RECORD OF PUBLIC COMMENTS

NOTICE OF INQUIRY: REQUEST FOR PUBLIC COMMENT ON FOREIGN PRODUCED ENCRYPTION ITEMS THAT ARE MADE FROM U.S.-ORIGIN ENCRYPTION TECHNOLOGY OR SOFTWARE

Publication in the Federal Register: January 6, 2009 (74 FR 413)
Comments due March 9, 2009

	SOURCE	SIGNER(S) OF COMMENT	DATE	NUMBER OF PAGES
1.	Bill Root	Bill Root	2/28/09	2
2.	Semiconductor Industry Association (SIA)	David Rose	3/9/09	6
3.	TechAmerica	Ken Montgomery	3/9/09	14

style. There shall be no discussion of proprietary information, costs or prices, market shares, or other commercial matters regulated by U.S. antitrust laws. A court reporter will record the proceedings of the public meeting, after which a transcript will be available on the above-referenced Web site.

After the public meeting and the close of the comment period on the Framework Document, DOE will begin collecting data, conducting the analyses as discussed in the Framework Document and at the public meeting, and reviewing the comments received.

DOE considers public participation to be a very important part of the process for setting energy conservation standards. DOE actively encourages the participation and interaction of the public during the comment period in each stage of the rulemaking process. Beginning with the Framework Document, and during each subsequent public meeting and comment period, interactions with and between members of the public provide a balanced discussion of the issues to assist DOE with the standards rulemaking process. Accordingly, anyone who would like to participate in the public meeting, receive meeting materials, or be added to the DOE mailing list to receive future notices and information regarding this rulemaking on walk-in coolers and walk-in freezers, should contact Brenda Edwards at (202) 586–2945, or via e-mail at: *Brenda.Edwards@ee.doe.gov*.

Issued in Washington, DC, on December 24, 2008.

John F. Mizroch,

Acting Assistant Secretary, Energy Efficiency and Renewable Energy.

[FR Doc. E8–31405 Filed 1–5–09; 8:45 am]

BILLING CODE 6450–01–P

DEPARTMENT OF COMMERCE

Bureau of Industry and Security

15 CFR Part 736

[Docket No. 0810231384–81391–01]

RIN 0694–XA15

Request for Public Comment on Foreign Produced Encryption Items That Are Made From U.S.-Origin Encryption Technology or Software

AGENCY: Bureau of Industry and Security.

ACTION: Notice of inquiry.

SUMMARY: To determine the appropriate extent and scope of U.S. export controls on foreign products that are the direct products of U.S.-origin encryption technology or software, BIS is seeking information on the potential impact of controlling such foreign made items for Encryption Items (''EI'') reasons under the EAR (i.e., those that are classified under ECCN 5A002 or 5D002) if the direct product of U.S.-origin ECCN 5E002 technology or ECCN 5D002 software. Specifically, BIS is requesting comments regarding the impact this control would have on both U.S. exporters of encryption technology and software and foreign manufacturers of products that are derived in whole or in part from U.S.-origin encryption technology or software.

DATES: Comments must be received no later than March 9, 2009.

ADDRESSES: Written comments may be submitted via *http://www.regulations.gov*; by e-mail directly to BIS at *publiccomments@bis.doc.gov*; in hardcopy to U.S. Department of Commerce, Bureau of Industry and Security, Regulatory Policy Division, 14th St. and Pennsylvania Ave., NW., Room H–2705, Washington, DC 20230; or by fax to 202–482–3355. Please input ''0694–XA15'' in the subject line of the written comments.

FOR FURTHER INFORMATION CONTACT: For General Information Contact: Sharron Cook, Office of Exporter Services, Regulatory Policy Division, Bureau of Industry and Security at 202–482–2440, or fax 202–482–3355, or e-mail at *scook@bis.doc.gov*.

For Specific Encryption Related Information Contact: C. Randall Pratt, Information Technology Division, Office of National Security and Technology Transfer Controls at 202–482–0707 or E-Mail: C. Randall Pratt at *cpratt@bis.doc.gov*.

SUPPLEMENTARY INFORMATION:

Background

The Foreign-Produced Direct Product Rule is found in General Prohibition No. 3 under section 736.2(b)(3) of the Export Administration Regulations (EAR) and in section 734.3(a)(4) of the EAR, ''Items Subject to the EAR.''

Under section 736.2(b)(3)(ii)(A) of the EAR, a foreign-made item is considered a direct product of U.S. technology or software if it meets the following conditions, it is the direct product of technology or software that requires a written assurance as a supporting document for a license, as defined in paragraph (o)(3)(i) of Supplement No. 2 to part 748 of the EAR, or as a precondition for the use of License Exception TSR at section 740.6 of the EAR, and it is subject to national security controls as designated on the applicable ECCN of the Commerce Control List at part 774 of the EAR.

Section 736.2(b)(3)(i) provides that if a foreign-made item is a direct product of U.S.-origin technology or software pursuant to the criteria set forth above, then it is subject to the EAR if it is exported from the country of manufacture to a destination in Country Group D:1 or E:2 (Cuba) of Supplement No. 1 to Part 740 of the EAR. General Prohibition 3 prohibits the reexport or export from abroad of items meeting the criteria of foreign direct products of U.S.-origin technology or software to Country Group D:1 destinations or Cuba unless authorization has been granted via a license or license exception.

Technology and software controlled under ECCN 5E002 and 5D002 of the Commerce Control List (CCL) (Supplement No. 1 to part 774 of the EAR) are subject to national security (''NS'') controls. When the foreign-produced direct product of such technology or software would be classified under ECCN 5A002 or 5D002, it would meet the definition of ''direct product'' under section 736.2(b)(3)(ii)(A) of the EAR.

BIS is seeking information on the impact of making the foreign-produced direct product of U.S.-origin ECCN 5E002 technology or ECCN 5D002 software, classified under ECCN 5A002 or 5D002 subject to the EAR if exported from the country of manufacture to any destination (except the United States or Canada). All such foreign-produced direct product ECCN 5A002 or 5D002 hardware or software would be subject to the license requirements of sections 742.15 (''EI'' encryption items) and 742.4 (''NS'' national security), or to the review requirements of section 740.17 (License Exception ENC). Reporting requirements under section 740.17(e) would not apply to exports from the country of manufacture of foreign-produced direct products, as reporting is required only for export from the United States or reexports from Canada.

