

Public Comments on Encryption Rule
Revisions to Encryption Items – [65 FR 2492](#)

- Enc 1. IBM Corporation
- Enc 2. Lyndon D.S. Marquez
- Enc 3. Bill Root
- Enc 4. Sun Microsystems
- Enc 5. Mercantec
- Enc 6. Hewlett-Packard
- Enc 7. Rider Bennett Egan & Arundel (Michael J. McGuire)
- Enc 8. Information Technology Association of America
- Enc 9. Americans for Computer Privacy
- Enc 10. Microsoft Corporation
- Enc 11. ILink Global
- Enc 12. Semiconductor Industry Association
- Enc 13. United States Council for International Business
- Enc 14. Alliance for Network Security
- Enc 15. Citigroup
- Enc 16. Regulations and Procedures Technical Advisory Committee
- Enc 17. Industry Coalition on Technology Transfer
- Enc 18. Hogan & Hartson LLP (Daniel B. Poneman)
- Enc 19. American Electronics Association



Federal Register

Friday

January 14, 2000

Part III

Department of Commerce

Bureau of Export Administration

15 CFR Parts 734, 740, et al.

Revisions to Encryption Items; Interim
Final Rule

DEPARTMENT OF COMMERCE**Bureau of Export Administration**

5 CFR Parts 734, 740, 742, 770, 772, and 774

[Docket No. 000110010-0010-01]

RIN: 0694-AC11

Revisions to Encryption Items

AGENCY: Bureau of Export Administration, Commerce.

ACTION: Interim final rule; request for comments.

SUMMARY: This rule amends the Export Administration Regulations (EAR) to allow the export and reexport of any encryption commodity or software to individuals, commercial firms, and other non-government end-users in all destinations. It also allows exports and reexports of retail encryption commodities and software to all end-users in all destinations. Post-export reporting requirements are streamlined, and changes are made to reflect amendments to the Wassenaar Arrangement. This rule implements the encryption policy announced by the White House on September 16 and will simplify U.S. encryption export rules. Restrictions on terrorist supporting states (Cuba, Iran, Iraq, Libya, North Korea, Sudan or Syria), their nationals and other sanctioned entities are not changed by this rule.

DATES: This rule is effective January 14, 2000. Comments must be received on or before May 15, 2000.

ADDRESSES: Written comments on this rule should be sent to Frank J. Ruggiero, Regulatory Policy Division, Bureau of Export Administration, Department of Commerce, P.O. Box 273, Washington, DC 20044. Express mail address: Frank J. Ruggiero, Regulatory Policy Division, Bureau of Export Administration, Department of Commerce, 14th Street and Pennsylvania Ave, N.W., Room 2705, Washington, DC 20230.

FOR FURTHER INFORMATION CONTACT: James A. Lewis, Director, Office of Strategic Trade, at (202) 482-0092.

SUPPLEMENTARY INFORMATION:**Background:**

On September 16, 1999, the U.S. announced a new approach to its encryption export control policy. This approach rests on three principles: A technical review of encryption products in advance of sale, a streamlined post-export reporting system, and a process that permits the government to review exports of strong encryption to foreign governments. The full range of national

interests continue to be served by this new policy: supporting law enforcement and national security, protecting privacy and promoting electronic commerce. Encryption export controls will be simplified and U.S. companies will have new opportunities to sell their products in the global marketplace.

This regulation also implements changes for encryption items made by the Wassenaar Arrangement, including: conversion of Category 5—Part 2 (Information Security) of the Commerce Control List (CCL) to a positive list; creation of a Cryptography Note and removal of encryption software from the General Software Note; decontrol of 64-bit mass market software and commodities, including components; and decontrol of certain 512-bit key management products.

The EAR is amended as follows:

1. In § 734.2, Important EAR Terms and Principles, unrestricted encryption source code under § 740.13(e), commercial encryption source code under § 740.17(a)(5)(i) and retail products under § 740.17(a)(3) are exempted from Internet download screening requirements in § 734.2(b)(9)(iii). A revised screening mechanism for other encryption products exported to government end-users is added. Please note that § 734.2(b)(9) contains the relevant definitions for the export of encryption source code and object code software. In addition, cross-referencing changes are made to §§ 734.7, 734.8, and 734.9.

