be deleted or 5B002 and the portions of 5A002 and perhaps 5D002 not addressed in (b)(1) be added to (b)(2).

3. 738.4(a)(2)(ii)(B):

This section states that, per 742.15(b), classification as well as registration requirements apply to NLR eligibility for certain mass market encryption items. However, 742.15(b)(1) applies only the registration pre-requisite for mass market exceeding 64 bits key length if not also described in 740.17(b)(2) or (b)(3)(iii) per 742.15(b) intro or the remainder of 740.17 (b)(3) per 742.15(b)(3). The classification request requirement makes 740.17(b)(2) and (b)(3) eligible for ENC applicable to 5A002, 5D002, or 5E002, not for NLR applicable to.5A992 or 5D992.

It is recommended that "and classification" be deleted from 738.4(a)(2)(ii)(B).

4. Items eligible for ENC:

The first sentence of 740.17 intro states that ENC applies to "equipment, commodities, and components therefor" classified 5A002.a.1, 2.,5. 6, and 9, "systems, equipment, and components therefor" classified 5B002, and "equivalent or related" software or technology classified 5D002 or 5E002. The same wording appears in 740.17(a)(2) and the "equivalent or related" wording" also appears in 740.17(a)(1) and (b)(1).

(a) 5A002 uses the term "equipment." rather than "commodities"; but "commodities" is a broader term which includes "equipment" ECCN 5B002 uses the term "equipment" but does not use the terms "systems" or "components therefor". 5B002 covers equipment for the development, production, or testing of all of 5A002, not just selected 5A002 sub-items. 5D002 and 5E002 do not use the term "equivalent or related."

It is recommended that "equipment, commodities, and components therefor"; "systems, equipment, and components therefor"; and "equivalent or related" be deleted from 740.17 intro and 740.17(a)(2); and "equivalent or related" be deleted from (a)(1), (b)(1), and (b)(3)(i) and that "therefor" be substituted where applicable.

(b) Coverage of 740.17(b)(1) explicitly excludes commodities described in (b)(2) or (b)(3). 5A002.a.2 (cryptanalytic) and a.9 (quantum) are, in substance, identical to (b)(2)(ii) and (b)(2)(i)(D), respectively..

It is recommended that a.2 and a.9 be deleted from 740.17(b)(1)

(c) The omitted 5A002 sub-items are a.4, a.7, and a.8. 5A002.a.8 (detect surreptitious intrusions) might be construed to cover parts of:

(b)(2)(i)(F) (penetration capabilities),
(b)(3)(ii) (non-standard cryptography), and
(b)(3)(iii) (vulnerability analysis).

5A002.a.4 (reduce compormising emanations) and a.7 (non-cryptographic), while not appearing to correspond with any (b)(2) or (b)(3) item, might be useful as starting points to seek explicit 5A002 coverage of such items as

(b)(2)(i)(G) (public safety),
(b)(2)(iii) (open cryptographic interface),
(b)(3)(i) (chips, development kits, toolkits)
(b)(3)(iv) (cryptographic enabling)

ENC now applies in 740.17(a)(1) and (a)(2) to all of 5D002 and 5E002 for 5B002, which in turn applies to all of 5A002.

It is recommended that ENC apply to all of 5A002.

(d) Many of the commodity items listed in 740.17(b)(2) and (b)(3) are not identified with a corresponding 5A002 sub-item. It is difficult to see the relationship even for those which are so identified. For example, (b)(3)(i) (chips, toolkits) vs. 5A002.a.1 (key length), a.5 (spread spectrum), and a.6 (wide bandwidth). There is no stated relationship to any 5A002 sub-item and no evident substantive relationship to any 5A002 sub-item for:

b.2.i.A (network infrastructure),
b.2.i.C (customized),
b.2.i.E (for 4A003 computers),
b.2.i.F (penetration capabilities),
b.2.i.G (public safety),
b.2.iii (open cryptographic interface),
b.3.i (chips, development kits, toolkits)
b.3.ii (non-standard cryptography), and
b.3.iii (vulnerability analysis).
b.3.iv (cryptographic enabling)
b.4.i (short-range wireless)
b.4.ii (foreign products developed with U.S.-origin encryption source code components or toolkits)

The extent to which 740.17(b)(2) and (b)(3) items are not, in fact, covered by 5A002 sub-items constitutes unilateral U.S. controls. Expired EAA section 5(c)(6) prohibits unilateral national security export controls in the absence of a no foreign availability determination or on-going efforts to obtain multilateral control. Executive Order 13222 calls for carrying out EAA provisions to the extent permitted by law.

It is recommended that:
to the extent possible, each 740.7(b) item be associated with 5A002 sub-item(s);
portions of 740.17(b) which are not covered by 5A002 be identified;
such portions either be deleted from 740.17(b) or be moved temporarily to new unilateral ECCNs 5x902; and
the United States seek Wassenaar coverage of what was moved to 5x902.

5. Direct product controls:

The Notes to 740.17(a)(1)(iii) and 740.17(a)(2) state that items produced with items exported or reexported under paragraph (a)(1) or (a)(2) are subject to the EAR. This is broader than General Prohibition 3 (Foreign-Produced Direct Product Reexports), e.g., the latter applies only to Cuba and Country Group D:1.

In addition 740.17.b.4.ii presumes that foreign products developed with U.S.-origin encryption source code components or toolkits are covered by 5A002 (or perhaps 5B002). (b)(4)(ii) would not be subject to the EAR unless the U.S. content were controlled, per 734.3(a)(3).

It is recommended that:
the differences between General Prohibition 3 and the Notes to 740.17(a)(1)(iii) and 740.17(a)(2) be resolved; and
740.17(b)(4)(ii) and 742.15(b)(4)(ii) be amended to insert “controlled” before “U.S.-origin”

6 End-users headquartered in another country.

Note 1 to the introductory text of 740.17(b)(2) states that items described in (b)(2), except cryptanalytic items, may be exported to end-users located, or headquartered, in a Supp. 3 country immediately after submission of a classification request. The (b)(2)(i) and (ii) introductory texts authorize export of (b)(2)(i)(A-G) and (b)(2)(ii) items to non-government end-users located, or headquartered, in a country not listed in Supp. 3. This authorization is conditioned on a 30-day wait after submission of a classification request (except for (b)(2)(i)(B), per Note 2 to the (b)(2) introductory text).

This means that end-users for A and C-G items in a non-Supp. 3 country headquartered in a Supp 3 country are authorized with no wait but also conditioned on a 30-day wait, as are end-users in a Supp. 3 country headquartered in a non-Supp. 3 country.

It is recommended that “except no 30-day wait for such end-users who are located, or headquartered, in a Supp. 3 country" be added to the (b)(2)(i) and (ii) introductory texts.

7. Reference to 5A991

The Notes to 740.17(b)(4)(i) and 742.15(b)(4)(i) state that mobile communication equipment classified under 5A991.g implementing short-range encryption are not excluded from classification, registration, or self classification reporting. However, 5A991 is controlled only to E:1 countries and License Exception ENC for ECCNs 5x002 and NLR pre-requisites for ECCNs 5x992 do not apply to E:1 countries. Therefore, 5A991 is irrelevant to both 740.17(b)(4)(i) and 742.15(b)(4)(i).

It is recommended that these Notes be revised as follows:

> ... this paragraph (b)(4)(i) does not apply to any commodities or software that would still be classified under an ECCN in Category 5 requiring a license to more than E:1 countries 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~~ communications equipment classified under ECCN 5A001, when implementing cryptographic functionality controlled by Cateogry 5 Part 2 are not excluded from encryption classification, registration or self-classification reporting by this paragraph unless eligible for CIV under 5A001 or, if eligible for GBS and not for CIV, the importing country is not in Country Group D:1.

8. Financial exclusion from reporting

740.17(e)(1)(iii)(D) excludes from post-export reporting encryption items for banking or financial operations. This is excluded from 5A002 controls (and controlled instead under 5A992) by part (d) of the 5A002 decontrol Note. Including only this portion of the 5A002 decontrol Note in the list of reporting exclusions puts the status of the remainder of that Note in doubt.

It is recommended that either all or none of the 5A002 decontrol Note be included in 740.17(e)(1)(iii).

9. Unilateral mass market controls

742.15(b) intro and (b)(1) authorize immediate export once an encryption registration is submitted to BIS for mass market items exceeding 64 bits. But 742.15(b) intro disqualifies 740.17(b)(2) and (b)(3)(iii) items from this treatment and 742.15(b)(3) disqualifies the remainder of 740.17(b)(3). Even the registration requirement is arguably an "export control" prohibited by EAA section 5(c)(6) in the absence of a no foreign availability determination or on-going efforts to obtain multilateral control. Certainly the exclusion of all (b)(2) and (b)(3) items from the

Wassenaar Cryptography Note 3 mass market carve-out is such a prohibited “export control.”

It is recommended that;
unilateral mass market controls either be deleted or be moved temporarily to new unilateral ECCNs 5xX902; and
the United States seek Wassenaar coverage of what was moved to 5xX902.

10. Mass market classification requests

742.15(b) intro, the N.B. to Note 3 (Cryptography Note), 5A002 Related Controls, and 5D002 related controls refer to classification request (or classification by BIS) as an alternative to registration prior to export without a license of mass market items exceeding 64 bits. However, a classification request is required only if such mass market items are also described in 740.17(b)(2) or (b)(3). In that event, they do not qualify for this mass market treatment. Even the (b)(2) or (b)(3) treatment requires only submission of a classification and either no wait or wait 30 days, with no requirement for classification by BIS prior to export.

It is recommended that all references to classification request or classification by BIS with respect to mass market treatment be deleted.

>>> "Steve Bird (stbird)" <stbird@cisco.com> 8/20/2010 5:44 PM >>>
Subject: Cisco Comments Regarding the Regulatory Simplification

Randy,

Included below are Cisco's comments regarding the regulations published on June 25, 2010 compiled by Ken Nellis and Steve Bird.

We also included suggestions for future regulatory simplifications.

Cisco does very much appreciate the regulatory simplifications BIS published on June 25, 2010 and looks forward to working closely with BIS on subsequent regulatory simplifications.

Issues and Concerns

ECCN Categories

U.S. unilateral controls on 5A002 and 5D002 products present difficulties for U.S. exporters in the global economy.

A unification of the ECCNs would be helpful to U.S. exporters as there too many similar ECCN categories that do not distinguish separate regulatory requirements.

For example:

*   5A002/5D002 (restricted)

*   5A992/5D992 (current weak encryption, mass market, 740.17(b)(1) and 740.17(b)(3)

*   5A991/5D991 (non-encryption AT-controlled items)

The focus should be the controls on the suggested categories of ECCN above rather than focus on the varying encryption functionality in products. From an export control perspective, a mass market item, a 740.17(b)(1) and a 740.17(b)(3) item should share the same ECCN of 5A992 or 5D992 as the export controls on all of these items is virtually identical.

As another justification, the export controls on a mass market item and a 740.17(b)(1) or 740.17(b)(3) item are virtually identical but when transiting Hong Kong, Singapore or the UK, a license is required for the 740.17(b)(1)/(b)(3) items as a result of the associated ECCN of 5A002 or 5D002. This additional licensing burden on 740.17(b)(1) and 740.17(b)(3) controlled items in Hong Kong, Singapore and the UK presents U.S. exporters with a significant burden not experienced by non-U.S. exporters.

Cisco suggests that the Export Administration Regulations align more closely with the Wassenaar interpretation on encryption controls for 5A002/5D002 items.

Biannual Reporting

Eliminate the biannual report and institute a process that facilitates "as needed" requests associated with encryption products of concern to the U.S. Government.

Definition of Government end-user

Simplify the definition of government end-user. Currently, too much interpretation is required to determine licensing requirements.

Proposed Changes to 740.17(b)(2) Thresholds

Equipment listed below that implements:

* symmetric algorithms with key lengths exceeding 128 bits

* asymmetric algorithms exceeding 1024 bit public key modulus size,

or

* elliptic curve algorithms with key lengths exceeding 160 bits, for privacy of users' data

(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 128-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 90 600 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 250 400 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

Best regards,

Ken Nellis and Steve Bird

TechAmerica
WHERE THE FUTURE BEGINS
THE ASSOCIATION OF COMPANIES DRIVING INNOVATION WORLDWIDE

August 24, 2010

U.S. Department of Commerce
Bureau of Industry and Security
Regulatory Policy Division
14th and Pennsylvania Ave NW, Room H-2705
Washington, DC 20230

Re: 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

Dear Sir or Madam:

Thank you for the opportunity to comment on the interim final rule published on June 25, 2010 that amends encryption export control regulations for purposes of streamlining the authorization process for some encryption-related exports. TechAmerica represents 1500 high technology companies which must adhere to the very complex U.S. export control system.

In general, our members believe the new rule succeeds in providing procedural relief in some areas and, thus, represents a modest step toward a badly needed restructuring of the regulations. Unfortunately, the price of this incremental approach to reform is to sizably increase the complexity of the regulations while leaving the pre-existing encryption control structure largely intact.

It is our longstanding view that the encryption controls must be fundamentally recalibrated so that only a narrow list of encryption-related items is subject to the controls. With this predicate in mind, our members have provided the following detailed comments on the recently issued rule:

<u>Registration and Classification Process</u>

- Immediate export authorizations enabled through the new registration and classification process for less sensitive products represent an improvement over burdensome product review and post-export reporting requirements.
- This new process, however, does not alter encryption classifications for the many remaining covered products that can trigger onerous import/export controls in other countries.

- Moreover, the process provides no improvement for exports of widely available products like semiconductors, software development kits and network infrastructure products.

Reduction in Post-Export Reporting

- The removal of unilateral requirements for semi-annual post-export sales reporting for most unrestricted commodities, software, and components is a positive procedural improvement.
- This benefit, however, is eroded by the new requirement for an annual self-classification report.

Encryption Technology

- Making most encryption technology eligible for License Exception ENC is favorable, since it will eliminate the need for numerous license approvals and ELA's.
- It is not clear why standard technology for open cryptographic interfaces is excluded from ENC treatment, given its ubiquity.
- In the end, much widely available technology will still be subject to government end user restrictions and licensing to D:1 countries.

Note 4, Ancillary Cryptography

- The use of an ancillary cryptography note to distinguish what is classifiable under Category 5, Part 2 is very useful.
- However, as currently constructed, its utility is highly limited within the Information and Communications Technology (ICT) industry. For example, computers and related operating systems/components with ancillary encryption capability are not covered by the note. Similarly, networking (including office operation, administration, management, and provisioning) falls outside the scope of this note.

The foregoing comments reflect the modest stature of improvements contained in the new rule and, hence, reinforce the need for large-scale reform of encryption export control regulations. It is especially timely to pursue an overhaul of the regulations in light of the Administration's overarching export control reform initiative.

Four basic issues make encryption export control reform a compelling proposition. First, encryption regulations are complex to the point of being nearly unintelligible to all but those relatively few companies, law firms, consultants, and government officials that possess highly sophisticated and unique expertise in this arcane area. Convoluted regulations are not conducive to effective compliance.

Second, the scope of the encryption export controls is far too broad, especially in a world where standardized encryption is becoming a commodity feature of widely available ICT hardware and software. The wide berth of current controls runs counter to the Administration's goal of making export controls more effective by establishing a "system where higher walls are placed around fewer, more critical items."[1]

[1] Quotation from speech by Secretary of Defense Robert Gates before the Business Executives for National Security on April 20, 2010.