The possible revision described above would apply to the foreign direct product of ECCN 5E002 technology and 5D002 software exported under license, not to the foreign direct product of technology and software exported under License Exception ENC of section 740.17 of the EAR.

Under the current provisions of section 736.2(b)(3), if ECCN 5E002 technology is exported under an export license for purposes of offshore manufacture of an encryption item that has previously been submitted to the U.S. Government for technical review and has been made eligible for export under License Exception ENC, the

foreign-produced direct product of the technology is *not* subject to the EAR unless: (1) It is exported from the country of manufacture to a destination in Country Group D:1 or E:2 (Cuba); or (2) it is exported from the United States after having been shipped to the United States from the country of manufacture.

However, all foreign-produced direct product of technology or software exported under License Exception ENC under either paragraph (a)(1) (for internal development of new products by a 'license-free zone' (Supplement No. 3 to part 740) ''private sector end-user'') or (a)(2) (to a ''U.S. subsidiary'' for internal use or development) are currently subject to the EAR by the terms of the notes to paragraphs (a)(1) and (a)(2).

Request for Comment

BIS is seeking public comment on the impact such a revision to section 736.2(b)(3)(i) would have on both U.S. manufacturers of encryption technology and software and foreign manufacturers of products (including under contract to U.S. companies who own and maintain the intellectual property, branding, marketing and distribution rights to the end-products manufactured offshore) that are derived in whole or in part from U.S.-origin encryption technology or software. BIS is also seeking information about the cost of compliance with such a revision, including U.S. Government review of foreign direct products prior to export from abroad. BIS is also seeking information on the burdens of complying with multiple sets of laws, foreign and U.S., which could result from the potential revision.

BIS would also like information about the various (commercial and military) applications of foreign products that are derived in whole or in part from U.S.-origin encryption technology or software. In addition, BIS is seeking information from foreign-manufacturers of encryption items about the factors that they or their competitors might consider in deciding to produce or use U.S.-origin encryption technology or software.

Additionally, BIS is interested in specific information (URL addresses, technical specifications, etc.) about the availability of foreign encryption technology and software that is equivalent to U.S.-origin encryption technology and software classified under ECCNs 5E002 and 5D002. Finally, BIS seeks information on the impact on the U.S. information technology manufacturing base and American jobs if encryption products continue to be not subject to the EAR when exported from abroad or reexported to countries other than those listed in Country Group D:1 and E:2, simply by being manufactured under an export license, when identical products manufactured onshore by U.S. companies (or overseas by U.S. subsidiaries pursuant to LE ENC or LE ENC-eligible ''private sector end-users'') are subject to the EAR.

Dated: December 29, 2008.

Christopher R. Wall,

Assistant Secretary for Export Administration.

[FR Doc. E8–31371 Filed 1–5–09; 8:45 am]

BILLING CODE 3510–33–P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

46 CFR Part 197

[USCG–1998–3786]

RIN 1625–AA21

Commercial Diving Operations

AGENCY: Coast Guard, DHS.

ACTION: Advance notice of proposed rulemaking.

SUMMARY: The Coast Guard proposes to amend the commercial diving regulations. We request public comment on industry standards and current practices that might be incorporated in our regulations or accepted as regulatory equivalents; the use of third-party auditing; new requirements for compliance documentation; the adoption of recommendations made following the investigation of a 1996 fatality; and possible additional regulatory revisions. This rulemaking will promote the enhancement of maritime safety which is a strategic goal of the Coast Guard.

DATES: Comments and related material must either be submitted to our online docket via *http://www.regulations.gov* on or before March 9, 2009 or reach the Docket Management Facility by that date.

ADDRESSES: You may submit comments identified by docket number USCG–1998–3786 using any one of the following methods:

(1) *Federal eRulemaking Portal: http://www.regulations.gov*.

(2) *Fax:* 202–493–2251.

(3) *Mail:* Docket Management Facility (M–30), U.S. Department of Transportation, West Building Ground Floor, Room W12–140, 1200 New Jersey Avenue, SE., Washington, DC 20590–0001.

(4) *Hand delivery:* Same as mail address above, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The telephone number is 202–366–9329.

To avoid duplication, please use only one of these methods. For instructions on submitting comments, see the ''Public Participation and Request for Comments'' portion of the **SUPPLEMENTARY INFORMATION** section below.

FOR FURTHER INFORMATION CONTACT: If you have questions on this proposed rule, call Lieutenant Commander Rogers Henderson, U.S. Coast Guard, telephone (202) 372–1411. If you have questions on viewing or submitting material to the docket, call Renee V. Wright, Program Manager, Docket Operations, telephone 202–366–9826.

SUPPLEMENTARY INFORMATION:

Table of Contents for Preamble

I. Public Participation and Request for Comments
A. Submitting Comments
B. Viewing Comments and Documents
C. Privacy Act
D. Public Meeting
II. Abbreviations
III. Background and Purpose

I. Public Participation and Request for Comments

We encourage you to participate in this rulemaking by submitting comments and related materials. All comments received will be posted, without change, to *http://www.regulations.gov* and will include any personal information you have provided.

A. Submitting Comments

If you submit a comment, please include the docket number for this rulemaking (USCG–1998–3786), indicate the specific section of this document to which each comment applies, and provide a reason for each suggestion or recommendation. You may submit your comments and material online, or by fax, mail or hand delivery, but please use only one of these means. We recommend that you include your name and a mailing address, an e-mail address, or a phone number in the body of your document so that we can contact you if we have questions regarding your submission.

To submit your comment online, go to *http://www.regulations.gov*, select the Advanced Docket Search option on the right side of the screen, insert ''USCG–1998–3786'' in the Docket ID box, press Enter, and then click on the balloon shape in the Actions column. If you submit your comments by mail or hand delivery, submit them in an unbound format, no larger than 8½ by 11 inches,

February 28, 2009

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

Subject: Foreign-Produced Encryption Items 0694-XA15

1. 736.2(b)(3) should be revised as follows simply to be consistent with existing encryption controls and to avoid unnecessary assertion of U.S. jurisdiction over the export from a foreign country of a foreign produced item:

General Prohibition Three - Reexport of U.S.-origin technology or software items in the form of the foreign-produced direct product of ~~U.S. technology and software~~ those items (Foreign-Produced Direct Product Reexports). This Prohibition applies to encryption items produced or developed with an item exported or reexported under paragraphs 740.17(a)(1), 740.17(b)(1), or 742.15(b)(3)(i). It also applies to other items subject to the conditions in 736.(b)(3)((i-iii).