2. In § 740.13, Technology and Software Unrestricted, changes are made to reflect amendments to the Wassenaar Arrangement. Specifically, encryption software is no longer eligible for mass market treatment under the General Software Note. Encryption commodities and software are now eligible for mass market treatment under the new Cryptography Note in Category 5—Part 2 of the CCL. This Note multilaterally decontrols mass market encryption commodities and software up to and including 64-bits. Such products, after review and classification by BXA, are classified under Export Commodity Control Numbers (ECCNs) 5A992 or 5D992, thereby releasing them from "EI" (Encryption Items) and "NS" (National Security) controls, and making them eligible for export and reexport to all destinations (see § 742.15(b)(1)(iii) of the EAR). Once mass market encryption software and commodities are released from "EI" controls they may be eligible for *de minimis* and publicly available treatment (see part 734 of the EAR).

3. Also in § 740.13, to, in part, take into account the "open source" approach to software development,

unrestricted encryption source code not subject to an express agreement for the payment of a licensing fee or royalty for commercial production or sale of any product developed using the source code can, without review, be released from "EI" controls and exported and reexported under License Exception TSU. Intellectual property protection (e.g., copyright, patent, or trademark) would not, by itself, be construed as an express agreement for the payment of a licensing fee or royalty for commercial production or sale of any product developed using the source code. To qualify, exporters must notify BXA of the Internet location (e.g., URL or Internet address) or provide a copy of the source code by the time of export. These notifications are only required for the initial export; there are no notification requirements for end-users subsequently using the source code. Notification can be made by e-mail to crypt@bxa.doc.gov.

Review and classification are not required for foreign made products using this source code. Moreover, under § 744.9, exporters of unrestricted encryption source code are not restrained from providing technical assistance to foreign persons working with such source code. In addition, exporters of source code are not subject to Internet download screening requirements under § 734.2(b)(9)(iii). Posting of the source code on the Internet (e.g., FTP or World Wide Web site), where it may be downloaded by anyone, would not establish "knowledge" (as that term is defined in the EAR) of a prohibited export or reexport. Such posting would not trigger "red flags" necessitating the affirmative duty to inquire under the "Know Your Customer" guidance provided in Supplement No. 3 to Part 732. Otherwise, compliance with EAR requirements as to prohibited exports and reexports still apply.

4. In § 740.17, Encryption Commodities and Software, language is added to implement the Administration's new policy. License Exception ENC (Encryption Commodities and Software) is revised as follows:

a. Encryption items under ECCNs 5A002, 5D002 or 5E002 can be exported and reexported to foreign subsidiaries of U.S. companies, including the transfer of encryption technology to their foreign employees in the U.S., without technical review and classification. Any items developed by the U.S. company for sale or retransfer outside the U.S. company are subject to review and classification by BXA. Foreign companies with subsidiaries in the U.S.

can apply for Encryption Licensing Arrangements (ELAs) to obtain treatment equivalent to that extended to foreign subsidiaries of U.S. parent companies.

b. A new paragraph, entitled "Encryption commodities and software," is created to implement the broad authorization for encryption exports contained in the September 16 announcement. Under this paragraph, any encryption commodity, software or components of any key length classified under ECCNs 5A002 and 5D002 can be exported and reexported to individuals, commercial firms and other non-government end-users. Previous sector-specific liberalizations for banks and financial institutions, health and medical end-users and on-line merchants are subsumed into this new paragraph. Previous restrictions limiting exports to foreign commercial firms for internal company proprietary use are removed. In addition, foreign products developed from encryption components, while subject to the EAR, do not require review and classification prior to reexport. Exports and reexports to government end-users require a license.

c. A new paragraph entitled "Retail encryption commodities and software" is created. Retail encryption commodities and software under ECCNs 5A002 and 5D002 are those which are widely available and can be exported and reexported to any end-user (including any Internet and telecommunications service provider), to provide products and services (e.g., e-commerce, client-server applications, or software subscriptions) to any end-user. The criteria to determine eligibility as a retail product include functionality, sales volume, distribution methods, ability to modify products and requirements for substantial support by the supplier. Substantial support for retail encryption commodities and software would mean a service contract or other significant vendor support beyond what is minimally necessary for the product's operation. Help desk calls are not considered substantial support. Refer to § 740.17(a)(3) of the EAR for a detailed definition of retail encryption commodities and software (which may include components as well as encryption source code) and an illustrative, yet non-restrictive, list of such products. Finance-specific, 56-bit non-mass market products with a key exchange greater than 512 bits and up to 1024 bits, network-based applications and other products which are functionally equivalent to retail products are considered retail products.