Third, many ICT products are subject to classification in Category 5, Part 2 for the sole purpose of having exporters provide the government with information on product capabilities and distribution patterns. Thus, ENC-Unrestricted items are variously subject to product review/post-export reporting or registration/self-classification reporting, but are not otherwise subject to export controls other than AT restrictions that broadly apply across the CCL in any case. By contrast, items subject to "actual" export controls for reasons of cryptographic capability are comparatively few in number as reflected by the particularized product categories referenced under 740.17(b)(2).

Fourth, the classification of products under Category 5, Part 2 outside of 5X992 can trigger the imposition of import and/or export controls in various countries. This extraterritorial consequence can occur even when items qualify for an ENC license exception in the U.S, resulting in heightened exposure to burdens and delays that can disrupt global supply chains.

TechAmerica recommends that the U.S. government address these issues in Phase 2 of its ongoing export control reform initiative by restructuring existing encryption export control regulations to deliver the following results:

- Applying encryption export controls solely to a narrow positive list of encryption items. Such a list should be kept narrow over time and regularly amended to reflect technological and global realities, including foreign availability and capability as well as controllability.
- Creating a viable alternative to government collection of product information that is decoupled from the export authorization process. The list of items subject to information collection requirements should be reduced to its lowest possible terms.
- Expanding mass market treatment to include any item with encryption capability that is, or will be, widely available or deployed, whether through retail or other channels. This would include efforts to broaden the scope of the General Cryptography Note.
- Ensuring that ICT items which do not have encryption capability as a primary function are classified outside of Category 5, Part 2 (or its equivalent within the tiered control architecture under development by the Administration.)

To facilitate consideration of these objectives, we have attached a list of detailed suggestions for a new encryption regulatory architecture that anticipates the Administration's conversion of existing control lists into a three-tiered hierarchy. The architecture is aligned with the Administration's goal of streamlining export controls to make them more effective. It also contains a specific mechanism for providing relevant product information to the government in manner that does not interfere with export activity.

In conclusion, while we are grateful for the incremental changes made, the new encryption rule falls far short of the fundamental reform sought by TechAmerica and implicitly contemplated within the Administration's transition to a streamlined, simplified export control system. We therefore stand ready to meet with BIS and others in the Administration in the soonest possible time frame to discuss our proposal for a new regulatory architecture applicable to encryption export controls.

Sincerely,

Ken Montgomery

Ken Montgomery
Vice President, International Trade Regulation
TechAmerica

TechAmerica

WHERE THE FUTURE BEGINS

THE ASSOCIATION OF COMPANIES DRIVING INNOVATION WORLDWIDE

Recommendations for Encryption Control Reform

Summary

TechAmerica has identified four key areas appropriate for encryption regulation revision. Part 1 of this paper proposes to establish a narrow positive list of encryption items subject to encryption controls. Part 2 of this paper recommends decoupling the export approval process from items for which the U.S. government only needs product information. Part 3 of this paper offers a plan to expand mass market treatment to any item with encryption capabilities where the item is, or will be, widely available. Part 4 of this paper suggests regulatory adjustments to ensure that items for which encryption capability is not their primary function are excluded from Category 5, Part 2. Part 5 of this paper proposes to remove from Category 5, Part 2 items that are transferred internally within a Wassenaar-headquartered company for internal use.

This document presents the following:

1. A table showing the proposed positive list of encryption items subject to control and accompanying rationale for control

2. A suggested format for a government-industry forum that would address the intelligence community’s equities as a substitute for the information collection process currently conducted through the export control system

3. Suggested language for revision of Note 3 to Category 5, Part 2 (the Cryptography Note)

4. Suggested language for revision of Note 4 to Category 5, Part 2 (the so-called “Ancillary Encryption” Note)

5. Suggested language for a new Note 5 to Category 5, Part 2

1. Proposed Items Subject to Control and Rationale for Control

The proposed positive list is based on the three-tiered approach articulated by the current administration.[1] We anticipate that as technologies mature, they will cascade down the tiered framework from higher control level tiers to lower control level tiers and may eventually move to EAR99. Table 1 below describes each tier.

Tier I contains those items with the highest sensitivity, often termed the "crown jewels." Tier I items are those designed for military use as described in the ITAR Munitions List in Category XIII(b).

Tier II contains items with an intermediate level of control. This includes the items currently in EAR section 740.17(b)(2), often termed the "restricted list," with two modifications as discussed in Table 1 below.

Tier III contains items with a low level of control. Items in section 740.17(b)(3), often termed "unrestricted, subject to technical review," provide the starting point for the Tier III list. Currently, exports of (b)(3) items require a classification request before immediate export to favorable treatment countries and a 30-day review prior to export to other countries. Tier III includes items currently in sections 740.17(b)(3)(ii)-(iv), which are controlled for reasons other than information collection (i.e., through the pre-export technical review and post-export reporting processes). Here, we have moved (b)(3)(i) items down one step in the cascading control tiers to EAR99. This is consistent with current regulations that place the least controls on (b)(3)(i) items as compared to the other (b)(3) items. For example, (b)(3)(ii) includes software and commodities utilizing non-standard cryptography, but its counterpart technology is currently singled out in the "restricted list" in (b)(2)(iv)(A). Unlike most other (b)(2) items, this technology is not authorized for License Exception ENC to non-Supplement No. 3 countries. In contrast, the (b)(3)(i) items have no such counterpart with this elevated "restricted list" status. Further, current regulations do not permit mass market treatment of (b)(3)(iii) items and impose post-export reporting requirements on (b)(3)(iii) items. In contrast, (b)(3)(i) items are currently eligible for mass market treatment and are not subject to the same post-export reporting requirements.

All other items not within Tiers I-III, including items currently in sections 740.17(b)(1) and (b)(4), fall into EAR99 unless described by an equivalent ECCN in Tiers I-III. For example, if microprocessors are subject to controls under the Tier III equivalent of 3A991, then they would continue to be controlled under the Tier III equivalent of 3A991, and not "cascade" down to EAR99. Since (b)(1) exports currently only require registration and an annual self-classification report, there is a better vehicle other than export controls to effectively collect

[1] See, e.g., Remarks by General Jones, National Security Advisor, "The Administration's Export Control Reform Plans," June 30, 2010.

product information. Thus, these items are logically removed from the export controls process. This is discussed further in the government-industry forum section in Part 2 of this paper.

The cascading nature of this tiered architecture allows controls to easily respond to technology lifecycles. For example, we have placed open cryptographic interface items currently in (b)(2)(iii) into Tier III and placed (b)(3)(i) items into EAR99. As new technologies emerge, we anticipate that the government will amend the items contained in each tier as necessary. This narrow positive list assists exporters in identifying the nature of controls related to their products and allows the government to maintain controls on those items of concern.

Table 1: Proposed Positive List of Encryption Items Subject to Control[2]

Tier	Description	Discussion & Example
Tier I "Crown Jewels"	Tier I items are described in the ITAR Munitions List[3] in Category XIII(b): Military Information Security Assurance Systems and equipment, cryptographic devices, software, and components specifically designed, developed, modified, adapted, or configured for military applications (including command, control and intelligence applications)…	The big word in this description is "military." "Dual-use" items are described in Tiers II and III. A Tier I example is a Type I cryptographic device such as a Motorola STU-III secure telephone.
Tier II Intermediate Controls	Tier II is based on the section 740.17(b)(2) list, with two modifications: 1) The first modification increases the aggregate throughput threshold for network infrastructure items in (b)(2)(i)(A)(1) from 90 to 600 Mbps. 2) The second modification removes (b)(2)(iii) open cryptographic interface items from Tier II.	The (b)(2) list represents those items BIS has identified as having a reason for which to control. The (b)(2)(i)(A)(1) throughput increase and (b)(2)(iii) removal are consistent with the foreign availability study certified by the Information Systems Technical Advisory Committee.[4]
Tier III Low Controls	Tier III includes section 740.17(b)(3)(ii)-(iv) items. Open cryptographic interface items in (b)(2)(iii) cascade down to Tier III from Tier II.	This list captures items that currently require a classification request for national security reasons. As discussed above, items in (b)(3)(i) currently enjoy the least controls and restrictions of items in the (b)(3) list. They are primarily included in (b)(3) for information collection purposes. Thus, (b)(3)(i) items are ripe for moving down the cascading controls to EAR99.
EAR99	Everything else would be classified under EAR99, unless it is described in another entry under Tier III. For example, if microprocessors are subject to controls under the Tier III equivalent of 3A991, then they would continue to be controlled under the Tier III equivalent of 3A991, and not "cascade" down to EAR99.	Items in (b)(1) currently only require registration and annual self classification reporting for information-gathering purposes and falls within the government-industry forum discussed in Part 2 of this paper.

[2] This document focuses on encryption reform. Category 5, Part 2 and ITAR Munitions List Category XIII(b) contain some items that are not encryption-related. See, e.g., ECCNs 5A002.a.4, a.7, and a.8. This document does not address these items.

[3] 22 C.F.R. § 121.1.

[4] Information Systems Technical Advisory Committee, "Report on Foreign Availability of Certain Encryption items," Nov. 12, 2009.

2. Government-Industry Forum

We propose creating a government-industry forum as a substitute for the information collection process currently conducted through the pre-export technical review, registration, self-classification, and reporting process.

The government-industry forum would feature the following characteristics:

a) The forum is jointly led by government and industry representatives. By taking a leadership role in the forum, both government and industry representatives will have a stake in and be fully committed to its success.

b) Participation is by invitation only. The forum is outside the Federal Advisory Committee Act[5] and its requirements. This is important in order to maintain full and candid sessions.

c) An outside third party separate from the intelligence community and industry coordinates the forum. This third party may be a Federally Funded Research and Development Center ("FFRDC") administrator,[6] such as Institute for Defense Analysis or MITRE Corp., which currently have or previously had contracts with the FBI to perform a similar function.

d) The forum includes U.S. and non-U.S. organizations. Participants may include companies not directly subject to the EAR process, but play a large role in industry. This could be expanded to include friendly governments (e.g., Canada) and companies incorporated in these countries (e.g., Research in Motion), making the forum even more useful than the current U.S. export control system for purposes of information collection and sharing.

One important responsibility of the forum is to create a viable alternative to the information-gathering framework currently handled by BIS through its reporting requirements. As discussed in Part 1 of this paper, we propose that certain encryption items currently controlled for information-gathering purposes be decoupled from the encryption export controls. This entity may operate by identifying trends in encryption technology and providing a forum in which valuable bilateral relationships can be forged between the government and specific industry participants for further, confidential, sharing of information.

The forum provides mutual benefits to both government and industry over the current review and reporting system administered by BIS. First, the forum provides a vehicle for NSA to obtain more information than is gathered through the current process. Since the forum includes non-U.S. entities, the government can have a dialog with entities that otherwise would not provide information through the EAR process. In addition, the current EAR process does not effectively

[5] 5 U.S.C. App. 2.

[6] For a list of FFRDC administrators, see http://www.nsf.gov/statistics/ffrdclist/. The third party administrator may be another suitable entity not on the list, such as Booz Allen Hamilton.

capture small U.S. companies that are developing innovative products using encryption features, but have not expanded sales or operations outside of the U.S.

Second, the forum provides a more efficient means for targeting valuable information. The current process is weighed down by an information overload where the government is collecting a large amount of non-useful and redundant information. The data is mined on the backend for small nuggets of critical information. This forum alleviates the inefficiencies in this process by focusing on collecting the desired information at the outset and drilling down to the specific target areas through dialog.

This government-industry forum serves to decouple NSA's information collection function from the government's export control functions, especially for items currently only requiring registration and self-classification. It provides NSA with the most efficient vehicle for performing more targeted information collection on a wider range of items. With industry participation, the government can more easily access timely information and anticipate advances in technologies. It also permits a two-way dialog between industry and government and provides industry with a platform for candid conversations with NSA.

There are other alternative methods for information collection that can be discussed as variants on this theme.

3. Revisions to Note 3 of Category 5, Part 2 (Cryptography Note)

We suggest the following revisions to Note 3 to Category 5, Part 2 (Cryptography Note):

Note 3: Cryptography Note: ECCNs 5A002 and 5D002 do not control:

(1) Items 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) that meet all of the following:

a. Generally available ~~to the public~~ by being sold, without restriction, ~~from stock~~ ~~at retail selling points~~ by means of any of the following:

1. Over-the-counter transactions;
2. Mail order transactions;
3. Electronic transactions; ~~or~~
4. Telephone call transactions; or

5. Commercial distribution channels through which the items are sold or will be sold in large volume;[7]

b. The cryptographic functionality cannot be easily changed by the user;

c. Designed for installation by the user without further substantial support by the supplier; and

d. 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) through (c) of this note~~.~~; or

(2) Components or software for items described in paragraph 1 to this Note 3.

~~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.~~

This revision eliminates N.B. to Note 3 and brings the language into the note's paragraph 1 preamble. This helps simplify the note.

The rationale for removing the reference to "the public" and "stock at retail selling points" is to eliminate ambiguous language and the reference to "retail," which historically served to confuse exporters.

The new Item 5 in sub-paragraph 1(a) and the new paragraph 2 seek to address the issue that some components and software of mass market items do not themselves qualify for mass market treatment and some non-retail distribution channels lead to identical wide-spread availability. These additions expand the distribution channel list to include multi-tier distribution channels and Original Equipment Manufacturer distribution, which lead to wide-spread availability of general purpose and non-customized products. The semiconductor industry is particularly impacted by the current distribution channel language because its products are not generally sold through traditional retail channels. Further, many integrated circuits use the same publicly available encryption algorithms used in software that does qualify for mass market treatment since the software is sold through retail channels. Thus, semiconductors could qualify for mass

[7] While there may be flexibility in defining the terms "commercial" and "large volume," our understanding of these terms is to include such distribution channels as OEM and multi-tier distribution.

market treatment with an update to Note 3 that equitably accounts for non-retail large-volume distribution.

Further, the components or software of mass market items may not currently qualify for ancillary treatment under Note 4 either. For example, the operating system for a smartphone may fall into this category. Similarly, Application-Specific Integrated Circuits (ASICs) for smartphones may fall into this category. This Note 3 revision covers these items that otherwise fall through the cracks of Notes 3 and 4.

In addition, BIS has historically included software and components in similar treatment as commodities. For example, the former ENC retail encryption designation did not separate software and components.[8]

4. Revisions to Note 4 to Category 5, Part 2 (the so-called "Ancillary Encryption" Note)

We suggest the following revisions to Note 4 to Category 5, Part 2 (the so-called "Ancillary Encryption" Note):

Note 4: Category 5, Part 2 only applies to items where:

1. Their primary function is "Information security"; and
2. Such items otherwise would be controlled under Category 4, Category 5, Part 1, or Category 7.

~~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);~~

[8] See, e.g., 15 C.F.R. § 740.17(b)(3) between 2001 and 2004.

~~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.~~

The rationale for the revisions is to identify with positive language those items controlled by Category 5, Part 2 and to more fully capture the spirit of "ancillary encryption" by excluding certain items for which their core functionality is not information security. Items excluded from Category 5, Part 2 by Note 4 should still be evaluated under other categories of the CCL.