(i) Country scope of prohibition. You may not ... reexport ... ~~or export from abroad items~~ technology or software subject to the scope of this General Prohibition Three to ...

(ii) Product scope of ~~foreign made items subject to~~ prohibition. This General Prohibition ~~3~~ Three applies if ~~an item~~ the foreign-produced product meets either the Conditions defining the direct product of technology or software in paragraph (b)(3)(ii)(A) of this section or the Conditions defining the direct product of a plant in paargraph (b)(3)((ii)~~(A)~~ (B) of this section:

(A) Conditions defining direct product of technology or software. ~~Foreign-made items are subject to t~~ This General Prohibition Three applies if ~~they~~ the foreign-made items meet both of the following conditions: ...

(B) Conditions defining direct product of a plant. ~~Foreign-made items are also subject to t~~ This General Prohibition Three also applies if the direct product ~~of~~ is a complete plant or any major component of a plant ...

2. In order to understand the intent of the Notice of Inquiry, it would help if BIS were first to revise 736.2(b)(3) as suggested in recommendation #1 above, to reflect existing controls, and then provide specific language as to how that language would be further revised to reflect the intended additional controls for which impact is desired. The last sentence of the Notice of Inquiry implies that the intent of the Notice is to seek the impact of a new requirement to require a license for the direct product of encryption technology or software which is exported under a license in addition to the existing requirement for a license for the direct product of encryption technology or software which is exported under License Exception ENC. It is difficult to measure that impact without knowing whether licenses in the past for exports from the United States of encryption technology or software have been conditioned on the requirement for an additional license if the encryption technology or software were to be used in a foreign-made 5A002 or 5D002 direct product of that U.S.-origin 5D002 or 5E002. In any event the fix for the last sentence would reasonably exclude from the new requirement use

within the private sector end-user which developed it, for consistency with 740.17(a)(1).

3. It is certainly open to question as to whether existing or proposed additional encryption direct product controls need to apply to reexports to all countries except Canada and the United States, given that all other direct product controls apply only to Cuba and D:1. It is also probably unintended that 736.2(b)(3) does not now apply to Iran, Sudan, or Syria..

SIA | SEMICONDUCTOR INDUSTRY ASSOCIATION

March 9, 2009

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–XA15

Re: Request for Public Comment on Foreign-Produced Encryption Items That Are Made From U.S.-Origin Encryption Technology or Software (74 Fed. Reg. 413)

Dear Ms. Cook:

The Semiconductor Industry Association ("SIA") is the premier trade association representing the U.S. semiconductor industry. Founded in 1977 by five microelectronics pioneers, SIA unites over 70 companies that account for nearly 90 percent of the semiconductor production of this country.

According to the request for public comment, the Bureau of Industry and Security ("BIS") is seeking information on the potential impact of increasing export controls on foreign-made items classified under Export Control Classification Number ("ECCN") ECCN 5A002 or 5D002 for Encryption Items (''EI'') if the items are the direct product of U.S.-origin ECCN 5E002 technology or ECCN 5D002 software.

BIS has also asked for comments concerning the impact this proposed change to the Export Administration Regulations ("EAR") would have on U.S. exporters of encryption technology and software, as well as on foreign manufacturers of products that are derived in whole or in part from U.S.-origin encryption technology or software.

SIA is pleased to respond to the request for public comments. In addition, SIA offers further recommendations on the need for fundamental reform of encryption export controls. SIA previously submitted comments on the need for encryption reforms in its response to BIS's Request for Public Comments on a Systematic Review of the Commerce Control List ("CCL"), Docket Number 070619210-7211-01 (72 Fed. Reg. 39,052).

181 Metro Drive, Suite 450 San Jose, CA 95110
p: 408.436.6000 f: 408.436.6646 www.sia-online.org

The Scope of the Proposed Revision Should Be Clarified to Ensure that the *de minimis* Content Rule is Unaffected

As a preliminary matter, BIS should clearly delineate the difference between the Foreign-Produced Direct Product Rule (EAR § 736.2(b)(3)) and U.S. *de minimis* Content Rule (EAR § 734.4). BIS should make clear that the Foreign-Produced Direct Product Rule is concerned with the "immediate product (including processes and services) produced directly by the use of technology or software" (EAR § 734.3(a)(4)) [emphasis added]; the *de minimis* Content Rule, on the other hand, is specifically concerned with "foreign made items that incorporate U.S.-origin items" (EAR § 734.4) [emphasis added].

The changes now proposed for public comment relate only to an expansion of the Foreign-Produced Direct Product Rule. In order to minimize confusion, BIS should emphasize that the incorporation of encryption parts, components and materials into foreign-made products and the comingling of encryption software with foreign-made products would be unaffected by the proposed change.

U.S.-origin encryption items and software – including most U.S.-origin semiconductor devices that contain encryption functionality – that are incorporated into or comingled with a foreign-made product without further adaptation or modification by a foreign manufacturer qualify for treatment under the *de minimis* Content Rule[1]. In order for U.S.-origin encryption technology or software to fall under the Foreign-Produced Direct Product Rule, the foreign manufacturer must use the U.S.-origin encryption technology or software in some way to create a new and immediate foreign-made product.

For example, if a U.S semiconductor manufacturer exports an integrated circuit containing embedded encryption technology, and that integrated circuit is then incorporated into a foreign-made product which is subsequently reexported, the *de minimis* Content Rule would apply to any reexport of the foreign-made end product. The

---

[1] BIS has created confusion by conflating in a single provision, § 734.4(a)(2), the *de minimis* Content Rule with the Foreign-Produced Direct Product Rule as follows:

> Foreign produced encryption technology that incorporates U.S. origin encryption technology controlled by ECCN 5E002 is subject to the EAR regardless of the amount of U.S. origin content [sic]

Section 734.4(a)(2) appears to make an explicit exception to the *de minimis* Content Rule for U.S. encryption technology that is incorporated into foreign produced encryption technology. But the *de minimis* Content Rule does not address technology, only parts, components, materials and software. In addition, the difference between foreign-made technology that "incorporates" U.S. technology and foreign-made technology that "uses" U.S. technology is obscure at best. Without clarification, the proposed changes could compound the existing ambiguity for encryption with respect to the *de minimis* Content Rule and the Foreign-Produced Direct Product Rule.