Encryption software patches for retail products remain eligible under License

Exception TSU and certain upgrades for retail products, where the cryptographic functionality has not changed, are authorized under License Exception ENC. Also, foreign products developed from retail encryption components, while subject to the EAR, require no technical review or license authorization prior to reexport; however, post-export reporting requirements exist. Retail encryption products are not subject to Internet download screening requirements listed in § 734.2(b)(9)(iii); however, all other general prohibitions, such as those for the seven terrorist-supporting countries, apply.

d. A new paragraph is added to License Exception ENC entitled "Telecommunications and Internet service providers." Telecommunications and Internet service providers can obtain and use any encryption product under this license exception to provide encryption services, including public key infrastructure services for the general public; however, provision of services specific to governments (e.g., running a virtual private network for a government agency), will require a license.

e. A paragraph entitled "Commercial encryption source code and general purpose encryption toolkits" is added. You may export and reexport general purpose encryption toolkits and encryption source code, not released under § 740.13, classified under ECCN 5D002, subject to the following provisions:

(1) Commercial encryption source code which would be considered publicly available under § 734.3 and which is subject to an express agreement for the payment of a licensing fee or royalty for commercial production or sale of any product developed using the source code, can be exported or reexported to any end-user. This source code, which includes some "community" source code, may be exported or reexported without review and classification, provided you have submitted to BXA, by the time of export, written notification of the Internet location (e.g., URL or Internet address) or a copy of the source code. These notifications are only required for the initial export; there are no notification requirements for end-users subsequently utilizing the source code. The notification can be sent via e-mail to crypt@bxa.doc.gov.

(2) Encryption source code which would not be considered publicly available may be exported or reexported to any non-government end-user after review and classification by BXA.

(3) General purpose encryption toolkits may be exported and reexported after review and classification by BXA to any non-government end-user.

Note to this paragraph: Neither review and classification nor reexport licensing requirements are required under this section for foreign finished products using U.S.-origin source code, toolkits and components; yet the foreign finished products remain subject to the EAR. Post-export reporting for foreign products developed for commercial sale with source code and general purpose encryption toolkits exported under this paragraph is limited to the name and address of the foreign manufacturer and certain non-proprietary technical information about the foreign product. Exporters should always be aware of the General Prohibitions identified in part 736 of the EAR (e.g., prohibited exports and reexports to Denied Persons and embargoed destinations).

f. Grandfathering and Upgrades in Key Length: Encryption commodities and software previously approved under a license, or eligible for License Exception ENC, excluding items previously approved only to U.S. subsidiaries, can be exported and reexported to non-government end-users without additional review and classification. Previously classified financial-specific or certain 56-bit products are eligible for export and reexport to any end-users without an additional classification. All previously classified products can be upgraded provided the only change is in the key length used for confidentiality and key exchange. Exporters must, prior to export of an upgraded product, certify in a letter from a corporate official the only change is the key length for confidentiality or key exchange algorithms and there is no other change in cryptographic functionality.

g. Exporters may export any product to any non-government end-user 30 days after receipt by BXA of a complete classification request, unless otherwise notified by BXA. No exports to government end-users are allowed under this provision and BXA reserves the right to suspend eligibility in those instances where requested additional information has not been provided or when the classification review is not proceeding in an appropriate fashion.

h. Reporting requirements under License Exception ENC are eliminated for many encryption items. Remaining reporting requirements are streamlined to reflect business models normally used by exporters. Note that reporting requirements for exports and reexports of encryption components can be adjusted or reduced, on a case-by-case basis, provided an exporter supplies BXA with sufficient information during the initial technical review of the U.S.

encryption component concerning its incorporation into a final foreign product. Examples include those components restricted by their design or use in certain types of products. BXA will notify exporters of such treatment in its classification determination. All required notifications, upgrade certifications and reports should be sent electronically or mailed to the addresses cited in this regulation.

Note to this paragraph: Post-export reporting is required for certain exports to foreign banks and financial institutions.

5. In part 740, Supplement No. 3 is removed. Supplement No. 3 previously listed countries eligible to receive certain encryption products; such products are now eligible for export and reexport to all destinations.

6. In § 742.15, the licensing policy section for exports and reexports of encryption items is changed as follows:

a. Review and classification are required by BXA before certain encryption items can be released from "EI" and "NS" controls under ECCNs 5A992, 5D992 and 5E992. These items include: 64-bit mass market encryption commodities and software; certain encryption items up to and including 64-bits; and asymmetric key exchange algorithms not exceeding 512 bits or an elliptic curve at 112 bits. Encryption items under these ECCNs do not require a license or license exception and may be exported and reexported as "NLR" (No License Required).