This revision presents a more realistic approach to the current technology landscape. Data storage, computing, data transmission, and networking products increasingly require the security features that encryption provides. As more devices are networked, there is a ubiquitous need for standard commercial encryption features in everyday computing and telecommunications devices so as to protect personal data. Thus, Category 5, Part 2 will inevitably swallow much of Category 4 and Category 5, Part 1. For example, the semiconductor industry is currently moving toward utilizing encryption features in standard commercial products. These products will find themselves re-controlled when they incorporate the encryption features.

This Note 4 revision does not exclude Category 7 items because BIS may have an interest in controlling certain airborne communications items in Category 5, Part 2.

This revision also presents a more focused and clearer approach to controlling cryptographic products. Exporters must currently identify each vendor's encryption components and functions, which may not fully be known by either the vendor or enforcement authorities. By continuing to control some ancillary encryption, exporters are reluctant to rely on vendors using the new self-classification process in fear of potential violations. As a result, exporters still require vendors to supply BIS classifications even when the vendors merely supply ancillary components. Thus, the current classification scheme falls short of its intended goal of reducing filings. This clearer "Ancillary Encryption" Note resolves the abovementioned issues and allows exporters to easily identify those products for which BIS classification is required.

5. New Note 5 to Category 5, Part 2

We suggest adding a new Note 5 to Category 5, Part 2:

Note 5: Category 5, Part 2 does not apply to items transferred within a company and meeting all of the following:

1. The company is headquartered in a Wassenaar member country; and
2. The transfer is for internal use only.

The rationale for this new note is to turn the authorization section 740.17(a)(2) grants to U.S. companies into a Wassenaar authorization. Although section 740.17(a)(2) is intended to allow U.S. companies to develop freely without the need for specific authorizations until the product is ready for distribution outside the U.S. company, it does not have that full effect in practice. Today, U.S. companies with global product development cannot fully utilize this provision due to the complexities of compliance with local country export regulations. For example, countries such as Canada and the U.K. require individual authorizations to share cryptographic source code within a company when subsidiaries in certain countries would be involved in the development process. Adding this as a note to Category 5, Part 2 allows U.S. and other Wassenaar member state companies to fully realize the efficiency offered by section 740.17(a)(2).

For additional information, please contact:

Ken Montgomery
Vice President, International Trade Regulation
TechAmerica
Ken.montgomery@techamerica.org
202-682-4433

SIA | SEMICONDUCTOR INDUSTRY ASSOCIATION

August 24, 2010

Ms. Sharron Cook
U.S. Department of Commerce
Bureau of Industry and Security, Regulatory Policy Division
14th Street and Pennsylvania Avenue, N.W.
Room H–2705
Washington, DC 20230

Subject: RIN 0694–AE89

Re: Request for Public Comment on 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 (75 Fed. Reg. 36,482)

Dear Ms. Cook:

The Semiconductor Industry Association ("SIA") is the trade association representing the U.S. semiconductor industry. Founded in 1977 by five microelectronics pioneers, SIA unites over 60 companies that account for nearly 90 percent of the semiconductor production of this country.

Interim Final Rule

The recent interim final rule amending the encryption controls in the Export Administrating Regulations ("EAR") contained positive changes in several areas. In particular, it: (i) eased the licensing requirements for the export and reexport of certain types of technology necessary for the development and use of encryption products, (ii) removed the requirement to file separate encryption classification requests with both the Bureau of Industry and Security ("BIS") and the ENC Encryption Request Coordinator, (iii) implemented the agreements pertaining to "information security" items made by the Wassenaar Arrangement at the plenary meeting in December 2009 and (iv) added a new definition for "non-standard cryptography."

While generally constructive, these changes primarily address administrative details as opposed to producing substantial reforms. The changes provide procedural improvements that affect various product categories, although they do little or nothing to improve the functioning of export controls applicable to semiconductor devices with encryption capability. More importantly, the amended regulations do not address the principal issues related to the control of these devices.

The EAR and its license requirements continue to apply to a large number of semiconductor devices that contain encryption functionality. At the same time, a number of exemptions and license exceptions are made applicable for these products, usually with a mandatory government classification determination and an obligation to submit product reviews and provide other reporting to U.S. officials. The end result is a complicated control regime in which ultimately there are few license applications, but extensive classification actions and wide-spread review and reporting requirements.

As currently structured, many sections of the EAR exist only to remove controls placed unnecessarily on broad categories of civilian items that are captured by Category 5, Part 2 of the Commerce Control List ("CCL"). To SIA, this calls out for substantial reform and simplification of encryption export controls.

Finally, the semiconductor industry must deal with the international repercussions of a U.S. encryption classification of its products. Many countries impose encryption controls on products based on their U.S. classification. Most U.S. semiconductor components that contain encryption are classified under ECCN 5A002, a classification that is subject to export licensing and often import controls by foreign countries. Foreign controls are applied on U.S. semiconductor components even when these components would qualify for license exception under the EAR. This is due to the fact that U.S. license exceptions for encryption items are not recognized in many foreign jurisdictions.

This imposition of foreign license requirements based on a U.S. export classification for which ultimately no U.S. license is required is illogical and unnecessary; it can, however, be particularly burdensome for U.S. companies operating overseas. This is yet another reason why SIA urges BIS to undertake prompt reform of encryption export controls on integrated circuits.

Develop a Positive List

SIA supports the Administration's efforts reportedly underway to combine the CCL and the U.S. Munitions List ("USML") into a single positive list structure. It is our understanding from Administration statements that such a single control list would maintain controls on defense articles in a top tier, with specific dual-use items set forth in lower tiers. SIA members believe that this positive list approach should apply to semiconductors with encryption as follows:

Top Tier Munitions Items

SIA maintains that semiconductors or integrated circuits should not qualify as defense articles, whether or not such devices contain encryption capability. These devices are merely electrical connections. They have no inherently military function, and the presence of encryption capability does not alter this fact. At most, they can serve as a component of an end-item or defense article.[1]

Lower Tier Dual-Use Encryption Items

Unlike the current structure of Category 5, Part 2 of the CCL, which identifies broad classes and categories of items related to information security, SIA believes that a lower tier of a unified, positive control list should, instead, identify particular devices that merit inclusion on a control list based on their specified properties, functions and capabilities.

SIA recommends that the Administration begin the creation of a positive list of integrated circuits containing encryption with a blank slate. A positive list for encryption items should then identify only those items – including semiconductor devices and components – that merit inclusion based upon their peculiar technical specifications and encryption-related technical properties and capabilities. The list should be objective and transparent. The mere inclusion of encryption functionality in any product should not be grounds for inclusion on such a positive list. Devices and components containing only standard encryption, or that are currently not subject to licensing requirements, classification review or post-export reporting, should not qualify for inclusion on a positive list.

Detach Information Gathering from Encryption Export Controls

SIA recommends that BIS detach export control requirements from information gathering with respect to semiconductor devices. SIA member companies are prepared to cooperate with the U.S. government with respect to encryption capabilities. However, SIA believes that the information gathering mechanism should stand apart from the export control regime.

Separating review and report requirements from export controls would (i) eliminate controls on many civilian items that the U.S. government does not intend to control for export, (ii) reduce the need for complex exemptions and license exceptions,

[1] If a particular integrated circuit is to be included in the top tier of a positive list in a “catch-all” category for components of a defense article (e.g., Category XV(e) or its future equivalent), the integrated circuit should at least be “specifically designed” for inclusion in the defense article. The inclusion of a commercial-off-the-shelf integrated circuit in a defense article should not be sufficient for its inclusion on a positive munitions list.

“Specifically designed” should be clearly distinguished from simply “designed.” A specifically designed item should have a singular purpose and not be readily susceptible to use in multiple applications. The ability to perform a particular function or application does not equate to a special or peculiar design for that application. Specifically designed requires particular action and intent on the part of the designers. It must be directly and uniquely related to the munitions or military function of the defense article. A positive list should make explicit that “specifically designed” cannot mean merely “capable of.”

and (iii) add consistency to the overall export control system, while not preventing the government collection of information that it determines is necessary to protect national security.

Alternative or Interim Steps to Reform Encryption Controls on Semiconductors

SIA recognizes that in lieu of a streamlined, positive export control listing of integrated circuits with encryption there are other regulatory changes that would substantially reduce unnecessary export controls on semiconductor devices and components. SIA also recognizes that the creation and implementation of a positive list may take a long time to complete. In these circumstances, and because of the urgent need for regulatory reform of encryption export controls on integrated circuits, SIA supports, alone or in combination, alternative or interim regulatory changes along the following lines:

- eliminate general purpose semiconductor devices from inclusion in Category 5, Part 2;
- eliminate encryption controls on semiconductor devices and components that utilize or incorporate “standard cryptography”;
- extend “no license” treatment to semiconductors distributed through broad distribution channels and in high volume; and
- revise the so-called “Ancillary Encryption” Note to include semiconductor devices whose primary purpose or operation is not encryption.

<u>Eliminate General Purpose Semiconductors from Inclusion in Category 5, Part 2</u>

SIA has long recommended the elimination of encryption and national security controls – but not anti-terrorism controls – on general or multiple purpose semiconductors that use or are dedicated to publicly available encryption algorithms that cannot be easily changed by the end-user and are generally available by being sold without restriction.

“General purpose” is a standard and well understood industry demarcation. It ensures the semiconductor device is not specialized or customized for encryption or an encryption infrastructure that characterize military or government applications. Instead, it consists of broad-based components that can serve multiple functions and are generally incorporated into mass market consumer products or commercial information infrastructure. General purpose semiconductor devices are overwhelmingly deployed in civilian personal and commercial applications and with minor exceptions are exported license-free.

The mere inclusion of encryption functionality in a general purpose integrated circuit should not lead to its control as an encryption item, and as such, it should not qualify under Category 5, Part 2. Instead, general purpose semiconductor devices should be controlled under the CCL category they would otherwise be subject to in the absence of encryption (e.g., ECCN 3A991). Such a change would maintain anti-terrorism and military end-use/end-user controls on semiconductor devices, while not imposing unnecessary new controls due to encryption.

Submitted as Attachment A to this response is an SIA white paper elaborating on why the encryption regulations need to be rebalanced to reflect the significant changes in the last decade, including the growing commodity nature of encryption in integrated circuits and the increased civilian need for information security.

Eliminate Controls on Semiconductor Devices that Utilize or Incorporate "Standard Cryptography"

SIA recommends that BIS eliminate encryption controls on semiconductor devices that utilize or incorporate standard cryptographic algorithms or protocols (i.e., encryption algorithms or protocols that have been adopted or approved by a duly recognized international standards body). Standard cryptographic algorithms and protocols that are publicly available – and in many cases, have been in use for nearly a decade – should no longer be considered worthy of control.

Extend Mass Market Treatment to Widely Distributed Semiconductors

Although a semiconductor may be sold in the millions, it is currently not eligible for mass market treatment because the commercial channels through which it is sold do not qualify as "retail." However, once a semiconductor is installed in a mass market end-product – the point at which the semiconductor device begins to provide some functionality – it loses its individual character and should fall outside of the export control regime.

In these circumstances, and just as it has done for encryption software, BIS should grant mass market treatment to semiconductors with encryption which are intended for use in mass market products and/or generally or widely available to the public through any commercial means of distribution.

Revise Note 4, the So-Called "Ancillary Encryption" Note

SIA recommends revising Note 4 in Category 5, Part 2, the so-called "Ancillary Encryption" Note, so that semiconductor components, whose main function is not encryption-related, qualify for exclusion from control under ECCN 5X002. General and multiple-purpose semiconductors that have long been eligible for export without a license are being controlled under Category 5, Part 2 due to the inclusion of encryption. The inclusion of encryption functionality into these devices does not and should not alter what the U.S. government perceives the devices' primary function to be and should not result in the addition of new controls.

*   *   *

SIA appreciates the opportunity to comment on the recent regulatory change and looks forward to continuing its cooperation with BIS on more fundamental reform of encryption controls on semiconductors. Please feel free to contact the undersigned or its counsel, Clark McFadden, if you have questions regarding these comments.

Cynthia Johnson	
Cynthia Johnson Co-Chair, SIA Trade Compliance Committee	David Rose Co-Chair, SIA Trade Compliance Committee

Enclosure

Attachment A

ENCRYPTION REFORM FOR SEMICONDUCTOR EXPORT CONTROLS

Semiconductor Industry Association
Trade Compliance Committee

March 12, 2010

For further information contact:

David W. Rose
Co-Chair, SIA Trade Compliance Committee
Intel Corporation
1634 I Street, NW, Suite 300
Washington, DC 20006
(202) 626-4390

Cynthia Johnson
Co-Chair, SIA Trade Compliance Committee
Texas Instruments Incorporated
1455 Pennsylvania Avenue, NW, Suite 375
Washington, DC 20004
(202) 220-9469

Daryl G. Hatano
Semiconductor Industry Association
181 Metro Drive, Suite 450
San Jose, CA 95110
(408) 436-6600

Counsel: Dewey & LeBoeuf LLP
W. Clark McFadden II
Stephen J. Lita, Trade Specialist
1101 New York Avenue, NW
Washington, DC 20005
(202) 346-8000

TABLE OF CONTENTS

We will double our exports over the next five years, an increase that will support two million jobs in America. To help meet this goal, we're launching a National Export Initiative that will […] reform export controls consistent with national security.

President Barack H. Obama
State of the Union Address
January 27, 2010

First, we're going to streamline the process certain companies need to go through to get their products to market – products with encryption capabilities like cell phone and network storage devices. Right now, they endure a technical review that can take between 30 and 60 days, and that puts that company at a distinct disadvantage to foreign competitors who don't face those same delays.

President Barack H. Obama
Remarks at the Export-Import Bank's Annual Conference
March 11, 2010

I. Executive Summary

Global commerce and the interaction among individuals are increasingly dependent upon information in digital form. People use vast public and private networks, like the Internet, to make information broadly accessible throughout the world. Security – protection from theft, diversion or unauthorized access – is essential for much of this information. Encryption is the primary means to achieve this security.

Recognizing the need for encryption to protect commercial and private information, the Clinton Administration created in 1996 an export license classification for mass market encryption based on its sale at retail, at the time the avenue by which most commercial encryption was sold. Although not without some risk, the granting of special treatment for mass market products with encryption was an acknowledgement that such encryption is not worthy of control and effective control is not feasible.

Because most semiconductors are not sold through retail outlets, mass market treatment has not been available to them. Indeed, the anomalous result is that encryption in software can qualify for mass market treatment, but the very same encryption in a semiconductor cannot. This disparity will not be sustainable as technology makes encryption virtually a cost-free commodity feature when embedded in a high-volume semiconductor.

The export licensing process for encryption creates several burdens for semiconductor companies, from extended product reviews to reporting requirements. It also subjects semiconductor devices to even more comprehensive encryption controls in other countries. This constrains the competitiveness and innovation of the U.S. electronics industry with no perceptible national benefit.

Most of the problems and burdens that handicap the export of semiconductors with encryption can be eliminated with an adjustment in the regulatory classification of integrated circuits. Accordingly, **the Semiconductor Industry Association ("SIA") proposes to eliminate encryption and national security controls – but not anti-terrorist controls – on general or multiple purpose integrated circuits that use or are dedicated to publicly available encryption algorithms that cannot be easily changed by the end-user and are generally available by being sold without restriction.**

"General purpose" is a standard and well understood industry demarcation. It ensures the device is not specialized or customized for encryption or an encryption infrastructure that characterize military or government applications. Instead, it consists of broad-based components that are incorporated into mass market consumer products or commercial information infrastructure.

By limiting the encryption algorithms to those that are publicly available, the SIA proposal does not go beyond the scope of current mass market encryption treatment.