Foreign-Produced Direct Product Rule, as it is applied to encryption technology and software, would not be implicated in this example because it is limited to those foreign-produced products that actually make use of U.S. encryption technology or software (e.g., the encryption algorithms or software source code) in such a way that the new foreign-made product is derived from the U.S. encryption technology.

The same holds true for certain U.S.-origin encryption software. The export of a U.S.-origin software package or kit containing encryption technology that is to be, without alteration, (i) embedded into an integrated circuit or (ii) used to enable the existing, but dormant, encryption in an integrated circuit, would not implicate the Foreign-Produced Direct Product Rule for any resulting reexport. In such circumstances, the U.S.-origin encryption technology is not used by the foreign manufacturer in the production of a new, foreign-made product.

In general, encryption technology is useful only for making encryption products. The mere incorporation of an integrated circuit with embedded U.S. encryption technology into a foreign-made product or the comingling of software with a foreign-made product does not result in a new product produced directly by the use of encryption technology or software.

This is a very important distinction to the U.S. semiconductor industry. Semiconductor manufacturers are increasingly embedding encryption functionality into their commercial semiconductor devices and their associated software. These semiconductor devices and software products are commonly shipped to original equipment manufacturers ("OEMs") around the world and incorporated into a great variety of products from computers to mobile telephones to information devices. The foreign OEMs typically do not alter or enhance the encryption technology of these semiconductor devices and software products and do not use the underlying encryption technology to modify the encryption that is resident in the foreign-made product. Hence, for the majority of foreign-made products incorporating semiconductor devices and software with encryption capability, the proposed rule should have no impact.

SIA believes it is important for BIS acknowledge and confirm that the proposed rule would not affect the treatment of U.S. commercial semiconductor devices with encryption capability based on U.S. encryption technology unless the encryption of the foreign-made device is the product of the combination of the original U.S. encryption technology and foreign encryption technology.

If this proposal would in any way reduce the scope of the *de minimis* Content Rule, it could have a massive impact on the U.S. semiconductor industry. It would constitute a totally duplicative and redundant review of encryption for a vast number of reexports. The result would be to impose major competitive burdens on the U.S. semiconductor industry with no accompanying national security benefits.

The U.S. Government Should Not Expand Unilateral Export Controls

Assuming the BIS proposal would apply only when foreign-made encryption products are derived from the use by foreign producers of U.S. encryption technology or software, BIS has set forth no explanation as to why the proposed change to the EAR is necessary. Nor has it demonstrated how the proposal will strengthen U.S. national security. The proposed change appears to be yet another unilateral export control that puts U.S. companies at a competitive disadvantage against foreign companies that face no such export barriers. Instead of creating more unilateral controls, the U.S. Government should work towards harmonizing U.S. export control regulations with other Wassenaar Arrangement member countries. SIA believes that there is no compelling reason to expand the scope of existing U.S. unilateral encryption export controls.

Indeed, the proposed change could have a damaging effect on U.S. competitiveness for those entities engaged in the development of encryption. First, increasing controls may compel U.S. companies to stop producing hardware products incorporating encryption that foreign entities could modify or enhance, thus ceding competitive advantage to foreign companies.

Second, expanding the U.S. export controls on foreign products that are the direct product of U.S.-origin encryption technology or software would create an incentive for foreign producers of encryption items to "design out" U.S.-origin encryption technology and software. The result to U.S. companies of such "designing out" would be a substantial loss of revenue from technology and software licenses.

Additionally, the proposed change is extraterritorial in nature. Extraterritorial export controls are contrary to the principles of international law, create confrontation with other Wassenaar Arrangement member countries and are difficult to enforce. The United States would be trying to use the Foreign-Produced Direct Product Rule to bootstrap its reexport controls onto foreign encryption, a measure that is surely to be strenuously resisted by our allies. This kind of unilateral intrusion can serve only to weaken an already fragile Wassenaar Agreement.

SIA believes that the current export license application and approval process is sufficient to address any potential concerns that the U.S. Government may have regarding the diversion of encryption technology by foreign manufacturers to countries other than Cuba and the D:1 countries.

The U.S. Government Should Fundamentally Reform Controls on Encryption Exports

Instead of expanding export controls on encryption items, the U.S. Government should investigate ways to fundamentally reform controls on encryption exports – widely considered to be the most complicated parts of the EAR – to remove needless barriers to the export of commercial, civil semiconductor devices.

Currently, semiconductor devices that are largely decontrolled under Category 3 and Category 5 Part 1 of the CCL or are EAR99, face the risk of being captured under Category 5 Part 2 controls due to the inclusion of encryption. This will become an increasing problem as semiconductor manufacturers are embedding encryption functionality into a larger portion of their commercial, civil semiconductor products.

As high-volumes of civil, commercial semiconductor devices increasingly qualify under Category 5 Part 2, they will become variously subject to a number of onerous licensing, notification and/or reporting requirements not encountered in existing classifications outside of Category 5 Part 2. The prospect of this collision threatens to chill U.S. hardware security innovation, disrupt long-standing global distribution models, and adversely impact U.S. research and development.

In order to avoid an impending re-control of high-volume, commercial semiconductor devices, BIS should undertake a review of encryption controls as they apply to such devices and promulgate new measures to ensure that no new barriers to the global distribution of semiconductor devices are implemented. Consistent with this end, SIA recommends the BIS implement the following encryption control reforms.

Grant mass market treatment to commercial components and related firmware and software that are designed and intended to be used in mass market products

BIS should establish a policy of allowing mass market treatment for components that are: (i) are classified as encryption items under Category 5 Part 2; (ii) intended for use in mass market products; and/or (iii) generally or widely available to the public through any means of distribution. The policy should also grant such mass market treatment to related firmware and software. Finally, the regulations should allow exporters to self-classify all mass market items, technology, software and firmware under ECCN 5X992 without a U.S. government review.

Revise the definition of mass market to remove any doubt over coverage of "mass market" distribution channels that may not be viewed as retail selling points

BIS should remove the word "retail" from the current description or revise the description in such a way to include the many semiconductor products that are sold via outlets that may not be perceived as retail in nature, even though these products are "mass market" in every meaningful sense of the term.

Eliminate Review Requirements in EAR §742.15 for Mass Market and ENC-Unrestricted Products

BIS should eliminate the detailed review requirement for encryption software, hardware, components and cryptographic functions that do not qualify for exclusion from

review under EAR § 742.15(b)(3)(i)-(iii), which must be conducted prior to an item being granted either mass market status or qualification under license exception ENC.