b. Upgrades: 40 and 56-bit DES or equivalent mass market commodities and software previously classified as eligible for License Exception ENC or TSU may be upgraded to 64-bits for the confidentiality algorithm. Exporters must, prior to export of an upgraded product, certify to BXA in a letter from a corporate official that the only change is the key length for confidentiality or key exchange algorithms and there is no other change in cryptographic functionality. Note that other mass market encryption commodities and software previously exported under License Exception ENC or TSU are now classified as either 5A992 or 5D992 and eligible for "NLR" treatment. Encryption items under 5A992, 5D992 and 5E992 are not subject to Internet download screening requirements listed in § 734.2(b)(9)(iii).

c. The licensing policies for exports and reexports of encryption items for banks and financial institutions, health and medical end-users, and on-line merchants, as well as U.S. subsidiaries, are subsumed into a new licensing policy paragraph for all encryption

items under ECCNs 5A002, 5D002 or 5E002 eligible for License Exception ENC. For U.S. subsidiaries, any encryption item (including technology classified under 5E002 to foreign employees located in the U.S.) is permitted for export or reexport under License Exception ENC without review and classification. Also, any encryption item, including components, under ECCNs 5A002 or 5D002 can be exported and reexported to non-government end-users in all destinations. Retail products under 5A002 or 5D002 can be exported and reexported to all end-users.

d. Licenses required for exports and reexports of encryption items to governments, or Internet and telecommunications service providers for the provision of services specific to governments, may be considered favorably for civil uses.

e. Under Encryption Licensing Arrangements (ELAs), distributors and resellers can export and reexport under ELAs as long as they comply with restrictions contained in the ELA.

7. In § 770.2, Commodity interpretations, a new interpretation for "Encryption commodity and software reviews" is added. This interpretation clarifies which encryption items require a review and what a review entails.

8. In part 772, Definition of terms, definitions for the following terms are added: Asymmetric Algorithm, Encryption Component, Government End-User, Open Cryptographic Interface and Symmetric Algorithm.

9. In part 774, the Commerce Control List, ECCNs 5A002 and 5D002 are revised to reflect changes in the Wassenaar Arrangement, and the Cryptography Note is added as Note 3 to Category 5—Part 2.

In addition to these changes, BXA is making the following clarifications and interpretations for all encryption items subject to the EAR.

1. The review and classification process is used to classify encryption items for their proper licensing mechanism and not to delay or deny a proposed transaction. Once a classification request is received, the item's specifications are reviewed and processed in accordance with § 748.3 of the EAR to determine its classification. Once completed, exporters will receive a document by mail informing them of the product's technical classification and proper licensing mechanism. The EAR also provides an appeal process for exporters unsatisfied with BXA's product classification (see § 756.2 of the EAR).

2. It is BXA's intent to allow end-users of encryption items to provide their customers with encryption

products and services. However, exports to Internet and telecommunications service providers are subject to restrictions when providing services specific to government end-users.

3. It was not the intent of the new Wassenaar language for ECCN 5A002 to be more restrictive concerning Message Authentication Codes (MAC). "Data authentication equipment that calculates a Message Authentication Code (MAC) or similar result to ensure no alteration of text has taken place, or to authenticate users, but does not allow for encryption of data, text or other media other than that needed for the authentication" continues to be excluded from control under 5A002. These commodities are controlled under ECCN 5A992.

4. Note that § 740.8, Key Management Infrastructure (KMI), authorizes the export and reexport of certain encryption software and commodities under License Exception KMI and will continue as an eligible licensing mechanism for encryption products.

5. A number of companies have expressed concern that the European Union (EU) may implement a general authorization permitting encryption items to be exported freely within the EU and other specified countries. If and when the EU implements such an authorization, the Administration will take the necessary steps to ensure U.S. exporters are not disadvantaged.

6. Note that Serbia and the Taliban controlled areas of Afghanistan are embargoed destinations.

7. Please refer to the BXA website at "www.bxa.doc.gov" for a detailed explanation of the EAR, the Commerce Control List, the licensing process and key terms used in this regulation. Although the Export Administration Act (EAA) expired on August 20, 1994, the President invoked the International Emergency Economic Powers Act and continued in effect the EAR, and, to the extent permitted by law, the provisions of the EAA in Executive Order 12924 of August 19, 1994, as extended by the President's notices of August 15, 1995 (60 FR 42767), August 14, 1996 (61 FR 42527), August 13, 1997 (62 FR 43629), August 13, 1998 (63 FR 44121), and August 10, 1999 (64 FR 44101).