In short, the proposed classification is a necessary rebalancing that reflects the changes in the last decade in the civilian need for information security and is consistent with the existing terms, rationale and risks inherent in mass market treatment for encryption.

II. Introduction

At the end of the Cold War, SIA called for a new calculus that would fundamentally alter the treatment of information technology under U.S. export controls. The changing threat to national security, the decentralization and dispersion of information technology, the competitive constraints on U.S. industry from unilateral export controls and the national interest in promoting global commerce and democracy in free markets all weighed in favor of the liberalization of export controls on information technology.

The ensuing changes in U.S. export controls took many forms. With few exceptions, memory devices and microprocessors became exempt from export license requirements. This liberalization stemmed in large part from the massive proliferation of semiconductors worldwide and the products that utilized them.

After almost 40 years of U.S. export controls on encryption technology, the first major change occurred in the late-1990s with, among other things, the creation of a license exception for certain products and software containing encryption. The encryption export control changes represented a major departure from a case-by-case licensing requirement for encryption items based exclusively on technical characteristics. The new encryption export controls acknowledged that certain products and software containing encryption were not worthy of control and such control was not feasible. But since the granting of special treatment for mass market items over a decade ago, there have been no other substantial changes in export controls on encryption items.

During this same period, the trend toward deployment of encryption items has accelerated dramatically. Activity on the World Wide Web has exploded; electronic storage of data of all types is now on a scale previously unimaginable; and strong encryption is readily available throughout the world. At the same time, the need and the commercial demand for privacy and security with respect to information has grown commensurately.

Of particular significance and as a result of ever increasing capability and capacity, semiconductor devices of all types today can readily accommodate encryption, thereby providing – broadly and inexpensively – the privacy and security that the commercial market demands. In these circumstances, fundamental change is again necessary in the export control treatment of encryption.

III. Structure of U.S. Encryption Export Controls

U.S. export controls on encryption products and software no longer have a military focus. Throughout the majority of the 20th century, encryption was primarily the domain of governments, because governments were (i) virtually the only entities that had a need for highly secure communications and (ii) the only entities that had the interest and resources to develop sophisticated encryption and decryption capabilities, e.g., high performance computing capabilities.

Because encryption was primarily used by governments to achieve military and foreign policy ends, all encryption products and software were deemed to be specifically designed or modified for a military end-use. Encryption items were classified as defense articles and subject exclusively to the U.S. Munitions List ("USML") under "cryptographic devices and software" of Category XIII – Auxiliary Military Equipment.[1] Encryption products remained subject to USML control throughout the Cold War and case-by-case licensing was required for exports of encryption items.

Throughout the 1970s and 1980s, businesses increasingly used computers, particularly mainframe computers and servers, in their day-to-day operations. With the expansion of the business and personal computing industries, the need for information security grew steadily and the dual-use characteristics of encryption became apparent.

By the 1990s, technology advanced such that vast amounts of digital information could be quickly generated, transferred and stored. The widespread adoption of the Internet by the end of the 1990s led to the global transmission of large volumes of commercial and personal electronic data. Based on a comprehensive analysis of the security needs of an information society, a committee of the National Academies of Science found "that the current national cryptography policy is not adequate to support the information security requirements of an information society."[2]

Beginning in 1996, with action initiated by the Clinton Administration,[3] U.S. export controls on encryption underwent an overhaul. The rationale for major changes derived from recognition that strong encryption is needed to protect sensitive information in the private sector "if the great promise of the electronic age is to be realized."[4] The Clinton Administration expressed its support for electronic commerce by permitting "the export of strong encryption when used to protect sensitive financial, health, medical, and business proprietary information in electronic form."[5]

In response to the growing need for civil uses of encryption and "in order to provide for appropriate controls on the export and foreign dissemination of encryption products," President Clinton moved encryption products from Category XIII of the USML and placed them on the Commerce Control List ("CCL").[6]

[1] 22 C.F.R. § 121.1 (2009). USML Category XIII (b) is a basket category that also includes other items unrelated to cryptography.

[2] Cryptography's Role in Securing the Information Society, K. W. Dam and H. S. Lin (Eds.), *Committee to Study National Cryptography Policy, National Research Council*, 1996, p. 6.

[3] See Exec. Order No. 13026, 3 C.F.R. 228 (1997); and Encryption Items Transferred From the U.S. Munitions List to the Commerce Control List, 61 Fed. Reg. 68,572 (Dec. 13, 1996).

[4] The White House Office of the Press Secretary, Administration Announces New Approach to Encryption, September 16, 1999, *available at* http://clinton6.nara.gov/1999/09/1999-09-16-statement-by-press-secretary-on-new-approach-to-encryption.html.

[5] See The White House Office of the Press Secretary, Administration Updates Encryption Policy, September 16, 1998, *available at* http://clinton6.nara.gov/1998/09/1998-09-16-statement-by-the-press-secretary-on-encryption-policy.html.

[6] See Exec. Order No. 13026 3 C.F.R 228 (1997); and Encryption Items Transferred From the U.S. Munitions List to the Commerce Control List, 61 Fed. Reg. 68,572 (Dec. 13, 1996). Encryption items incorporated into

The centerpiece of the reform was the establishment of a new license exception "ENC" and a procedure to obtain a mass market encryption classification. Under License Exception ENC, encryption items avoid an export license requirement but had to undergo a 30-day review and confirmation of eligibility for the license exception by U.S. officials with follow-on semi-annual reporting requirements. In contrast, if an item met the criteria defined for mass market treatment and was reviewed and classified by the U.S. officials as such, it could be freely exported to most countries. Encryption and national security controls were eliminated for items qualifying for mass market treatment. Only anti-terrorism controls remained.[7]

Further changes to export controls on encryption included implementing policies for distribution of encryption to banks and financial institutions;[8] the granting of special treatment to the U.S. subsidiaries, online merchants and certain other end-users;[9] and the relaxation of controls for encryption with a key recovery feature.[10]

The apparent rationale for mass market treatment was to differentiate between security specific items for special environments or end-users and the broad, general purpose encryption products that were utilized by the public without on-going support. Mass market items were determined to be items sold to consumers "off the shelf." See Table 1.

Table 1
Criteria for Mass Market Treatment

a. Sold from stock at retail selling points, without restriction, by means of:

   1. Over the counter transactions;
   2. Mail order transactions; or
   3. Telephone call transactions; and

b. Designed for installation by the user without further substantial support by the supplier.

Although this change constituted a major breakthrough for exporters of products and software incorporating encryption, mass market treatment was then, and remains today, limited

defense articles or specifically designed, developed or modified for defense articles or applications remained on the USML.

[7] Encryption Items Transferred From the U.S. Munitions List to the Commerce Control List, 61 Fed. Reg. 68,572 (Dec. 13, 1996); and Revisions to Encryption Items, 65 Fed. Reg. 2,492 (Jan. 14, 2000).

[8] Encryption Items, 63 Fed. Reg. 50,516 (Sept. 22, 1998).

[9] Encryption Items, 63 Fed. Reg. 72,156 (Dec. 31, 1998).

[10] Id.

to consumer end-products "sold from stock at retail selling points."[11] The result is that mass market treatment has provided almost no relief to the U.S. semiconductor industry over the ensuing years, because while semiconductor devices (e.g., microprocessors, microcontrollers and memory) are sold in massive quantities (hundreds of millions of items per year), and are present in nearly all information products used by the public, semiconductor devices are not typically sold through retail outlets. Instead, semiconductors serve only as components, which are sold primarily, on an indirect or direct basis, to original equipment manufacturers ("OEMs").

Instead of receiving mass market treatment, components such as semiconductors are eligible for the ENC license exception to most destinations with a variety of restrictions, which as stated above, include the submission of the semiconductor components to U.S. officials for review at least 30 days prior to export with semi-annual post-export reporting requirements.

IV. Changes in Commercial Needs for Encryption

Information technology has changed dramatically since the mid-1990s, and proliferation, decentralization and dispersion of information technology has driven the commercial demand for privacy and security.

A key enabler of this proliferation of information technology is the Internet. Since its privatization in the 1990s, the Internet has become critical to the global economy.[12] More than a billion people use the Internet worldwide and it now underpins a range of economic activities, touching "practically everything and everyone."[13]

Worldwide, the number of individual networks – autonomous systems such as those managed by AT&T and Google – that connect to the Internet grew to 26,000 in 2007, up from 3,000 in 1997, demonstrating the increasing importance of Internet connectivity to businesses.[14] In 2008, there were 540 million Internet hosts – a computer or device connected to the Internet and uniquely identified with an Internet Protocol (IP) address – as against 30 million in 1998; 33 million web servers (i.e., computers that serve content, such as web sites) connected to the Internet, as against two million in 1998; and 168 million domain name registrations, as against 25 million in 2000.[15] These are growth rates of 767 percent, 1,700 percent, 1,550 percent and

[11] Id.

[12] The White House Office of the Press Secretary, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, April 17, 2009, at Preface.

[13] "The Future of the Internet Economy," *Organization for Economic Co-operation and Development Policy Brief*, June 2008, p. 1; and The White House Office of the Press Secretary, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, April 17, 2009, pp. iii, Preface, 1, 31 *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

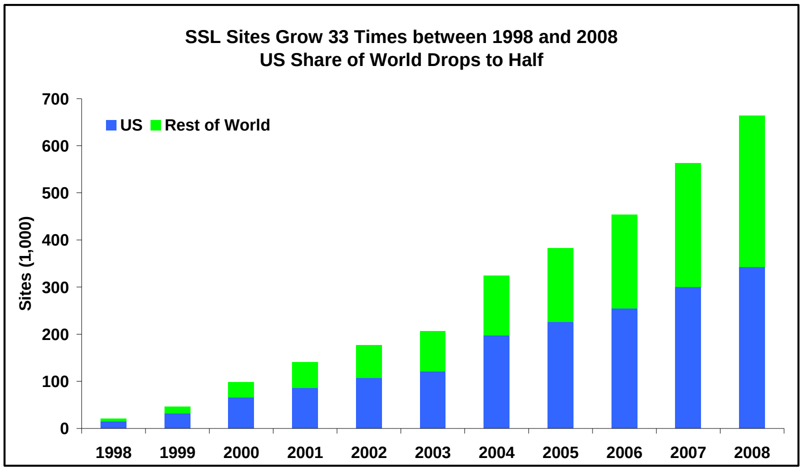
[14] "OECD Communications Outlook 2009," *Organization for Economic Co-operation and Development* (2009), p. 148 and following.

[15] Id.

572 percent, respectively. In the United States alone, some 79 percent of the U.S. adult population had used the Internet in some fashion in 2009, up from 14 percent in 1995.[16]

In addition, the ever-improving capabilities of digital voice and data communication, over both wired and wireless networks, have greatly expanded the ability of businesses, individuals and governments to digitally store, retrieve and transfer vast amounts data from almost anywhere on the planet. The generation and transmission of data are massive and growing without constraint.[17] According to Cisco Systems, Inc., by 2013, the amount of traffic flowing over the Internet annually will reach 667 exabytes.[18] Continuing advances and the convergence of information and communication technologies has led to the emergence of "cloud computing," whereby individuals and businesses increasingly generate, store and transmit data remotely.

The ability to effortlessly generate, store and transmit vast amounts of private, confidential and classified digital information has driven efforts to protect this information from unauthorized access or diversion, including by hackers, criminal organizations, industrial competitors and adversarial governments. This has created a commercial information security market that generates between $14 billion and $79 billion annually in revenues, depending upon measurement conventions.[19]



Information security is particularly relevant for e-commerce and banking. Today, approximately 50 percent of the population of U.S. Internet users makes purchases online or banks online.[20] The result is a growing commercial demand for security protection through the use of encryption. In 2008, there were 660,000 secure servers connected to the Internet, as

[16] "Internet, Broadband and Cell Phone Statistics," *Pew Internet and American Life Project Series*, various.

[17] <u>See</u> "Data, Data Everywhere: A Special Report on Managing Information," *The Economist*, February 27, 2010.

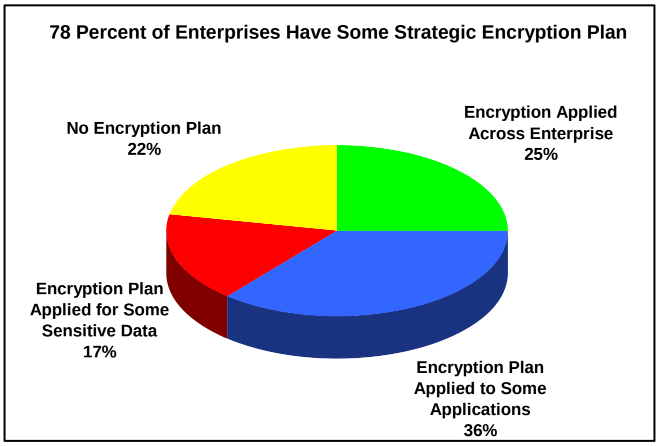
[18] "Cisco Visual Networking Index: Forecast and Methodology, 2008-2013," Cisco Systems, Inc., June 9, 2009. An exabyte is a billion billion, or ten to the 18th power, bytes.

[19] "Gartner Says Worldwide Security Software Market on Pace to Grow 8 Percent in 2009," *Gartner Dataquest*, September 21, 2009 and "Information Security Market Forecast to Reach $79 Billion by 2010," *Military Aerospace Electronics*, July 18, 2007.

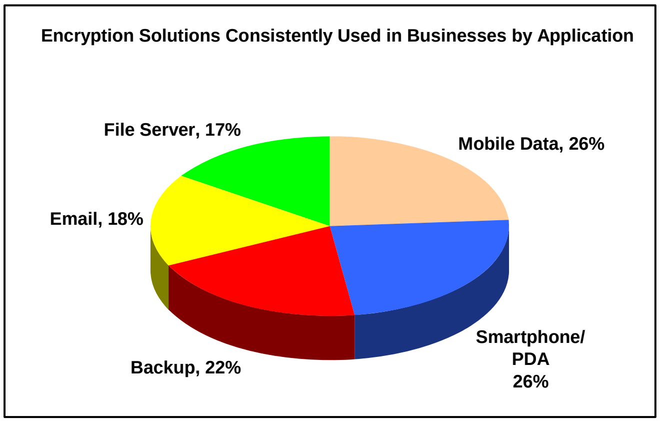
[20] "Internet, Broadband and Cell Phone Statistics," *Pew Internet and American Life Project Series*, various and "Online Banking: Surfing to the Bank," *Pew Internet & American Life Project*, June 14, 2006.

against approximately 20,000 in 1998.[21]

Secure sockets layer (SSL) sites, which are used for e-commerce, online banking and other financial services provide security by allowing an encrypted connection between server and browser.[22] These sites are increasingly operated from outside of the United States. In 1998, the United States accounted for 72 percent of the world total, but by 2008, that share had dropped to approximately half.[23]



In turn, businesses increasingly seek encrypted solutions. By most measures, encryption use by enterprises is up significantly. According to surveys by information security consultants PricewaterhouseCoopers and Deloitte Touche Tomatsu, over 50 percent of the business populations surveyed used some form of encryption in recent years.[24]



More focused surveys suggest even higher usage rates. According to InformationWeek Analytics, some 86 percent of organizations surveyed used some level of encryption in 2009, while 78 percent were developing longer-term strategic plans for various uses of encryption within their organizations.[25] These businesses are consistently using encryption to secure mobile data (26 percent of respondents), peripheral telecommunications devices such as smart phones and personal digital assistants (26 percent), stored data (22 percent), servers (17 percent) and email (18 percent).[26]

[21] "OECD Communications Outlook 2009," *Organization for Economic Co-operation and Development* (2009), p. 151.