Reclassify unpackaged semiconductor die that contain encryption

Unpackaged semiconductor die that contain encryption capability currently classifiable under ECCN 5A002 should be reclassified as Category 3 or Category 5 Part 1 or if subject under Category 5 Part 2, ECCN 5A992. The related wafers should not be controlled under the EAR.

* * *

SIA appreciates the opportunity to comment on the proposed regulatory change and looks forward to continuing its cooperation with BIS on this subject. Please feel free to contact the undersigned if you have questions regarding these comments.

Sincerely,

David Rose
Chairman
SIA Export Controls Committee

March 9, 2009

Sent via email to: publiccomments@bis.doc.gov

U.S. Department of Commerce
Bureau of Industry and Security
Regulatory Policy Division
Office of Exporter Services
14th St. and Constitution Ave. NW, Room 2705
Washington, DC 20230

RE: Federal Register: January 6, 2009 (Volume 74, Number 3)
RIN 0694-XA15

Request for Public Comment on Foreign Produced Encryption Items That Are Made From U.S.-Origin Encryption Technology or Software

Dear Sir or Madam:

TechAmerica is pleased to provide comments on the above-referenced Notice of Inquiry published by the Bureau of Industry and Security. Our 1500 members believe that the proposed expansion of encryption export controls contemplated in the notice is unwarranted and should be supplanted with efforts to implement fundamental reform of existing encryption control regulations.

Background

The subject notice describes a proposal to expand controls on foreign-made products that are derived in whole or in part from U.S.-origin encryption technology or software. In certain cases, foreign-produced products (those that would be classified under Export Control Classification Number (ECCN) 5A002 or 5D002), which are the direct product of U.S. technology and software (ECCN 5E002 technology or ECCN 5D002 software), currently require a license or license exception for export or reexport from abroad to Cuba or Country Group D:1 countries. The license requirement arises from Export Administration Regulations (EAR) General Prohibition Three (EAR § 736.2(b)(3)), which applies to countries controlled for national security purposes. For matters relating to encryption, that includes software classified for export under ECCN 5D002, and technology under ECCN 5E002. BIS is considering a possible revision to General

Prohibition Three that would expand or alter the scope of the requirement by requiring either a license or applicable exception for exports or reexports of foreign-produced direct products of 5D002 software or 5E002 technology from the country of manufacture ***to all countries*** except the United States or Canada, rather than just Group D:1 countries or Cuba as is currently the case. All such exports would be subject to the requirements of EAR §§ 742.15 (“EI” encryption items), 742.4 (“NS” national security), or the review requirements found in section 740.17 (License Exception ENC). Although the ENC exception would be available to foreign manufacturers, BIS notes that the reporting requirements associated with that exception would not be imposed on foreign producers.

It should be noted that the proposed revision described above would apply to the foreign direct product of ECCN 5E002 technology and 5D002 software exported under license, not to the foreign direct product of technology and software exported under License Exception ENC of section 740.17 of the EAR. (All foreign-produced direct product of technology or software exported under License Exception ENC under either paragraph (a)(1) (for internal development of new products by a `license-free zone' (Supplement No. 3 to part 740) ``private sector end-user'') or (a)(2) (to a ``U.S. subsidiary'' for internal use or development) are currently subject to the EAR by the terms of the notes to paragraphs (a)(1) and (a)(2)).

BIS is seeking information on the impact of making the foreign-produced direct product of U.S.-origin encryption technology or software, classified under ECCN 5A002 or 5D002 subject to the EAR if exported from the country of manufacture to ***any*** destination (except the United States or Canada). Specifically, BIS is seeking public comment on the impact such a revision to section 736.2(b)(3)(i) would have on both U.S. manufacturers of encryption technology and software and foreign manufacturers of products (including those under contract to U.S. companies) that are derived in whole or in part from U.S.-origin encryption technology or software.

Analysis

TechAmerica respectfully submits that there is no compelling reason to expand the scope of U.S. unilateral encryption export controls in the proposed manner since this proposed change could increase the existing burdens of complying with multiple sets of applicable foreign and U.S. laws. Under the current provisions of section 736.2(b)(3), if ECCN 5E002 technology is exported under an export license for purposes of offshore manufacture of an encryption item that has previously been submitted to the U.S. Government for technical review and has been made eligible for export under License Exception ENC, the foreign-produced direct product of the technology is not subject to the EAR unless: (1) it is exported from the country of manufacture to a destination in Country Group D:1 or E:2 (Cuba); or (2) it is exported from the United States after having been shipped to the United States from the country of manufacture. TechAmerica submits that the existing export licensing application and approval process, coupled with the existing requirement that an item has previously been submitted to the U.S. Government for review, should be more than sufficient to address any potential concerns

the U.S. government may have with respect to exports by foreign manufacturers to countries other than Cuba and the existing D1 countries.

Encryption controls already take up an increasing amount of the time and resources of U.S companies. These U.S. companies are competing aggressively with non-U.S. companies which are not subject to U.S. encryption controls, including those that are imposed on a unilateral basis. Existing U.S. encryption controls apply to more and more products as the industry has incorporated commonly available encryption functionality into most software, computer and telecommunications equipment, and components used in such equipment, such as microprocessors. Increasingly burdened by complex product classification and reporting requirements and devoting more and more company resources on ongoing compliance efforts, U.S. industry has been advocating fundamental encryption reform, favoring simplification of the current complicated system of encryption export controls, harmonizing U.S. interpretations with those of our Wassenaar partners, and most importantly eliminating certain burdensome controls and requirements imposed by the U.S. government on a unilateral basis.

The proposed rule is contrary to the ongoing efforts to minimize the impact of U.S. unilateral export controls, especially as they apply to encryption, since there are increasingly more and more non-US sources for encryption software and technology. Foreign manufacturers in countries such as India, Singapore, South Korea and Taiwan, just to name a few countries, have had and continue to have access to non-US sources for encryption software and technology that can be used to manufacture encryption items outside of the U.S. Generally, when foreign manufacturer consignees in these and other countries receive encryption software or technology pursuant to an export license issued by the BIS, the consignees are put on notice that the products developed using the licensed encryption items are subject to the EAR and would require prior written authorization from BIS to re-export, resale or transfer, unless already authorized by the EAR. In addition, there already exists a requirement for the ultimate consignee to execute a letter of assurance. Additional restrictive riders and conditions have also been imposed on a case by case basis pursuant to the existing licensing process. A large extent of the encryption software and technology licensed by U.S. companies to foreign parties is available as open source from repositories like OpenSSL.org, OpenSSH.org, and various Linux distributions. Furthermore, much of the encryption software and technology used by U.S. companies is developed in industry forums like the IEEE, the IETF and other, similar organizations. Requiring foreign manufacturers in these countries, as well as other countries, to comply with yet an additional layer of U.S. unilateral export controls just does not make sense.