Rulemaking Requirements

1. This interim final rule has been determined to be significant for purposes of E.O. 12866.

2. Notwithstanding any other provision of law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with a collection of information, subject to the requirements of the Paperwork

Reduction Act (PRA), unless that collection of information displays a currently valid OMB Control Number. This rule involves collections of information subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*). These collections have been approved by the Office of Management and Budget under control numbers 0694-0088, "Multi-Purpose Application" and 0694-0104, "Commercial Encryption Items Transferred from the Department of State to the Department of Commerce." The Department has submitted to OMB an emergency request for approval of the changes to the collection of information under OMB control number 0694-0104.

This interim final rule reduces the annual burden hours associated with collection 0694-0104 from 703 hours to 692 hours, and reduces collection 0694-0088 by 200 burden hours. For collection 0694-0104, it is estimated it will take companies 5 minutes to complete notifications for source code under License Exceptions TSU and ENC. It will take companies 15 minutes to complete upgrade notifications. For reporting under License Exception ENC and licenses for encryption items, it will take companies 4 hours to complete semi-annual reporting requirements.

Comments on collection 0694-0104 are welcome, and will be accepted until April 13, 2000. Comments are invited on: (a) Whether the collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; (b) the accuracy of the agency's estimate of the burden of the proposed collection of information; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden of the collection of information on respondents, including through the use of automated collection techniques or other forms of information technology. Comments regarding these burden estimates or any other aspect of the collection of information, including suggestions for reducing the burdens, should be forward to Frank J. Ruggiero, Regulatory Policy Division, Office of Exporter Services, Bureau of Export Administration, Department of Commerce, P.O. Box 273, Washington, D.C. 20044, and David Rostker, Office of Management and Budget, OMB/OIRA, 25 17th Street, NW, NEOB Rm. 10202, Washington, D.C. 20503.

3. This rule does not contain policies with Federalism implications sufficient to warrant preparation of a Federalism

assessment under Executive Order 13132.

4. The provisions of the Administrative Procedure Act (5 U.S.C. 553) requiring notice of proposed Rulemaking, the opportunity for public participation, and a delay in effective date, are inapplicable because this regulation involves a military and foreign affairs function of the United States (Sec. 5 U.S.C. 553(a)(1)). Further, no other law requires that a notice of proposed rulemaking and an opportunity for public comment be given for this interim final rule. Because a notice of proposed rulemaking and an opportunity for public comment are not required to be given for this rule under 5 U.S.C. or by any other law, the analytical requirements of the Regulatory Flexibility Act (5 U.S.C. 601 *et seq.*) are not applicable.

However, because of the importance of the issues raised by this regulation, it is issued in interim final form and comments will be considered in the development of final regulations. Accordingly, the Department of Commerce encourages interested persons who wish to comment to do so at the earliest possible time to permit the fullest consideration of their views.

The period for submission of comments will close May 15, 2000. The Department will consider all comments received before the close of the comment period in developing final regulations. Comments received after the end of the comment period will be considered if possible, but their consideration cannot be assured. The Department 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. The Department will return such comments and materials to the persons submitting the comments and will not consider them in the development of final regulations. All public comments on these regulations will be a matter of public record and will be available for public inspection and copying. In the interest of accuracy and completeness, the Department requires comments in written form. Comments should be provided with 5 copies.

Oral comments must be followed by written memoranda, which will also be a matter of public record and will be available for public review and copying.

The public record concerning these regulations will be maintained in the Bureau of Export Administration Freedom of Information Records Inspection Facility, Room 6881, Department of Commerce, 14th Street

and Pennsylvania Avenue, N.W., Washington, DC 20230. Records in this facility, including written public comments and memoranda summarizing the substance of oral communications, may be inspected and copied in accordance with regulations published in Part 4 of Title 15 of the Code of Federal Regulations. Information about the inspection and copying of records at the facility may be obtained from the Bureau of Export Administration Freedom of Information Officer, at the above address or by calling (202) 482-0500.

List of Subjects

15 CFR Part 734

Administrative practice and procedure, Exports, Foreign trade.

15 CFR Part 740

Administrative practice and procedure, Exports, Foreign trade, Reporting and record keeping requirements.

15 CFR Parts 742, 770, 772, and 774

Exports, Foreign Trade.

Accordingly, parts 734, 740, 742, 770, 772, and 774 of the Export Administration Regulations (15 CFR parts 730 through 799) are amended as follows:

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

Authority: 50 U.S.C. app. 2401 *et seq.*; 59 U.S.C. 1701 *et seq.*; E.O. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; 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; Notice of November 12, 1998, 63 FR 63589, 3 CFR, 1998 Comp., p. 305; Notice of August 10, 1999, 64 FR 44101 (August 13, 1999).

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

Authority: 50 U.S.C. app. 2401 *et seq.*; 59 U.S.C. 1701 *et seq.*; E.O. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; Notice of August 10, 1999, 64 FR 44101 (August 13, 1999).