[22] "OECD Communications Outlook 2009," *Organization for Economic Co-operation and Development* (2009), p. 151.

[23] Id., p. 173.

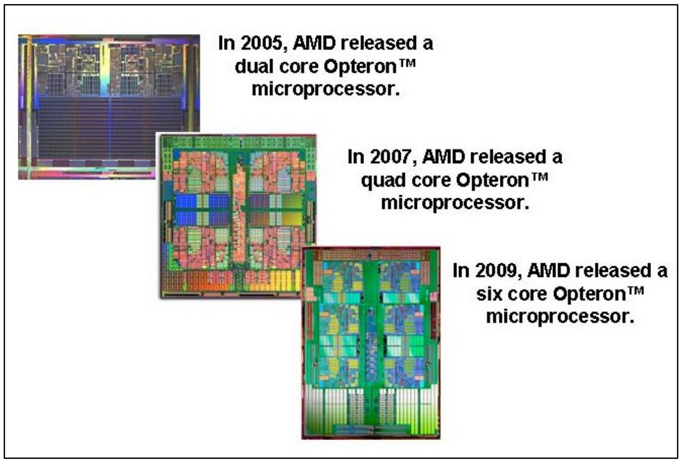
[24] "Losing Ground," *2009 TMT Global Security Survey*, p. 21 and "The Global State of Information Security," *2009 Global Information Security Survey*, p. 6 and *2008 Global State of Information Security Survey*, p. 14.

[25] "Encryption in the Enterprise," *InformationWeek Analytics*, November 2009, p. 8 and "2009 Annual Study: US Enterprise Encryption Trends," *Poneman Institute*, July 2009, p. 9.

[26] "2009 Annual Study: US Enterprise Encryption Trends," *Poneman Institute*, July 2009, p. 15.

Due to continuing advances in semiconductor technology, semiconductor devices can increasingly incorporate various advanced encryption capabilities. The number of transistors that are placed on an integrated circuit doubles approximately every two years. This scaling, also referred to as Moore's Law, allows semiconductor manufacturers to increase the performance of products in all areas while decreasing costs. The inclusion of added features can be seen in the addition of cores to high volume, general purpose microprocessors roughly every two years.[27]

In addition to processor cores, semiconductor companies are able to add a variety of new features to product dies including cache memory, controllers, digital signal processors, microcontrollers or integrated graphics. Semiconductor manufacturers sell devices that integrate several components of a computer or electronic device on a single integrated circuit, known as a system-on-a-chip ("SOC"). Scaling and the development of SOC technology has meant that semiconductor manufacturers can now manufacture devices with strong encryption, without altering the size or function of their products or significantly increasing costs.


In 2005, AMD released a dual core Opteron™ microprocessor.
In 2007, AMD released a quad core Opteron™ microprocessor.
In 2009, AMD released a six core Opteron™ microprocessor.

A. *Strong Encryption Can Be Incorporated into Semiconductor Devices*

In response to global demand for strong encryption and other security features, U.S. semiconductor manufacturers and designers have already started and will continue to incorporate encryption functionality in high volumes of semiconductor devices over a broad range of commercial applications. Because of the ease with which encryption is added to semiconductor devices, such encryption can utilize powerful standardized forms of encryption that have developed around the world (e.g., the Advanced Encryption Standard ("AES")).[28] Adoption of standardized encryption has long been encouraged by the U.S. government.[29]

[27] One reason hardware encryption has only now become common place was the great amount of time it took microprocessors to encrypt and decrypt information. However, the overall increase in processing power over the past several technology generations and the inclusion of multiple cores within an integrated circuit means that encryption and decryption can now occur very quickly.

[28] Intel Corporation's Westmere server processors – based on the 32 nanometer microarchitecture – will include instructions to enable secure data encryption and decryption using AES. See "White Paper Intel® Advanced Encryption Standard (AES) Instructions Set," Shay Gueron, January 26, 2010 *available at* http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-aes-instructions-set/.

[29] Announcing Development of a Federal Information Processing Standard for Advanced Encryption Standard, 62 Fed. Reg. 93 (Jan. 2, 1997).

With the major increase in the demand for encryption and semiconductor manufacturing efficiencies proceeding on the pace of Moore's Law, semiconductor devices with encryption will be as broadly available as encryption software. As a result, increasingly high volumes of semiconductor devices will incorporate encryption functionality and provide capabilities that are now typically gained through the installation of software. Encryption capability in integrated circuits has already started to move towards commodity status and is already considered just another feature in a semiconductor device. Encryption functionality will increasingly become inexpensive and ubiquitous, included by manufacturers in nearly every semiconductor device intended for end-use in mass market and information infrastructure products.

Because families of semiconductor products are manufactured in very high volumes and will likely all contain the same encryption algorithm, there is a large degree of *de facto* encryption standardization and utilization in semiconductor devices. This standardization aligns with earlier attempts by the U.S. government to allow the widespread use of personal encryption, but in fewer forms (e.g., the Data Encryption Standard ("DES"), Triple DES and AES).

Once incorporated into a semiconductor device, the encryption cannot be easily altered, thereby offering a degree of stability and standardization that U.S. officials have been seeking. Because encryption will typically be an inexpensive commodity feature created as a small part of integrated circuits that perform functions other than encryption, it is likely to be both cheaper and more power-efficient than a software solution; the substantial benefits that this provides to both the manufacturer and the end-user will result in ever-increasing use of hardware encryption. This is in contrast to the software dominated encryption market that prevailed in the late 1990s.

Unlike many software applications, encryption is not easily deconstructed or altered once it is embedded in a semiconductor device. In this way, hardware-embedded encryption provides a greater level of security than encryption provided to a device or application as software. There is no hardware feature analogous to source code that can be hacked, altered or copied. And because of the shrinking size of transistors in semiconductor devices – measured in nanometers – reverse engineering a semiconductor device to determine how the encryption within it operates is nearly impossible. Efforts to access and record the encryption operations in a semiconductor device are beyond the scope of the average commercial end-user.[30]

High volume semiconductor devices are simpler to use than other stand-alone encryption software applications, are less prone to user error and more cost-efficient than most alternative

[30] In February 2010, details of a method to access the programming instructions of an Infineon Technologies AG ("Infineon") integrated circuit that uses the Trusted Platform Module ("TPM") were released at the Black Hat DC Conference. The method – which requires direct access to the integrated circuit and special equipment, such as a focused ion beam microscope – allows a user to intercept instructions concerning encryption sent between the integrated circuit and the computer's memory.

According to an Infineon official, the hacked integrated circuit is obsolete – and was only intended for smart cards. The Infineon official stated that there is a new generation of TPM products which offer additional physical anti-intrusion measures and cryptographic features. See "Security Chip That Does Encryption in PCs Hacked," J. Robertson, *Associated Press*, February 8, 2010; and "Hacker Extracts Crypto Key from TPM Chip," *The H*, February 10, 2010, *available at* http://www.h-online.com/security/news/item/Hacker-extracts-crypto-key-from-TPM-chip-927077.html.

forms of encryption. As the market penetration of high volume semiconductor devices incorporating encryption increases, the need for other forms of encryption (e.g., novel algorithms and proprietary software) decreases. This further establishes the formation of *de facto* global encryption standards.

B. Commercial Activity Benefits from the Use of Encryption

The integrity and effectiveness of the commercial treatment of data storage and transmission increasingly depends upon the type of security that encryption can provide. As greater amounts of commercial activity are occurring through networks (witness the increasing use of cloud computing), the need for heightened computer and network security increases.

Encryption provides benefits beyond simply securing the transit and storage of digital information; authentication, authorization and validation are critical security functions that benefit from the use of encryption. Electronic devices of all types, and the information that they contain, need to be protected from viruses, malware, network security breaches, data and asset theft, etc. Improved protection increases the level of trust companies and individuals place in the transit of information, which, in turn, makes them much more willing to engage in e-commerce.

In addition, there are regulatory and cost catalysts to adopting encryption. Regulations in 45 states require that individuals be notified if their personal data has been compromised.[31] The average cost per company reporting a data security breach in 2009 was $6.75 million per breach, according to one study, mostly for compliance with these regulations.[32] Encryption can reduce that cost because although state regulations vary, organizations may not have to notify individuals when breached data is protected by encryption.[33] This helps to explain why, when surveyed, some 64 percent of survey respondents point to state privacy laws or selected federal statutes as a reason for adopting encryption.[34]

Additionally, because hardware-embedded encryption is primarily passive, i.e., the end-user will not typically interact with it, the widespread use of high volume semiconductor devices with encryption increases the ease and reliability of protecting the storage, access and transmission of digital information.

[31] "State Security Breach Notification Laws," *National Council of State Legislatures*, December 9, 2009, *available at* http://www.ncsl.org/Default.aspx?TabId=13489.

[32] The study is based on a survey of U.S.-based entities experiencing a breach involving loss or theft of customer data over a 12-month period. "U.S. Cost of a Data Breach Study," as cited in "Ponemon Study Shows the Cost of a Data Breach Continues to Increase," *PR Newswire*, January 25, 2010 and "2008 Annual Study: Cost of a Data Breach: Understanding Financial Impact, Customer Turnover, and Preventative Solutions," *Ponemon Institute*, February 2009, p. 4.

[33] "2008 Annual Study: Cost of a Data Breach: Understanding Financial Impact, Customer Turnover, and Preventative Solutions," *Ponemon Institute*, February 2009, p. 3 and "The Critical Need for Encrypted Email and File Transfer Solutions," *Osterman Research Inc.*, July 2009, p. 10.

[34] "2009 Study: U.S. Enterprise Encryption Trends," *Ponemon Institute*, July 2009, p. 11.

In response to the demand from producers and consumers for effective security of commercial transactions (e.g., online banking and purchases), semiconductor companies globally will be adding encryption to their products that are otherwise designed and dedicated to non-encryption functions. The result will be that encryption, which is a secondary or ancillary function of a semiconductor, will soon become a feature that customers require before considering other aspects of a product's capabilities. OEMs will market their end-products based on the general-purpose features present in semiconductor components, but customers will refuse to consider those features in the absence of a product's ability to save power (and money) by performing encryption in hardware rather than software.

V. Challenges of Current Encryption Controls for Semiconductors

The necessary realignment of export controls for encryption in the 1990s left obstacles and distortions in the treatment of semiconductors that have become more and more costly in today's environment. This has been a function of both the nature of the controls and the particular characteristics of semiconductor devices. Several features of the controls on semiconductor devices with encryption present needless impediments for the U.S. semiconductor industry.

A. Controls on Products Rather Than Encryption

Export controls on encryption are tied to implementation of encryption in a device or product rather than to encryption itself, e.g., encryption algorithms. In part, this is a legacy of munitions controls that focused on defense articles. In part, it reflects an interest of U.S. officials to review how encryption is implemented for a particular application.

Imposing licensing requirements on products with encryption rather than on encryption itself poses two problems with respect to semiconductors. First, a great many semiconductors, which in past decades have been freed from export license requirements, will be re-controlled, that is, become again subject to export license requirements as a result of introducing encryption. And this will occur even though the rationale for control – to gain visibility in the implementation of encryption in particular products – does not pertain to semiconductors with encryption. Standing alone, a semiconductor offers little insight into how encryption has been embedded in an end-product. Since a semiconductor device has no ability to act as an end-product – it can serve only as component of an end-product – how encryption is implemented in a semiconductor device, as opposed to how encryption is implemented in the end-product itself, should have no export control significance.

Second, the same encryption in the same semiconductor component can trigger a separate export review for each different product in which the component may be incorporated. This leads to repetitive and redundant reviews.

B. Proliferation of Controls through See-Through Rule

Export controls for encryption effectively impose a "see-through" rule so that inclusion of components containing encryption, such as semiconductor devices, can change the classification of an end-product as well as that of the semiconductor itself. An end-product can become subject to export controls merely because of incorporation of a semiconductor device with encryption.

C. Technical Limits on Encryption

The strength of encryption has long been a criterion in establishing export licensing thresholds; key length, for example, has historically been a significant determinant of licensing requirements. However, the non-security functions of a semiconductor component are wholly unaffected by the strength of the encryption that is embedded in the device. Indeed, most semiconductor companies are not in the encryption business. Instead, they generally rely on others for encryption and for most products are content to use standard encryption so long as it can provide adequate security.

D. No Self-Classification

Current export controls do not allow for self-classification of many products with encryption; for most destinations, exporters must submit products containing encryption for prior review by U.S. officials. This runs counter to the otherwise universal approach of the EAR for self-classification by exporters. It also means that an exporter must engage the Commerce Department with respect to classification of every type of semiconductor device that utilizes encryption. Utilizing a formal classification procedure, in lieu of normal self-classification, requires the application of much greater resources from industry and government and results in substantial delays, all without any evidence of net benefit.

E. Minimal Eligibility for Mass Market Treatment

Components containing encryption have generally not been eligible for mass market treatment due to the nature of how they are sold, i.e., not through retail outlets directly to consumers. This disqualification from mass market treatment has penalized encryption hardware components that have the same encryption functionality as software but are rarely sold directly to consumers. The distinction and differences simply do not comport with the performance of hardware and software encryption.

By their very nature and structure, integrated circuits provide almost no visibility into the manner in which they function; removing the packaging of an integrated circuit and visually inspecting its construction will not provide a user-interface nor will it reveal how the embedded encryption engine functions. In fact, reverse engineering a modern-day integrated circuit that may include the integration of more than a billion devices[35] requires advanced tools and imaging software, chemical etching and the use of scanning-electron-microscopy. Moreover, companies can incorporate physical anti-intrusion measures and encrypt internal data transfers.[36] This is in stark contrast to the nature of encryption software, where inspection of source code for

[35] Intel Corporation's newly released quad-core server processor, Tukwila, contains two billion transistors. "Intel Ships Itanium Server Processor," A. Gonsalves, *InformationWeek*, February 9, 2010, *available at* http://www.informationweek.com/news/hardware/processors/showArticle.jhtml?articleID=222700595.

[36] "Hacker Extracts Crypto Key from TPM Chip," *The H*, February 10, 2010.

encryption algorithms and application programming interfaces can provide a great deal of information about how a software application functions.

In all material respects, the semiconductor component of a mass market product shares the characteristics of a mass market item except for being sold through retail outlets. By design, development and production, the semiconductor component of a mass market item is tied to the volume and distribution of the finished product. It is self-contained and does not require on-going support from the manufacturer or interaction with the end-user. The semiconductor component is generally distributed in large quantities through more than one channel. This discrimination against encryption hardware components serves no useful purpose.

VI. Unnecessary Burdens of the Encryption Licensing Process for Semiconductors

The principal export control process for semiconductor devices that are not devoted exclusively to encryption or contain proprietary encryption is License Exception ENC. This vehicle imposes many requirements on semiconductor components that complicate and disrupt global trade flows.