Meanwhile, the inclusion of encryption reform in Presidential National Security Directive 55 stimulated more high-level attention to the encryption reform issue, but nothing has really been done to date to implement most of the essential recommended reforms. As part of its implementation of Presidential National Security Directive *55* issued in January 2008, BIS has published its latest interim final rule revising the EAR's encryption provisions. *73 Fed. Reg. 57495* (Oct. 3, 2008). This rule helped in cleaning up to some degree the extremely convoluted encryption regulations. Yet, even in light of

these recent changes, the EAR's encryption provisions remain the most complicated parts of the EAR.

The notice of inquiry is not consistent with past simplification efforts and would seem to be directly contrary to the types of fundamental reforms to the existing regulations industry has been advocating for some time now. In fact, the inquiry represents an expansion of the scope of the existing regulations. TechAmerica does not believe there is any compelling reason to expand the scope of existing encryption regulations, especially those that are unilateral in nature, at a time when there is still a pressing need for these regulations to be reformed in fundamental and meaningful ways that would help eliminate the negative competitive impact these regulations continue to have on U.S. industry, which is facing intense competition from foreign companies during challenging economic times characterized by unprecedented global market conditions. Rather than pursuing this type of expansion of U.S. unilateral encryption regulations, BIS should increase its efforts towards fundamental reform of the existing regulations. TechAmerica has gone on record many times with specific ways the current encryption regulations can be changed in ways that would help U.S companies to remain competitive vis-a-vis their foreign competitors. The notice of inquiry is clearly not consistent with the positions TechAmerica has been advocating for a number of years.

TechAmerica appreciates the efforts by BIS and other agencies to amend the encryption export regulations to streamline and clarify certain encryption export control requirements. In particular, we appreciate the willingness of BIS to regularly meet with industry and engage in substantive dialogue on the policy and regulatory implications of these controls. However, our member companies stress that additional work is required to deliver fundamental reforms that significantly eliminate administrative burdens and obstacles to US competitiveness and innovation. The concept of reforms for encryption is valuable, long overdue and a first step toward keeping U.S companies competitive.

Recommendations

While recent modest reforms are a step in the right direction, far-reaching changes to U.S. encryption export controls are needed in the near future. Such changes should take account of the major encryption trends and related export control implications raised by various high technology industry executives during the government / industry encryption control forum held at the U.S. Department of Commerce on February 20, 2008 and a subsequent meeting with BIS and NSA officials on October 16, 2008. In particular, the reform of encryption controls should include measures that:

1. Eliminate reporting requirements.
2. Eliminate review requirements for mass market and ENC-unrestricted products.
3. Enact classification and control reforms, including but not limited to elimination of controls on publicly accessible software and technology, removal of controls on Open Cryptographic Interfaces, and eliminating controls on components that are incorporated into mass market products or are otherwise widely available.

For a comprehensive list of TechAmerica's recommendations for fundamental reform, please refer to the paper attached, entitled "TechAmerica Recommendations for Encryption Control Reform."

Thank you for the opportunity to provide comments on this Notice of Inquiry. We believe these comments are consistent with the recent National Academies study Beyond "Fortress America" National Security Controls on Science and Technology in a Globalized World (2009). This study states "The national security controls that regulate access to and export of science and technology are broken. As currently structured, many of these controls undermine our national and homeland security and stifle American engagement in the global economy, as well as research in science and technology. Fixing these controls does not mean putting an end to them, but implementing reforms based on the realities of the risks and opportunities of today's threats to the nation."

Sincerely,

Ken Montgomery
Senior Director, International Trade Regulation

Attachment: TechAmerica Recommendations for Encryption Control Reform – March 9, 2009

Recommendations for Encryption Control Reform

1. Eliminate reporting requirements.
2. Eliminate review requirements for mass market and ENC-unrestricted products.
3. Enact classification and control reforms, including elimination of controls on publicly accessible software and technology and on Open Cryptographic Interfaces.

TechAmerica endorses the technical recommendations made by the Department of Commerce's Regulation and Procedures Technical Advisory Committee on Sept. 26, 2006, in particular as it identifies priority areas for specific, immediate action.

With this in mind, TechAmerica makes the following general recommendations. **A list of detailed encryption recommendations is included as Attachment 1.**

Eliminate Reporting Requirements

Extensive semi-annual reporting continues to be required under EAR Section 740.17 (e) for cryptographic items shipped under License Exception ENC to all destinations except Canada.

This is a unilateral requirement, in the sense that no other member of the Wassenaar control regime demands it. From the business perspective, it is costly and time consuming to collect and report the data. However, the most compelling reason for eliminating this reporting requirement is risk of inadvertent error: under current penalty levels, mistakes made in such reporting can in principle be subject to up to $50,000 each in civil penalties.

The burden for complying with these reporting requirements falls disproportionately on small, specialized exporters. Cryptographic functions are now found in a wide variety of software applications that would otherwise have little or no export controls. Many U.S. domestic producers of such products are often completely unaware of complex export control requirements as their products begin being shipped or downloaded across national borders. Often past violations show up during due diligence reviews as small companies are acquired by larger firms.

Initially, these requirements were intended to provide the National Security Agency (NSA) and the rest of the intelligence community with a picture of cross-national demand for cryptographic products and product flows. However, after a decade of such reporting, this purpose has long since become redundant, and the data obtained is not always verifiable.

As the use of cryptographic functions has proliferated in the last ten years, so have products subject to reporting requirements. It is not clear whether at current levels NSA can use or even effectively review the mass of data that is being fed to it as a result of this outdated requirement.

TechAmerica feels that the cost and risk to exporters of continuing these reporting requirements now far outweighs any theoretical intelligence benefits. We further urge that these reporting requirements be **eliminated.** Past attempts to create complex exception categories have only compounded the cost and risk of reporting.