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

Authority: 50 U.S.C. app. 2401 *et seq.*; 59 U.S.C. 1701 *et seq.*; 18 U.S.C. 2510 *et seq.*; 22 U.S.C. 3201 *et seq.*; 42 U.S.C. 2139a; 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. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; E.O. 12938, 59 FR 59099, 3 CFR, 1994 Comp., p. 950; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; Notice of November 12, 1998, 63 FR 63589, 3 CFR, 1998 Comp., p. 305; Notice of August 10, 1999, 64 FR 44101 (August 13, 1999).

4. The authority citation for part 770 continues to read as follows:

Authority: 50 U.S.C. app. 2401 *et seq.*; 50 U.S.C. 1701 *et seq.*; E.O. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; Notice of August 10, 1999, 64 FR 44101 (August 13, 1999).

5. 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. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; Notice of August 10, 1999, 64 FR 44101 (August 13, 1999).

6. 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); 18 U.S.C. 2510 *et seq.*; 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; 46 U.S.C. app. 466c; 50 U.S.C. app. 5; E.O. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; Notice of August 10, 1999, 64 FR 44101 (August 13, 1999).

PART 734—[AMENDED]

7. Section 734.2 is amended by revising paragraph (b)(9)(ii) and adding new paragraph (b)(9)(iii) to read as follows:

§ 734.2 Important EAR terms and principles.

* * * * *

- (b) * * *
(9) * * *
(i) * * *

(ii) The export of encryption source code and object code software controlled for "EI" reasons under ECCN 5D002 on the Commerce Control List (see Supplement No. 1 to part 774 of the EAR), except for source code eligible for export under §§ 740.13(e) and 740.17(a)(5)(i), includes downloading, or causing the downloading of, such software to locations (including electronic bulletin boards, Internet file transfer protocol, and World Wide Web sites) outside the U.S., or making such software available for transfer outside the United States, over wire, cable, radio, electromagnetic, photo optical, photoelectric or other comparable communications facilities accessible to persons outside the United States, including transfers from electronic bulletin boards, Internet file transfer protocol and World Wide Web sites, unless the person making the software available takes precautions adequate to prevent unauthorized transfer of such code.

(iii) Subject to the General Prohibitions described in part 736 of the EAR, such precautions for Internet transfers of products eligible for export under §§ 740.17(a)(2) (encryption software products), (a)(5)(ii) (certain encryption source code) and (a)(5)(iii) (encryption toolkits) shall include such measures as:

(A) The access control system, either through automated means or human intervention, checks the address of every system outside of the U.S. or Canada requesting or receiving a transfer and verifies such systems do not have a domain name or Internet address of a foreign government end-user (e.g., ".gov," ".gouv," ".mil" or similar addresses);

(B) The access control system provides every requesting or receiving party with notice that the transfer includes or would include cryptographic software subject to export controls under the Export Administration Regulations, and anyone receiving such a transfer cannot export the software without a license or other authorization; and

(C) Every party requesting or receiving a transfer of such software must acknowledge affirmatively that the software is not intended for use by a government end-user, as defined in part 772, and he or she understands the cryptographic software is subject to export controls under the Export Administration Regulations and anyone receiving the transfer cannot export the software without a license or other authorization. BXA will consider acknowledgments in electronic form provided they are adequate to assure legal undertakings similar to written acknowledgments.

§ 734.4 [Amended]

8. Section 734.4 is amended by revising the last sentence of paragraph (b) to read as follows: "Certain encryption commodities, software and technology controlled under ECCNs 5A992, 5D992, and 5E992 may be eligible for *de minimis* (refer to § 742.15(b)(1))."

9. Section 734.7 is amended by revising paragraph (c) to read as follows:

§ 734.7 Published information and software.

* * * * *

(c) Notwithstanding paragraphs (a) and (b) of this section, note that encryption software controlled under ECCN 5D002 for "EI" reasons on the Commerce Control List (refer to Supplement No. 1 to part 774 of the EAR) remains subject to the EAR (refer to §§ 740.13(e) and 740.17(a)(5)(i) of the

EAR for release under license exception).

§ 734.8 [Amended]

10. Section 734.8 is amended by revising the last sentence of paragraph (a) to read as follows: "Note that the provisions of this section do not apply to encryption software controlled under ECCN 5D002 for "EI" reasons on the Commerce Control List (refer to §§ 740.13(e) and 740.17(a)(5)(i) of the EAR for release under license exception)."