A. Minimum 30-Day Export Delay

For most destinations, the existing ENC license exception available to semiconductor devices requires a delay of at least 30 days for a product review accompanied by the prospect of the imposition of special export conditions. This can cause significant operational instabilities. The uncertainty of the review period – both as to length of time and outcome – can create problems, especially for large and complex product introductions. Results from a government encryption review inevitably come in the final days of a product introduction. Even a lack of response from the government at the end of the review period can cause uncertainty over the appropriate classification of a device and the requirements for its export, e.g., can the item be exported to government end users?[37]

B. Impact on Foreign National Employees and Supply Chain

Another complication for exporters of semiconductors is that they may have to change how they treat OEMs and suppliers as a result of introducing encryption into a particular semiconductor device.[38] Exports to these entities currently need license authority and hence must proceed at least under License Exception ENC.

This is particularly burdensome because semiconductor companies need to segment their design process in a way that prevents the inclusion of foreign nationals in portions of product designs that involve encryption. This regulatory requirement persists even though the encryption

[37] See 15 C.F.R. § 740.17(b)(2) (2010).

[38] License Exception ENC authorizes the export and reexport of certain encryption items to any U.S. subsidiary wherever located (except to countries supporting terrorism), without prior review by the U.S. Commerce Department. See 15 C.F.R. § 740.17(a)(2) (2010). It does not provide such treatment to third-party vendor relationships. Similarly, the license exception does not extend to related encryption technology so foreign nationals need export authority to gain access to such technology.

algorithm embedded in a semiconductor device may be publicly available and not accessible or subject to modification.

C. International Repercussions of U.S. Classification of Semiconductors with Encryption

Many countries impose encryption controls on products based on their U.S. classification. Most U.S. semiconductor components that contain encryption are classified under ECCN 5A002, a U.S. designation that is subject to export and often import controls by foreign countries. The foreign controls are applied on U.S. components even when these components would qualify for the ENC license exception in the United States. License exceptions for encryption items are not generally available in foreign jurisdictions. This imposition of foreign requirements based on a U.S. export classification can be particularly burdensome for U.S. companies operating overseas.

D. Bifurcating Global Market into Domestic and International Sectors

It is difficult to participate in a global market when there are separate requirements for exports that apply to the overseas market but not to the domestic market. This discrepancy makes for inefficient production and dampens innovation for encryption products generally. It can also provide an impetus to move research and development offshore to avoid U.S. export controls on encryption technology. The current regulatory system creates a disincentive to build strong encryption capabilities into commercial products as recommended by the U.S. Government because it is not economically feasible for U.S. semiconductor companies to create separate, general purpose products for both the domestic and foreign markets.

E. Collateral Reporting Burdens

Accounting and reporting requirements impose a bureaucratic cost that reduces productivity and adds nothing to protecting U.S. interests.[39]

Taken together, these encryption requirements for semiconductor components impose a competitive constraint on U.S. semiconductors that can be very damaging in a highly contested global market.

VII. SIA Proposal: Classification Adjustment for Certain Semiconductors

Most of the problems and burdens that handicap the exports of semiconductor devices with encryption can be eliminated with an adjustment in the classification of integrated circuits.

[39] Under License Exception ENC, semi-annual reporting is required for exports to all destinations other than Canada as well as for reexports from Canada. Reports must include for each item, the Commodity Classification Automated Tracking System (CCATS) number and the name of the item exported (or reexported from Canada). Depending on the nature of the export or reexport, the exporter may need to submit to the Commerce Department the names and addresses of the distributors, recipients, re-sellers, individual consumers or end-users; the name of the item and the quantity exported or reexported; and the name and address of the manufacturer using the encryption items. The exporter may also be required to submit a non-proprietary technical description of the foreign product for which the encryption item will be used, the algorithm and key lengths used; general programming interfaces to the product; any standards or protocols that the foreign product adheres to; and source code. See 15 C.F.R. § 740.17(e).

Currently, all integrated circuits for information security are initially subject to encryption, national security and anti-terrorist controls. No distinction is made between devices that are dedicated to information security – e.g., encryption specific integrated circuits, Trusted Platform Modules, etc. – and devices that perform the ordinary functions of integrated circuits but also contain encryption.

By focusing encryption and national security controls on those integrated circuits dedicated to information security and removing such controls from those devices with encryption that are components for consumer and broad information infrastructure, most of the economic costs and inefficiencies of the current export controls on integrated circuits with encryption can be avoided. At the same time, there is no evidence to suggest that the risks to national security will significantly increase. Indeed, the change should not create national security risks that are materially distinct from what mass market treatment entails for software.[40]

Anti-terrorism controls have had a very limited effect on the export of semiconductors with encryption. Hence, SIA does not propose to eliminate anti-terrorism controls on semiconductors with encryption.

To minimize the adverse affects of encryption controls on the U.S. industry and the information security needs of the nation while not introducing new types of risks to national security and law enforcement interests**, SIA proposes to extend mass market treatment to general purpose semiconductors with publicly available encryption.** Mass market treatment for such semiconductors would be achieved by enabling exporters to classify them under ECCN 5A992.

The proposed classification adjustment would be limited to integrated circuits that:

a. are designed and developed to be:

    1. general purpose;

    2. capable of being incorporated into more than one type of end-product; or

    3. able to perform multiple functions in one end-product (e.g., digital signal processing and encryption).

b. can utilize or are dedicated to a publicly available encryption algorithm that cannot be easily changed by the user of the end-product; and

[40] Because general purpose integrated circuits will contain encryption that is publicly available and currently in use globally, there is no risk of providing terrorist or criminal organizations with novel or proprietary encryption capabilities. The encryption contained in integrated circuits under the adjusted classification will merely duplicate encryption that is currently available to the public at large in commercial software applications.

c. are generally available by being sold without restriction.

Such an adjustment to the classification of integrated circuits for information security could most readily take the form of a note in the CCL to make clear that the integrated circuits designated above do not fall into the primary and initial listing for information security systems, equipment and components therefor (i.e., ECCN 5A002). Instead, the designated integrated circuits would fall into the residual or secondary category for information security systems, equipment and components therefor (i.e., ECCN 5A992)[41] which is not subject to encryption or national security controls.

The terms of the designation are clear and straightforward. "General purpose" is a well-understood, long established standard in the semiconductor industry. It is usually characterized by broad applications utilized in high volumes. It encompasses a variety of microprocessors, network processors, digital signal processors, server processors and embedded processors. It stands in contrast to ASICs (application specific integrated circuits) which are specially designed and developed for a particular use. Capability for incorporation into more than one type of end-product and multiple functions expand the scope of the designation in a way that is consistent with the concept of general purpose. These types of devices are overwhelmingly deployed in personal and commercial applications that are pervasive in the digital and Internet activity that has grown so massively in the last decade.

A particular category of encryption is central to the designation. By restricting the encryption to that which is publicly available, the designation ensures that U.S. officials can have access to the encryption so as to minimize any adverse national security implications. If a general purpose semiconductor contains publicly available encryption or is designed to use or is capable of using, interacting with or facilitating publicly available encryption, it should be eligible for mass market treatment. Only the incorporation of private or proprietary encryption in the semiconductor should disqualify it from mass market treatment.

Mass market treatment is not tied only to broad functionality and publicly available encryption; it must also be made generally available. This requirement ensures that national security controls remain on the most threatening items to national security: special and specific encryption applications that are adapted to unique security complexes or infrastructures. These are the encryption items that would be of interest to government or military entities.

VIII. Benefits of Classification Adjustment for Certain Semiconductors

A. Focus on Encryption Rather Than Component

The proposed adjusted classification would relieve the affected semiconductors from most of the problems encountered under existing export controls on integrated circuits with encryption.

[41] The integrated circuits could be classified under any of the existing subcategories of ECCN 5A992 depending upon the facts and circumstances of the particular device. The essential point is that encryption and national security controls would not be applicable.

The proposed regulatory change would place the focus of export controls where it belongs: on devices dedicated to proprietary or customized encryption. This is the type of encryption capable of posing significant national security risks; it is not encryption that goes into components for consumer or information infrastructure. General purpose semiconductors with publicly available encryption are mass market devices and deserve mass market treatment.

B. Elimination of See-Through Rule

The proposed regulatory change for certain general or multiple purpose integrated circuits containing encryption would remove the need for the Commerce Department to apply a see-through rule to end-products containing such components. The new designations for integrated circuits would eliminate the need for the U.S. government to examine consumer electronic or information infrastructure products merely due to the presence of publicly available encryption in a general purpose or multiple purpose integrated circuit. Elimination of a see-through rule will greatly simplify controls and reduce the disproportionate effect of a secondary or ancillary encryption function on what are ultimately mass market or widely available items.

C. No Limitation on Strength of Encryption

The encryption algorithms embedded in the newly designated integrated circuits would be publicly available and thereby likely to be (i) well known to the U.S. government; (ii) in use around the world; and (iii) already present in end-products that are currently exported license-free from the United States under mass market treatment.

Items qualifying under the proposed regulatory change will be utilized in commercial applications that are so broad or commonplace that they cannot present a high level or strategic threat to U.S. national interests no matter what their strength. Thus, the strength of encryption in these devices should not be relevant to national security.

D. Self-Classification Available

The proposed classification adjustment would be self-executing so as to allow exporters themselves to classify integrated circuits with encryption as they do with their other products including certain ancillary encryption items.[42] Such self-classification is feasible with the clear criteria of the adjusted classification and will minimize export delays and uncertainty. Although self-classification differs from the current procedure to obtain a mass market classification, the result would be the same: an ECCN 5A992 classification.

[42] The EAR define ancillary cryptography as: "The incorporation or application of 'cryptography' by items that are not primarily useful for computing (including the operation of 'digital computers'), communications, networking (includes operation, administration, management and provisioning) or 'information security'." See 31 C.F.R. § 772 (2010).

Self-classification for general purpose integrated circuits would eliminate many duplicative and unnecessary encryption product reviews to the benefit of the U.S. government and industry alike. No government notification or review should be necessary since the encryption contained in the general purpose integrated circuit will be publicly available and intended for use in mass market or information infrastructure products. This is in keeping with the wide proliferation of commercial encryption products as well as the decentralized nature of the semiconductor industry.

E. Remedy for Lack of Mass Market Treatment

Rather than relying on marketing criteria, the proposed classification adjustment, like most parameters of the CCL and the USML, would be based on the functionality for which a device is designed and developed. Like virtually all general purpose consumer products, the integrated circuits captured by the classification adjustment would be broadly available, distributed without restriction and for final end-use in consumer products and the global information infrastructure. Specially designed or developed devices or ASICs that are relevant to a particular, installed encryption infrastructure would not be affected by the classification adjustment.

The proposed classification adjustment would treat general purpose integrated circuits in nearly the same manner as the mass market end-products in which they are incorporated. This is consistent with the spirit of the EAR and reduces controls on items that have become so ubiquitous that they no longer warrant control.

Not only should general purpose integrated circuits have encryption and national security controls removed, they should also be excluded from unnecessary and redundant product reviews and notifications to the U.S. government. This liberalization is merited because the proposed classification change is limited to hardware components. While encryption software, especially source code, can be diverted to multiple purposes, encryption embedded in firmware or an integrated circuit cannot be easily deconstructed, altered or removed. Because the encryption in general purpose integrated circuits would be effectively protected from access and diversion by an end-user, such devices should receive a commensurate level of decontrol.

IX. Rebalancing National Security and Law Enforcement Concerns with Inexorable Security Needs of an Information Society

The proposed classification adjustment is narrowly defined. It recognizes the growing needs of an information society and the opportunities that come with advances in technology. It represents not a new departure from the current export control regime for encryption but rather a natural extension of it. It relieves the major burdens of encryption export controls on semiconductors without creating major new risks to U.S. security and law enforcement interests.

There are several grounds that justify the adjusted classification for general purpose semiconductors.

A. Expansion of Existing Mass Market Treatment

The proposed classification adjustment is a natural outgrowth of mass market treatment rather than a structural change in export policy or procedure. It embraces the characteristics of mass market treatment: standardized, publicly available encryption that supports general purpose or multiple applications that are most commonly found in consumer products and information infrastructure. It extends this treatment to certain integrated circuits that ultimately are widely distributed and are cannot be easily altered. The only defining dimension that is missing is the use of certain marketing channels that constitute retail. But this reflects merely a particular means to get to the same end products – standard, broad-based products – and hence is a distinction without a difference.

The amended classification would not apply to customized applications or applications that are peculiar to an installed security infrastructure that a government or military organization would maintain. The national security risks associated with specialized and proprietary encryption would not be affected by the adjusted classification.

B. Ready Implementation of Adjusted Classification

The Administration has full authority to adopt a classification adjustment for certain semiconductors. No legislation would be necessary. The change could be made as part of the current review by the National Security Council staff of U.S. export controls generally.

In addition, such a classification adjustment could be accommodated on the international front within the national discretion of the United States. There would be no need to amend the classification of integrated circuits for information security as maintained by the Wassenaar Arrangement. Instead, the United States would construe the term "integrated circuits for information security" to mean the obvious – i.e., those integrated circuits specially designed for information security. By doing so, the current discontinuity that results from U.S. classification of integrated circuits with encryption and the lack of international license exceptions for integrated circuits with encryption could be eliminated.

C. Existing Controls Misguided and Futile

The enormous and continuously growing need for personal and commercial security in the generation, transmission and storage of information will create a demand for encryption in semiconductors that will affect a huge swath of general and multiple purpose devices. The inevitable volume of such semiconductors will not be susceptible to individual licenses or even product reviews. Re-controlling such devices because of the presence of encryption will provide no more benefit to national security than simply re-controlling processor and memory devices generally, something the U.S. government concluded long ago was counterproductive.

A global information society now depends on security and demands free access to encryption. Advanced technology now makes it possible for this security to be provided within the integrated circuits that are providing the processing power for consumer information products and information infrastructure products. These integrated circuits have already demonstrated that their volumes cannot be effectively controlled through the export license processes. Attempting to re-control them is simply doomed to fail.

That general and multiple purpose semiconductors with publicly available encryption are not worthy of control is confirmed by the widespread foreign availability of such devices. There are no significant barriers to foreign semiconductor manufacturers incorporating publicly available encryption in their general purpose devices. This foreign availability has been amply demonstrated.[43] For the U.S. semiconductor industry to maintain its innovation and competitiveness, it is essential that it not be penalized with unnecessary export restrictions.

D. An Appropriate Balance of National Interests

Information security is essential to electronic commerce and utilization of the Internet. Personal security and privacy must be preserved as more and more personal affairs connect through information products and depend on the information infrastructure. Human rights and political freedom around the world rely on a basic level of information security.[44] To reach the potential of the electronic age requires an expanded application of encryption in broad-based information products and infrastructure.

Publicly available encryption in semiconductors that serve as components to mass market information products and infrastructure can provide the next level of security for the electronic age. The decision to relax export restrictions on mass market products sold at retail was made over a decade ago. General purpose semiconductors with publicly available encryption provide the same type of information security as software sold at retail. Removing encryption and national security controls from such semiconductors should not raise significantly different national security risks for the nation.

[43] According to the *Washington Tariff & Trade Letter*, the Bureau of Industry and Security's ("BIS") Information Systems Technical Advisory Committee (ISTAC) submitted a 461-page report to BIS providing information on the foreign availability of encryption capabilities from non-Wassenaar Arrangement member countries and showing that encryption technology and products are available "in sufficient quality and quantity to negate the value of current export restrictions." "Advisory Committee Claims Encryption Foreign Availability," *Washington Tariff & Trade Letter*, December 14, 2009, p. 1.