Eliminate Review Requirements for Mass Market and ENC-Unrestricted Products

Most current encryption software, hardware, and components, as well as products including cryptographic functions, are subject to detailed review requirements in order to qualify for either mass-market status or for shipment under license exception ENC. TechAmerica members feel that the utility of this requirement has largely eroded over time, and should be eliminated.

With all other parts of the U.S. export control system, including munitions control, exporters are permitted to self classify. Classification decisions by exporters are subject to review and verification at any time. Cryptographic products are unique in that most must be reviewed by U.S. Government agencies prior to becoming eligible for export.

This review requirement is unique among Wassenaar allies, which control the same list of products and which have substantial numbers of indigenous producers. As is the case with reporting requirements, this mandatory classification procedure may have had some justification when initially imposed ten years ago. However, since then it has become a mechanical requirement which has taxed resources not only among companies, but among the BIS and NSA staff that must process thousands of reviews of commercial products each year.

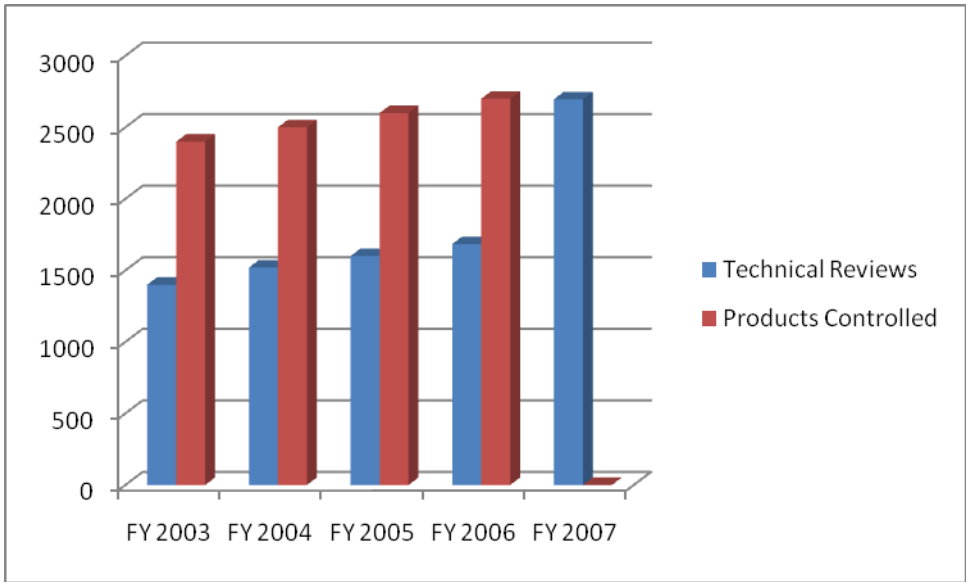
As Figure 1 below demonstrates, the number of reviews processed by BIS as well as the number of products affected by such reviews has increased substantially over the past five fiscal years. During this period reviews have increased by over 92%, and now constitute over a third of the total classifications issued by BIS for **all** dual-use products controlled by the Department of Commerce.

These increases have continued into the current ('08) fiscal year, and have resulted in a dramatic increase in backlogs for BIS and NSA reviews, consuming resources that are

already tight. This backlog in turn translates into delays in issuing these mandatory classifications, and needless disruption in product introduction and shipment. In addition the additional processing time required by BIS and NSA constitutes diversion of government resources from higher priority work.

Figure 1

BIS Encryption Technical Reviews and Products Controlled
Fiscal Years 2003-2007



Source: BIS Annual Reports
Note: Products controlled not reported in 2007

Review requirements are repetitive, being required of essentially the same encryption function applied in different application software packages. As "different" has historically been defined as any change in code or functionality, software variants that are fundamentally similar but which have undergone improvements or modifications even in capabilities unrelated to encryption are required to undergo the same onerous review process.

Review requirements are also affecting an ever widening range of products, as basic encryption now appears in a very wide range of applications, including medical devices, operating systems, word processors and tape storage. Almost all modern software has encryption functions, virtually all of them of the same types that have been reviewed before in thousands of other products.

Many of the serious burdens that the current approach to review requirements have created are a direct result of the sea change that has occurred in the need for and use of encryption in commercial applications in the last decade. In order to adapt the system to contemporary technological and market conditions, TechAmerica urges that the review requirement be eliminated.

Enact Classification and Specific Control Reforms

a. Eliminate Controls on Publicly Accessible Software and Technology

Encryption is also unique in that items in the public domain, or that are generally available to the public, remain subject to the EAR, meaning that they retain controls to some destinations. Specifically, notifications requirements and controls remain on embargoed destinations.

These controls are again a legacy of encryption's pre-1997 history as a munitions item. At that time, steps were taken to prevent public release of cryptographic code on the grounds of their unique sensitivity. However, these conditions no longer hold, not only because of the great increase in the amount of encryption software available commercially, but also because of the large amount made publicly accessible subject to minimal controls since 1996.

While the EAR (reflecting original policy pronouncements), states that the reason for this unique treatment of publicly accessible software is that the national security concern is centered on what the code does, rather than what it says, this rationale would apply to many categories of controlled software. However, encryption is the unique category where such special controls apply.

The disruptive effect of these controls is greatly disproportionate to any national security value that they may now provide. Companies now actively pursue an "open source" strategy, in which they intentionally make their software publicly accessible via open source licenses. This is done so that their products may be quickly accepted by developer and other target groups. To the extent that cryptographic functions are an intrinsic feature of their products (e.g., operating systems), even residual controls on these open source uncontrollable products have disproportionate and significant competitive effects.

In order to bring controls on cryptographic software and technology in line with other controls, TechAmerica recommends that the exemption to their removal from EAR jurisdiction be eliminated.

b. Grant Mass Market Treatment to Components and Related Software for Mass Market Products

Mass market treatment should be accorded to commercial components classifiable under Category 5, Part 2 (including related firmware/software/technology) that are designed

and produced for use in mass market products or that are otherwise generally available. If a PC, cell phone or other widely available product enjoys mass market status under the regulations, the components and related firmware/software/technology designed for such products should not be treated differently. Such treatment is highly important and relevant because components are increasingly incorporating cryptographic functions to meet customer demands for security and to protect critical information infrastructure in general.