§ 734.9 [Amended]

11. Section 734.9 is amended by revising the last sentence to read as follows: "Note that the provisions of this section do not apply to encryption software controlled under ECCN 5D002 for "EI" reasons on the Commerce Control List (refer to §§ 740.13(e) and 740.17(a)(5)(i) of the EAR for release under license exception)."

PART 740—[AMENDED]

12. Section 740.8 is amended by revising the address in paragraph (b)(2) to read as follows:

§ 740.8 Key management infrastructure (KMI).

* * * * *

- (b) * * *
(2) * * *

Attn: KMI Encryption Request Coordinator, 9800 Savage Road, Suite 6131, Fort Meade, MD 20755-6000.

* * * * *

13. Section 740.13 is amended by:
a. By revising the introductory paragraph;
b. By revising paragraph (d)(2); and
c. By adding new paragraph (e) to read as follows:

§ 740.13 Technology and software—unrestricted (TSU)

This license exception authorizes exports and reexports of operation technology and software; sales technology and software; software updates (bug fixes); "mass market" software subject to the General Software Note; and unrestricted encryption source code. Note that encryption software is not subject to the General Software Note (see paragraph (d)(2) of this section).

* * * * *

- (d) * * *

(2) *Software not eligible for this license exception.* This license exception is not available for certain encryption software controlled under ECCN 5D002. (Refer to the Cryptography Note in Category 5—Part 2 of the Commerce Control List for information

on Mass Market Encryption commodities and software. Also refer to §§ 742.15(b)(1) and 748.3(b) of the EAR for information on item classifications or release from "EI" controls and "NS" controls).

* * * * *

(e) *Unrestricted encryption source code.*

(1) Encryption source code controlled under 5D002, which would be considered publicly available under § 734.3(b)(3) and which is not subject to an express agreement for the payment of a licensing fee or royalty for commercial production or sale of any product developed with the source code, is released from "EI" controls and may be exported or reexported without review under License Exception TSU, provided you have submitted written notification to BXA of the Internet location (e.g., URL or Internet address) or a copy of the source code by the time of export. Submit the notification to BXA and send a copy to ENC Encryption Request Coordinator (see § 740.17(g)(5) for mailing addresses). Intellectual property protection (e.g., copyright, patent or trademark) will not, by itself, be construed as an express agreement for the payment of a licensing fee or royalty for commercial production or sale of any product developed using the source code.

(2) You may not knowingly export or reexport source code or products developed with this source code to Cuba, Iran, Iraq, Libya, North Korea, Sudan or Syria.

(3) Posting of the source code on the Internet (e.g., FTP or World Wide Web site) where the source code may be downloaded by anyone would not establish "knowledge" of a prohibited export or reexport, including that described in paragraph (e)(2) of this section. In addition, such posting would not trigger "red flags" necessitating the affirmative duty to inquire under the "Know Your Customer" guidance provided in Supplement No. 3 to part 732 of the EAR.

14. Section 740.17 is revised to read as follows:

§ 740.17 Encryption commodities and software (ENC).

(a) *Exports and reexports of certain encryption commodities and software.* As enumerated in this section, you may export and reexport encryption commodities, software and components (as defined in part 772 EAR) under License Exception ENC. License Exception ENC cannot be used if the encryption commodity or software provides an open cryptographic interface (as defined in part 772), unless

the export is to a subsidiary of a U.S. company, as described in paragraph (a)(1) of this section.

(1) *Encryption commodities, software, and technology for U.S. subsidiaries.* You may export and reexport any encryption item of any key length under ECCNs 5A002, 5D002 and 5E002 to foreign subsidiaries of U.S. companies (as defined in part 772) without review and classification. This includes source code and technology for internal company use, such as the development of new products. U.S. firms may also transfer under License Exception ENC encryption technology (5E002) to their foreign employees in the U.S. (except nationals of Cuba, Iran, Iraq, Libya, North Korea, Sudan or Syria) for internal company use, including the development of new products. All items produced or developed by U.S. subsidiaries with encryption commodities, software and technology exported under this paragraph are subject to the EAR and require review and classification before any sale or retransfer outside of the U.S. company.

(2) *Encryption commodities and software.* You may export and reexport any encryption commodity, software and component after review and classification by BXA under ECCNs 5A002 and 5D002 to any individual, commercial firm or other non-government end-user. Encryption products classified under this paragraph require a license for export and reexport to government end-users (as defined in part 772). The former restriction limiting exports or reexports to internal company proprietary use is removed.