[44] This is exemplified by the recent decision by the U.S. Department of State to waive certain sanctions against Iran with respect to the export of certain mass market software classified under ECCN 5D992 and "essential for the exchange of personal communications and/or sharing of information over the Internet" (e.g., chat, e-mail and social networking applications). The U.S. Department of State determined that such software is "necessary to foster and support the free flow of information" and "is essential to the national interest of the United States." At the same time, the U.S. Treasury Department authorized the export of certain "services incident to the exchange of personal communications over the Internet" to persons in Cuba. Cuban Assets Control Regulations; Sudanese Sanctions Regulations; Iranian Transactions Regulations, 75 Fed. Reg. 10,997 (Mar. 10, 2010).

X. Conclusion

General and multiple purpose semiconductors that are now largely decontrolled are being broadly re-captured under U.S. export controls due to the inclusion of encryption. This places a significant constraint on competitiveness of the U.S. semiconductor industry as encryption becomes a virtually cost-free commodity feature of semiconductors.

Over the last decade, the march of technology and the changing needs of a global information economy have altered the feasibility and effectiveness of export controls. President Obama recognized these changes in his State of the Union address when he set the goal to double U.S. exports in five years and to "reform export controls consistent with national security."[45]

SIA's proposed regulatory adjustment represents a rebalancing of encryption controls that responds to both the vast increase in the generation, transmission and storage of information and improvements in semiconductor technology. The proposed regulatory change is consistent with growing personal and commercial needs for information security and with the existing risks inherent in mass market treatment, and furthers the President's call for export control reform that enhances U.S. exports.

[45] The White House Office of the Press Secretary, Remarks by the President in State of the Union Address, January 27, 2010, *available at* http://www.whitehouse.gov/the-press-office/remarks-president-state-union-address.

Alliance for
Network
Security

August 24, 2010

U.S. Department of Commerce
Bureau of Industry and Security
Regulatory Policy Division
14th and Pennsylvania Avenue, NW
Room H-2705
Washington, DC 20230

Re: **Encryption Export Controls – RIN 0694-AE89**

Dear Sir/Madam:

The Alliance for Network Security ("ANS") is an industry association comprised of 3Com Corporation, Cisco Systems, Hewlett-Packard Company, Hitachi Data Systems Corp., Intel Corp., Juniper Networks, Alcatel-Lucent, McAfee Corp., Microsoft Corp. and Novell, Inc. For over ten years, ANS has advised the United States and foreign governments with respect to export and import controls on cryptography. We appreciate this opportunity to provide comments with respect to the Interim Final Rule with Request for Comments entitled *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* which was published in the Federal Register on June 25, 2010.

First, we would like to congratulate the Bureau of Industry and Security ("BIS") for its inclusion of the changes to Category 5, Part 2 reflecting the 2009 Wassenaar list review in this regulation. Important changes agreed to by the participating member states of the Wassenaar Arrangement, including the new Note 4, significantly reduce the burden on exporters of affected items. Our first set of comments is designed to address future Wassenaar list review exercises.

Second, we would like to congratulate BIS on taking 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. The reduction in pre-export technical review and post-export reporting requirements benefit some companies more than others, but overall represent progress that should be acknowledged. Our second set of comments is intended to further this agenda.

Third, we appreciate the commitment to review other issues related to encryption controls, in keeping with national security requirements and multilateral regime commitments. Our third set of comments is intended to address some specific technologies that we believe are deserving of priority attention.

Comment Set No. 1: Wassenaar List Review

1. Positive list based on Section 740.17(b)(2) (with key length increases and modifications for network infrastructure, OCI, and electronic components)
2. Revision of Note 3 (Cryptography Note) to decontrol components of mass market items
3. Revision of Note 4 (so-called Ancillary Note) to expand the scope of decontrol
4. Addition of new Note 5 to expand Section 740.17(a)(2) coverage to companies headquartered in Wassenaar member states

Comment Set No. 2: Fulfilling the President's Mandate

1. Controls on Encryption in the Single Control List
2. Decoupling of Information Collection from the Export Control Regulations
3. Revision of the Definition of "Government End-User"

Comment Set No. 3: Specific Technologies Requiring Attention

1. Network Infrastructure Products
2. Open Cryptographic Interfaces
3. Electronic Components
4. Publicly Available Source Code
5. Redline Edits to Sections 740.17(b)(2) and (b)(3)

Finally, we urge BIS and other interested agencies to reflect on the new complexity that has been introduced by this new regulation, which exceeds twenty pages of fine print sprinkled throughout various sections of the Export Administration Regulations ("EAR"). Perhaps, reform must come at the cost of some additional complexity, but we would like to work with you, through these suggestions and others that you may introduce, toward a goal of not only reducing the burden on industry but also the complexity of the regulations, while always protecting the national security interests of the United States.

Sincerely,

Roszel C. Thomsen II
Counsel
Alliance for Network Security

WASSENAAR ARRANGEMENT EXPERT GROUP – PROPOSAL
2011 LIST REVIEW

Submitting Country	United States
Title of Proposal	Cat 5 Pt 2 – Positive List of Items Controlled
Current text	5. A. Part 2. SYSTEMS, EQUIPMENT AND COMPONENTS 5. A. 2. "Information security" systems, equipment and components therefor, as follows: 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 Global Navigation Satellite Systems (GNSS) receiving equipment containing or employing decryption, see 7.A.5.* 5. A. 2. 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 unauthorised access.* *3. "Cryptography" does not include "fixed" data compression or coding techniques.* *Note 5.A.2.a.1. includes equipment designed or modified to use "cryptography" employing analogue principles when implemented with digital techniques.* 5. A. 2. a. 1. a. A "symmetric algorithm" employing a key length in excess of 56 bits; or b. An "asymmetric algorithm" where the security of the algorithm is based on any of the following: 1. Factorisation of integers in excess of 512 bits (e.g., RSA); 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 3. Discrete logarithms in a group other than mentioned in 5.A.2.a.1.b.2. in excess of 112 bits (e.g., Diffie-Hellman over an elliptic curve); 5. A. 2. a. 2. Designed or modified to perform cryptanalytic functions; 3. Not used since 1998

	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; 5. Designed or modified to use cryptographic techniques to generate the spreading code for "spread spectrum" systems, not specified by 5.A.2.a.6., including the hopping code for "frequency hopping" systems; 5. A. 2. 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. A bandwidth exceeding 500MHz; or b. A "fractional bandwidth" of 20% or more; 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; 8. Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion; 9. Designed or modified to use "quantum cryptography". *Technical Note* *"Quantum cryptography" is also known as Quantum Key Distribution (QKD).* …
Proposed text	**5. A. Part 2. SYSTEMS, EQUIPMENT AND COMPONENTS** **5. A. 2. "Information security" systems, equipment and components therefor, that use any of the following for privacy of users' data:** **(i) Key lengths exceeding 128 bits for symmetric algorithms;** **(ii) Public key modulus sizes exceeding 1024 bits for asymmetric algorithms; or** **(iii) Key lengths exceeding 160 bits for elliptic curve algorithms:** **5. A. 2. a. 1. Cryptographic commodities, software and components:** **5. A. 2. a. 1. 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 128-bits for symmetric algorithms meeting any of the following: **1. Aggregate encrypted WAN, MAN, VPN or backhaul throughput (including communications through wireless network elements such as gateways, mobile switches, and controllers) greater than 600 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 400 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:** **a. Maximum transmission data rates exceeding 10 Mbps (at operating ranges beyond 1,000 meters);** **b. Maximum number of concurrent full-duplex voice channels exceeding 30; or** **c. (Substantial support is required for installation or use;** **b. Encryption source code that is not publicly available;** **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) that is user-accessible and can be easily changed by the user;** **d. Encryption commodities and software that provide functions necessary for "quantum cryptography";** ***Technical Note*** ***"Quantum cryptography" is also known as Quantum Key Distribution (QKD).*** **e. Encryption commodities and software that have been modified or customized for computers classified under 4.A.3.;**

	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);** **5. A. 2. a. 2. Cryptanalytic commodities and software;** **5. A. 2. a. 3. Specific encryption technology. Specific encryption technology as follows:** **a. Technology for "non-standard cryptography". Encryption technology classified under 5.E.2. for "non-standard cryptography";** **b. Other technology. Encryption technology classified under 5.E.2. except technology for "cryptanalytic items", "non-standard cryptography" or any "open cryptographic interface";** ***Note*** ***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.*** **...**
Background	In its effort to reform export controls on encryption items, the United States seeks to create a new positive list of encryption items suitable for control.
Technical justification	The proposed 5.A.2. list reflects those dual-use encryption items that the United States has identified as warranting control. The proposed list mirrors the current United States “Restricted” list in 15 CFR 740.17(b)(2), with several modifications that are consistent with foreign availability. First, there are key length increases as outlined in 5.A.2. and 5.A.2.a.1.a. Second, the network throughput threshold is increased to 600Mbps as outlined in 5.A.2.a.1.a.1. Third, the threshold for number of encrypted data channels is increased to 400 channels as outlined in 5.A.2.a.1.a.4. Fourth, open cryptographic interface items are not included.
Major/key element	Replacing 5.A.2. with a new list of controlled items.
Foreign Availability	N/A.
Controllability	N/A.
Controlled in another regime?	No.
Consequential changes?	None.
Proposed Review Date	None.
Other information	None.

WASSENAAR ARRANGEMENT EXPERT GROUP – PROPOSAL
2011 LIST REVIEW

Submitting Country	United States
Title of Proposal	Cat 5 Pt 2 – Note 3
Current text	*Note 3* *Cryptography Note* *5.A.2. and 5.D.2. do not apply to items that meet all of the following:* *a. Generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of the following:* *1. Over-the-counter transactions;* *2. Mail order transactions;* *3. Electronic transactions; or* *4. Telephone call transactions;* *b. The cryptographic functionality cannot easily be changed by the user;* *c. Designed for installation by the user without further substantial support by the supplier; and* *d. Not used since 2000* *e. 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. to c. above.*
Proposed text	*Note 3* *Cryptography Note* *5.A.2. and 5.D.2. do not apply to items that meet all of the following:* ***(1)*** ***a. Generally available by being sold, without restriction, by means of any of the following:*** ***1. Over-the-counter transactions;*** ***2. Mail order transactions;*** ***3. Electronic transactions;*** ***4. Telephone call transactions; or*** ***5. Commercial distribution channels through which the items are sold or will be sold in large volume;*** *b. The cryptographic functionality cannot easily be changed by the user;* *c. Designed for installation by the user without further substantial support by the supplier; and* *d. Not used since 2000* *e. 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. to c. above.* ***(2) Components or software for items described in part 1 to this note above.***
Background	The new item 5 in part 1(a) and the new part 2 seek to address the issue that some components and software of mass market items do not themselves qualify for mass market treatment and some non-retail distribution channels lead to identical wide-spread availability. Further, the components or software of mass market items may not currently qualify for ancillary treatment under Note 4 either. For example, the

	operating system for a smartphone may fall into this category. Similarly, Application-Specific Integrated Circuits (ASICs) for smartphones may fall into this category. This Note 3 revision covers these items that otherwise fall through the cracks of Notes 3 and 4.
Technical justification	The rationale for removing the reference to "the public" and "stock at retail selling points" is to eliminate ambiguous language and the reference to "retail," which historically served to confuse exporters. The new item 5 in part 1(a) and the new part 2 expand the distribution channel list to include multi-tier distribution channels and Original Equipment Manufacturer distribution, which lead to wide-spread availability of general purpose and non-customized products. The semiconductor industry is particularly impacted by the current distribution channel language because its products are not generally sold through traditional retail channels. Further, many integrated circuits use the same publicly available encryption algorithms used in software that does qualify for mass market treatment since the software is sold through retail channels. Thus, semiconductors could qualify for mass market treatment with an update to Note 3 that equitably accounts for non-retail large-volume distribution.
Major/key element	New part 2 that includes components and software. New item 5 under part 1(a) that includes commercial distribution channels. Updated part 1(a) language that removes the reference to "the public" and "stock at retail selling points."
Foreign Availability	N/A.
Controllability	N/A.
Controlled in another regime?	No.
Consequential changes?	None.
Proposed Review Date	None.
Other information	None.

WASSENAAR ARRANGEMENT EXPERT GROUP – PROPOSAL
2011 LIST REVIEW

Submitting Country	United States
Title of Proposal	Cat 5 Pt 2 – Note 4
Current text	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.*
Proposed text	Note 4 ***Category 5–Part 2 only applies to items where:*** ***a. Their primary function is "Information security"; and*** ***b. Such items otherwise would be controlled under Category 4, Category 5–Part 1, or Category 7.***
Background	This revision presents a more realistic approach to the current technology landscape. Data storage, computing, data transmission, and networking products increasingly require the security features that encryption provides. As more devices are networked, there is a ubiquitous need for standard commercial encryption features in everyday computing and telecommunications devices so as to protect personal data. Thus, Category 5, Part 2 will inevitably swallow much of Category 4 and Category 5, Part 1. For example, the semiconductor industry is currently moving toward utilizing encryption features in standard commercial products. These products will find themselves re-controlled when they incorporate the ancillary encryption features.
Technical justification	The rationale for the revisions is to identify with positive language those items controlled by Category 5, Part 2 and to more fully capture the spirit of "ancillary encryption" by excluding certain items for which their core functionality is not information security. Items excluded from Category 5, Part 2 by Note 4 should still be evaluated under other categories. This Note 4 revision does not exclude Category 7 items because there may be an interest for Category 5, Part 2 to control certain airborne communications.
Major/key element	Replacing the Note 4 language.
Foreign Availability	N/A.
Controllability	N/A.
Controlled in another regime?	No.

Consequential changes?	None.
Proposed Review Date	None.
Other information	None.

**WASSENAAR ARRANGEMENT EXPERT GROUP – PROPOSAL
2011 LIST REVIEW**

Submitting Country	United States
Title of Proposal	Cat 5 Pt 2 – Note 5
Current text	N/A.
Proposed text	***Note 5*** ***Category 5–Part 2 does not apply to items transferred within a company and meeting all of the following:*** ***a. The company is headquartered in a Wassenaar member country; and*** ***b. The transfer is for internal use only.***
Background	Some Wassenaar member states currently require individual authorizations to share cryptographic items, such as source code, within a company when subsidiaries in other countries would be involved in the development process.
Technical justification	This new note is intended to allow Wassenaar member state companies to develop globally without the need for specific authorizations until the product is ready for distribution outside the company.
Major/key element	Adding a new Note 5 to Category 5–Part 2.
Foreign Availability	N/A.
Controllability	N/A.
Controlled in another regime?	No.
Consequential changes?	None.
Proposed Review Date	None.
Other information	None.

ANS Alliance for Network Security

Comment Set No. 2: Fulfilling the President’s Mandate

1. Controls on Encryption in the Single Control List

The proposed positive list is based on the three-tiered approach articulated by the current administration.[1] We anticipate that as technologies mature, they cascade down the tiered framework from higher control tiers to lower control tiers and may eventually move to EAR99.