Semiconductors and other widely available commercial components of mass market products are inherently non-military and designed and intended to serve as the basic building blocks of the global information infrastructure. For example, the United States and the Wassenaar Arrangement have recognized the non-threatening nature of commercial processor components, removing them from civilian end use controls. Components are produced in high volumes for distribution all over the world. While not sold over the counter at the same level as the mass market products into which they are incorporated, commercial components are nevertheless generally available from worldwide distributors.

The civilian nature of these items is enhanced by the fact that many components comply with ISO, IEEE, FIPS and PKCS standards, which only support publicly available civilian end-use cryptographic algorithms. Typical applications for products containing such components include home/office networking and home/car access control.

Mass market treatment for components for products with mass market status was previously considered by the U.S. Government under the "retail" classification during the encryption regulation reform (1999-2002). Unfortunately, upon the publication of the final rule that revised the vernacular to "mass market," the ability to apply mass market treatment for components used in mass market products was not included.

Meanwhile, there is a significant un-level playing field with regard to the international treatment of "EI" components in mass market products. A number of countries treat these items as 5X992, while the U.S. treats them as 5X002. Such disparate treatment is contrary to the multilateral controls intended by all countries seeking similar export control goals, as well as how other countries apply the Mass Market Crypto Note for commercial components used in mass market items.

TechAmerica therefore respectfully requests that the U.S. Government establish a policy of allowing mass market treatment for components (and related firmware/software) that are classifiable under Category 5, Part 2 and that are used in mass market products or are otherwise generally available. This is consistent with the direction of the components-related policy we thought had been agreed by the U.S. Government. The policy should include:

1. Allowing self-classification under 5X992 of all mass market "items" without any one time review, including technology and software/firmware for mass market products.

2. Clarifying the scope of the mass market Cryptography Note and ensuring that its scope covers commercial semiconductors/integrated circuits and related software, firmware and technology.

c. Eliminate controls on Open Cryptographic Interface ("OCI")

The OCI restriction is a unilateral U.S. restriction not set forth in the Wassenaar Arrangement International List or other restrictions. The OCI restriction does not apply to open source products, of which there are now millions around the world. Open Source software has OCI by its nature and can be exported under License Exception TSU worldwide (except for AT only controlled destinations) with only a notification. Thus, the OCI restriction creates a competitive disadvantage for U.S. companies with proprietary software.

d. *Eliminate Controls on Open Crypto Aware*

Products that simply call on encryption but do not contain native encrypt coding should be exempt from notification and review. Requiring notification on handshake or calls to cryptography, referred to as "Crypto Aware" is burdensome since microwaves, hotel Mini bars, TVs, videogames, and other common household articles and commercial wireless communication devices can have these functionalities in today's domestic and export markets.

e. *Eliminate Controls on Dormant Encryption*

Exporters are currently required to complete a one time technical review for dormant encryption items prior to export under 5X992. Under the EAR, "dormant cryptography" refers to items which, at the time of export, contain embedded cryptographic parts or components which are rendered functionally inert or inactive by design. This dormant cryptography must be "activated" or "enabled" (typically using special components or software purchased separately) by the manufacturer before it can be used to encrypt data. TechAmerica believes that dormant cryptography controls should be eliminated where cryptographic functionality in products like semiconductors is rendered inactive by design and can only be activated via proprietary software or other mechanisms, which are otherwise variously controlled under ECCN's such as 5X992 and 5X002.

f. *Expand the Coverage of EAR Part 740.17 to Cover Third Party Contractors*

The existing license exceptions set forth in sections 740.17(a)(1) and 740.17(b)(1) should be expanded to include any third party contractors used by the parent company or their foreign subsidiary as long as the specific conditions set forth under the license exception are met. Because the current exception allows technology transfers to individuals/persons who are "contractors" or "interns", as those terms are currently defined in the EAR, certain legal entities/juridical persons should be afforded the same treatment under the regulations, subject to the license exception conditions of Part 740.17, i.e., the contractor is only permitted to avail itself of the technology for internal purposes, and hence cannot share the technology with another party, unless such a party

is afforded the same status. Further, the contractor must only use the technology for the sole benefit of the U.S. company and its foreign subsidiaries and in compliance with the terms and conditions imposed on the contractor by such entities. Finally, any product developed by such entities and its contractor using the transferred technology would remain subject to the encryption regulations.

Attachment 1: Specific Priority Recommendations for Streamlining Encryption Controls

Note: Recommendations taken from the September 29, 2006, RPTAC letter are in italics.

Reporting Requirements

1. Eliminate EAR 740.17(e) reporting requirements.

Review Requirements

1. Eliminate review requirements for mass-market and ENC-unrestricted products, including specially-designed components.

Classification and Control Issues

1. Eliminate controls (i.e. EAR jurisdiction) over publicly available encryption software and technology.
2. Narrow the U.S. definition of mass-market to conform to Wassenaar Cryptography Note 3.
3. Classify short-range wireless products and secure network management products as 5X992.
4. Eliminate review of electronic transfer of information that is copyright protected under the current Note 3 for Digital Rights Management.
5. Eliminate review for bundling of products that have been previously classified. This would apply to products bundled for marketing purposes, rather than for those that have undergone a fundamental change.
6. Eliminate review for products that contain decryption functions only.
7. Eliminate the notification requirement for Crypto-Aware products/products that call on encryption including those that have no Crypto code.
8. Eliminate requirements to notify BIS when exporting beta test software under License Exception TMP.
9. Dormant cryptography controls should be eliminated where cryptographic functionality in products like semiconductors is rendered inactive by design and can only be activated via proprietary software or other mechanisms.
10. The existing license exceptions set forth in sections 740.17(a)(1) and 740.17(b)(1) should be expanded to include any third party contractors used by the parent company or their foreign subsidiary as long as the specific conditions set forth under the license exception are met.
11. *Eliminate vestiges of the "virtual ITAR" provisions included in the 1996 controls (e.g., restrictions on technical assistance, de minimis eligibility, foreign availability ineligibility, etc.).*

12. *Eliminate restrictions on open cryptographic interfaces in proprietary encryption products.*
13. *Treat "EI" components and software that are designed and produced for mass-market items, or that are otherwise generally available, as mass-market 5X992 items rather than ENC-restricted.*
14. *Classify ENC-unrestricted 740.(b)(3) eligible hardware and software under ECCN's 5A992 and 5D992.*
15. *Eliminate ECCN 4A001.b and 4D003.c as redundant and confusing.*

For additional information, please contact:

Ken Montgomery
Sr. Director, International Trade Regulation
ken.montgomery@techamerica.org
202-682-4433