Table 1: Proposed Positive List of Encryption Items Subject to Control[2]

Tier	Description	Discussion & Example
Tier I “Crown Jewels”	Tier I items are described in the ITAR Munitions List[3] in Category XIII(b): Military Information Security Assurance Systems and equipment, cryptographic devices, software, and components specifically designed, developed, modified, adapted, or configured for military applications …	The big word in this description is “military.” “Dual-use” items are described in Tiers II and III. A Tier I example is a Type I cryptographic device such as a Motorola STU-III secure telephone.
Tier II Intermediate Controls	Tier II is based on section 740.17(b)(2), the “restricted” list.	The (b)(2) list represents those items BIS has identified as having a reason for which to control.
Tier III Low Controls	Tier III is based on section 740.17(b)(3), the “unrestricted, subject to technical review” list.	This list captures items that currently require a classification request for national security reasons.
EAR99	Everything else would be classified under EAR99, unless it is described in another entry under Tier III.	Items in (b)(1) currently only require registration and annual self classification reporting. This reporting for information-gathering purposes falls within the government-industry forum discussed in Part 2 of this Comment Set. Encryption items not captured by the above tiered framework, may still be captured by their equivalent ECCN. For example, if microprocessors are subject to controls under the Tier III equivalent of 3A991, then they would continue to be controlled under the Tier III equivalent of 3A991, and not "cascade" down to EAR99.

[1] See, e.g., Remarks by General Jones, National Security Advisor, “The Administration’s Export Control Reform Plans,” June 30, 2010.

[2] This document focuses on encryption reform. Category 5, Part 2 and ITAR Munitions List Category XIII(b) contain some items that are not encryption-related. See, e.g., ECCNs 5A002.a.4, a.7, and a.8. This document does not address these items.

[3] 22 C.F.R. § 121.1.

Tier I contains those items with the highest sensitivity, often termed the “crown jewels.” Tier I items are those designed for military use as described in the ITAR Munitions List in Category XIII(b).

Tier II contains items with an intermediate level of control. This includes the items currently in EAR section 740.17(b)(2), often termed the “restricted list,” with two modifications as discussed in Table 1 above.

Tier III contains items with a low level of control. Items in section 740.17(b)(3), often termed “unrestricted, subject to technical review,” provide the starting point for the Tier III list. Currently, exports of (b)(3) items require a classification request before immediate export to favorable treatment countries and a 30-day review prior to export to other countries. Tier III includes items currently in sections 740.17(b)(3)(ii)-(iv), which are controlled for reasons other than information collection (i.e., through the pre-export technical review and post-export reporting processes). Here, we have moved (b)(3)(i) items down one step in the cascading control tiers to EAR99. This is consistent with current regulations that place the least controls on (b)(3)(i) items as compared to the other (b)(3) items. For example, (b)(3)(ii) includes software and commodities utilizing non-standard cryptography, but its counterpart technology is currently singled out in the “restricted list” in (b)(2)(iv)(A). Unlike most other (b)(2) items, this technology is not authorized for License Exception ENC to non-Supplement No. 3 countries. In contrast, the (b)(3)(i) items have no such counterpart with this elevated “restricted list” status. Further, current regulations do not permit mass market treatment of (b)(3)(iii) items and impose post-export reporting requirements on (b)(3)(iii) items. In contrast, (b)(3)(i) items are currently eligible for mass market treatment and are not subject to the same post-export reporting requirements.

All other items not within Tiers I-III, including items currently in sections 740.17(b)(1) and (b)(4), fall into EAR99 unless described by an equivalent ECCN in Tiers I-III. For example, if microprocessors are subject to controls under the Tier III equivalent of 3A991, then they would continue to be controlled under the Tier III equivalent of 3A991, and not "cascade" down to EAR99. Since (b)(1) exports currently only require registration and an annual self-classification report, there is a better vehicle other than export controls to effectively collect product information. Thus, these items are logically removed from the export controls process. This is discussed further in the government-industry forum section in Part 2 of this Comment Set.

The cascading nature of this tiered architecture allows controls to easily respond to technology lifecycles. For example, we have placed open cryptographic interface items currently in (b)(2)(iii) into Tier III and placed (b)(3)(i) items into EAR99. As new technologies emerge, we anticipate that the government will amend the items contained in each tier as necessary. This narrow positive list assists exporters in identifying the nature of controls related to their products and allows the government to maintain controls on those items of concern.

2. Decoupling of Information Collection from the Export Control Regulations

We propose creating a government-industry forum as a substitute for the information collection process currently conducted through the pre-export technical review, registration, self-classification, and reporting process.

The government-industry forum would feature the following characteristics:

a) The forum is jointly led by government and industry representatives. By taking a leadership role in the forum, both government and industry representatives will have a stake in and be fully committed to its success.

b) Participation is by invitation only. The forum is outside the Federal Advisory Committee Act[4] and its requirements. This is important in order to maintain full and candid sessions.

c) An outside third party separate from the intelligence community and industry coordinates the forum. This third party may be a Federally Funded Research and Development Center ("FFRDC") administrator,[5] such as Institute for Defense Analysis or MITRE Corp., which currently have or previously had contracts with the FBI to perform a similar function.

d) The forum includes U.S. and non-U.S. organizations. Participants may include companies not directly subject to the EAR process, but play a large role in industry. This could be expanded to include friendly governments (e.g., Canada) and companies incorporated in these countries (e.g., Research in Motion), making the forum even more useful than the current U.S. export control system for purposes of information collection and sharing.

One important responsibility of the forum is to create a viable alternative to the information-gathering framework currently handled by BIS through its reporting requirements. As discussed in Part 1 of this memorandum, we propose that certain encryption items currently controlled for information-gathering purposes be decoupled from the encryption export controls. This entity may operate by identifying trends in encryption technology and providing a forum in which valuable bilateral relationships can be forged between the government and specific industry participants for further, confidential, sharing of information.

The forum provides mutual benefits to both government and industry over the current review and reporting system administered by BIS. First, the forum provides a vehicle for NSA

[4] 5 U.S.C. App. 2.

[5] For a list of FFRDC administrators, see http://www.nsf.gov/statistics/ffrdclist/. The third party administrator may be another suitable entity not on the list, such as Booz Allen Hamilton.

to obtain more information than is gathered through the current process. Since the forum includes non-U.S. entities, the government can have a dialog with entities that otherwise would not provide information through the EAR process. In addition, the current EAR process does not effectively capture small U.S. companies that are developing innovative products using encryption features, but have not expanded sales or operations outside of the U.S.

Second, the forum provides a more efficient means for targeting valuable information. The current process is weighed down by an information overload where the government is collecting a large amount of non-useful and redundant information. The data is mined on the backend for small nuggets of critical information. This forum alleviates the inefficiencies in this process by focusing on collecting the desired information at the outset and drilling down to the specific target areas through dialog.

This government-industry forum serves to decouple NSA's information collection function from the government's export control functions, especially for items currently only requiring registration and self-classification. It provides NSA with the most efficient vehicle for performing more targeted information collection on a wider range of items. With industry participation, the government can more easily access timely information and anticipate advances in technologies. It also permits a two-way dialog between industry and government and provides industry with a platform for candid conversations with NSA.

There are other alternative methods for information collection that can be discussed as variants on this theme.

3. Revision of the Definition of "Government End-User"

The current definition of "Government end-user" in part 772 of the EAR creates interpretive issues, because it describes not only entities that meet the definition of "government end-user" but also entities that do not. (Of course, many end-users do not comfortably fit into either category!) Further interpretive issues arise in the various listings of "government end-user" set forth in the riders and conditions on Encryption Licensing Arrangements issued by the Bureau of Industry and Security over the years.

Proposed Revision

We propose that the definition of "Government end-user" should be revised so that it specifies only those entities for which a license is required. Any entity that is not included in this "positive" list would not require a license.

1. EXECUTIVE AGENTS OF STATE (INCLUDING OFFICES OF PRESIDENT / VICE PRESIDENT / PRIME MINISTER, ROYAL COURTS, NATIONAL SECURITY COUNCILS, CABINET / COUNCIL OF MINISTERS / SUPREME COUNCILS /

EXECUTIVE COUNCILS, CROWN PRINCES AND OTHER DEPUTIES OF THE RULERS, DEPARTMENTS AND OFFICES OF POLITICAL / CONSTITUTIONAL / MAINLAND AFFAIRS)

2. LEGISLATIVE BODIES RESPONSIBLE FOR THE ENACTMENT OF LAWS

3. JUDICIARY (INCLUDING SUPREME COURTS AND OTHER NATIONAL / FEDERAL / REGIONAL / ROYAL HIGH COURTS AND TRIBUNALS)

4. MINISTRIES, DEPARTMENTS AND GARRISONS OF DEFENSE, INCLUDING MILITARY AND ARMED SERVICES (INCLUDING NATIONAL GUARD, COAST GUARD, SECURITY BUREAUS AND PARAMILITARY) AND DEFENSE TECHNOLOGY AGENCIES

5. MINISTRIES AND DEPARTMENTS OF INTELLIGENCE

6. MINISTRIES AND DEPARTMENTS OF FOREIGN AFFAIRS / FOREIGN RELATIONS / CONSULATES / EMBASSIES

7. MINISTRIES AND DEPARTMENTS OF INTERIOR, INTERNAL / HOME / MAINLAND AFFAIRS, AND HOMELAND SECURITY

8. MINISTRIES AND DEPARTMENTS OF IMPORT/EXPORT CONTROL, CUSTOMS AND IMMIGRATION

9. POLICE, INVESTIGATION AND OTHER LAW ENFORCEMENT AGENCIES (INCLUDING DIGITAL CRIME / CYBER CRIME / COMPUTER FORENSICS, COUNTER NARCOTICS / COUNTER TERRORISM / COUNTER PROLIFERATION) AND PRISONS

10. PUBLIC SAFETY (INCLUDING NATIONAL / FEDERAL / ROYAL AGENCIES AND DEPARTMENTS OF CIVIL DEFENSE, EMERGENCY MANAGEMENT, AND FIRST RESPONDERS).

Comment Set No. 3: Specific Technologies Requiring Attention

1. Network Infrastructure Products

Based on the foreign availability study certified by the Information Systems Technical Advisory Committee,[6] we suggest two modifications to section 740.17(b)(2)(i)(A):

1) Increase the aggregate encrypted WAN, MAN, VPN or backhaul throughput threshold from 90 to 600 Mbps in section 740.17(b)(2)(i)(A)(1).

2) Increase the number of concurrent encrypted data channels for media encryption or centralized key management threshold from 250 to 400 in (b)(2)(i)(A)(4). Although (b)(2)(i)(A)(4) could be eliminated based on foreign availability of equipment, we have chosen to retain controls based on the number of data channels in order to capture certain items, such as software firewalls.

2. Open Cryptographic Interfaces

We suggest removing (b)(2)(iii) open cryptographic interface items from the (b)(2) “restricted” list and placing it in the (b)(3) “unrestricted” list. This is consistent with the foreign availability study certified by the Information Systems Technical Advisory Committee.[7] Considering the framework presented in Comment Set No. 2, (b)(2)(iii) items cascade out of Tier II and into Tier III.

3. Electronic Components

Based on the foreign availability study certified by the Information Systems Technical Advisory Committee,[8] we suggest removing (b)(3)(i) items from the “unrestricted” list in (b)(3) and any reference to these items in (b)(3). Considering the framework presented in Comment Set No. 2, (b)(3)(i) items cascade down the controls tiers out of Tier III. This is consistent with current regulations that place the least controls on (b)(3)(i) items as compared to the other (b)(3) items. For example, (b)(3)(ii) includes software and commodities utilizing non-standard cryptography, but its counterpart technology is currently singled out in the “restricted list” in (b)(2)(iv)(A). Unlike most other (b)(2) items, this technology is not authorized for License Exception ENC to non-Supplement No. 3 countries. In contrast, the (b)(3)(i) items have no such counterpart with this elevated “restricted list” status. Further, current regulations do not permit mass market treatment of (b)(3)(iii) items and impose post-export reporting requirements on

[6] Information Systems Technical Advisory Committee, “Report on Foreign Availability of Certain Encryption items,” Nov. 12, 2009.

[7] *Id.*

[8] *Id.*

(b)(3)(iii) items. In contrast, (b)(3)(i) items are currently eligible for mass market treatment and are not subject to the same post-export reporting requirements.

4. Publicly Available Source Code

The remaining controls on publicly available source code in part 734 of the EAR should be removed so that publicly available encryption source code is treated as any other publicly available source code within the EAR.

5. Redline Edits to 740.17(b)(2) and (b)(3)

In accordance with the discussion above, we suggest the following redline edits to section 740.17(b)(2):

***

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:*

***

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

Equipment listed below, that uses any of the following for privacy of users' data:

- Key lengths exceeding 128 bits for symmetric algorithms;
- Public key modulus sizes exceeding 1024 bits for asymmetric algorithms; or
- Key lengths exceeding 160 bits for elliptic curve algorithms:

(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~~ 128-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~~ 600 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~~ 400 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

***

(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.~~ [Reserved]

***

In accordance with the discussion above, we suggest the following redline edits to section 740.17(b)(3):

***

(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.~~ [Reserved]

(ii) Encryption commodities, software and components that provide or perform "non-standard cryptography".

(iii) Encryption commodities and software 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~~ paragraph (b)(2) ~~or (b)(3)(i)~~ of this section.

(v) Items providing an "open cryptographic interface".

eCrypt

U.S. Department of Commerce
Bureau of Industry and Security
Regulatory Policy Division
14th Street and Pennsylvania Avenue, NW.
Room H–2705
Washington, DC 20230

Re: RIN 0694–AE89 – Encryption Export Controls Request for Comments

Dear Sir or Madam:

eCrypt is providing the following comments on the June 25, 2010 encryption rule issued by the Department of Commerce's Bureau of Industry and Security ("BIS")Liberalization is minimal. While the ability to self-classify is beneficial, the imposition of encryption registration and self-classification reporting requirements create new burdens that cancel the effect of the liberalization.

As you know, encryption items used to be controlled under the International Traffic in Arms Regulations ("ITAR") and, under the ITAR, manufacturers and exporters of ITAR-controlled items must register with the State Department's Directorate of Defense Trade Controls ("DDTC"). Once most encryption items were moved under the jurisdiction of the Commerce Department's Export Administration Regulation in 1996, this registration requirement was eliminated for commercial manufacturers and exporters of encryption items. eCrypt views it as a step backwards that Commerce has now imposed an ITAR-like registration requirement applicable to commercial companies. While the encryption registration requires less information from companies than does a DDTC registration, eCrypt notes that, in addition to collecting and filing the information initially, it requires companies to keep track of their answers and update them with changes over time in a way that was not previously required of software companies who make or sell encryption products. Accordingly, one burden (encryption review requests) was traded for another (encryption registration with attendant updates).

In addition, for products that can be self-classified there is now the new burden of annual self-classification reports. Previously for mass market products and for some ENC Unrestricted products (that were excluded from semi-annual reporting), once a review request was filed and the CCATS was issued, a company was not required to make additional submissions until such time as the encryption in or used by its product changed. Now, a company has to track the self-classification reporting information in a specific format and make formal filings the BIS for those products that are both self-classified and exported. While the delay in exporting to some countries needed to be factored in under the prior rule, filing the encryption review request was easier. Companies essentially still need to collect and document the same information previously contained in an encryption review for their self-classifications in order to arrive at the correct classification. Once the information is organized, the encryption review request was easier than the current combined registration and reporting burden of self-classification.

In addition to opposing the new administrative burdens, eCrypt believes as a matter of policy that focusing resources on commercial companies is not likely to be the most efficient use of national security resources. Commercial encryption products are widely available around the globe and the registration and reporting requirements seem to add significant burdens on numerous companies without a clear national security benefit.

Sincerely,

Brad Lever
President/CEO
eCrypt Technologies Inc.
1.866.241.6868 f/p