(3) *Retail encryption commodities and software.* You may export and reexport to any end-user encryption commodities, software and components which have been reviewed and classified as retail under ECCNs 5A002 and 5D002. Retail encryption commodities, software and components are products:

(i) Generally available to the public by means of any of the following:

(A) Sold in tangible form through retail outlets independent of the manufacturer;

(B) Specifically designed for individual consumer use and sold or transferred through tangible or intangible means; or

(C) Sold in large volume without restriction through mail order transactions, electronic transactions, or telephone call transactions; and

(ii) Meeting all of the following:

(A) The cryptographic functionality cannot be easily changed by the user;

(B) Do not require substantial support for installation and use;

(C) The cryptographic functionality has not been modified or customized to customer specification; and

(D) Are not network infrastructure products such as high end routers or switches designed for large volume communications.

(iii) Subject to the criteria in paragraphs (a)(3)(i) and (ii) of this section, retail encryption products include (but are not limited to) general purpose operating systems and their associated user-interface client software or general purpose operating systems with embedded networking and server capabilities; non-programmable encryption chips and chips that are constrained by design for retail products; low-end routers, firewalls and networking or cable equipment designed for small office or home use; programmable database management systems and associated application servers; low-end servers and application-specific servers (including client-server applications, e.g., Secure Socket Layer (SSL)-based applications) that interface directly with the user; and encryption products distributed without charge or through free or anonymous downloads.

(iv) Encryption products and network-based applications which provide functionality equivalent to other encryption products classified as retail will be considered retail.

(v) Encryption products exported or reexported under paragraph (a)(3) of this section can be used to provide services to any entity.

(vi) Finance-specific encryption commodities and software of any key length restricted by design (e.g., highly field-formatted with validation procedures and not easily diverted to other end-uses) and used to secure financial communications such as electronic commerce will be considered retail encryption products.

(vii) 56-bit products with key exchange mechanisms greater than 512 bits and up to and including 1024 bits, or equivalent products not classified as mass market, will be considered retail.

(4) *Internet and Telecommunications service providers.* Certain restrictions apply to Internet and telecommunications service providers. Any Internet or telecommunications service provider can obtain retail products under License Exception ENC and use them to provide any service to any entity. Internet and telecommunications service providers can obtain and use any encryption product for their internal use and to provide any service under License Exception ENC. However, a license is required for the use of any product not

classified as retail to provide services specific to government end-users, e.g., WAN, LAN, VPN, voice and dedicated-link services; application specific and e-commerce services and PKI encryption services specifically for government end-users only.

(5) *Commercial encryption source code and general purpose toolkits.* You may export and reexport encryption source code not released under § 740.13(e) or general purpose toolkits (application specific toolkits are covered under components, as defined in part 772), subject to the following provisions:

(i) Encryption source code, which would be considered publicly available under § 734.3(b)(3) of the EAR and which is subject to an express agreement for the payment of a licensing fee or royalty for commercial production or sale of any product developed using the source code, can be exported or reexported using License Exception ENC to any end-user without review and classification, provided you have submitted to BXA, by the time of export, written notification of the Internet location (e.g. URL or Internet address) or a copy of the source code. You may not knowingly export or reexport source code or products developed with this source code to Cuba, Iran, Iraq, Libya, North Korea, Sudan or Syria. Posting of the source code on the Internet (e.g., FTP or World Wide Web site) where the source code may be downloaded by anyone would not establish "knowledge" of a prohibited export or reexport. In addition, such posting would not trigger "red flags" necessitating the affirmative duty to inquire under the "Know Your Customer" guidance provided in Supplement No. 3 to part 732 of the EAR.

(ii) Encryption source code which would neither be considered publicly available nor includes source code that when compiled provides an open cryptographic interface (see § 740.17(f)), may be exported or reexported using License Exception ENC to any non-government end-user after review and classification by BXA.

(iii) General purpose encryption toolkits may be exported or reexported after review and classification by BXA under License Exception ENC to any non-government end-user.

(iv) Any foreign product developed for commercial sale using encryption source code or general purpose toolkits exported under paragraph (a)(5) of this section is subject to reporting requirements under paragraph (g)(3) of this section. Foreign products developed by bundling or compiling of

source code are not subject to this reporting requirement.

(b) *Ineligible destinations.* No encryption item(s) may be exported or reexported under this license exception to Cuba, Iran, Iraq, Libya, North Korea, Sudan or Syria.

(c) *Transfers.* Transfers of encryption items listed in paragraph (a) of this section to government end-users or end-users within the same country are prohibited unless otherwise authorized by license or license exception.

(d) *Exports and reexports of foreign products incorporating U.S. encryption source code, components or general purpose encryption toolkits.* Foreign products developed with or incorporating U.S.-origin encryption source code, components or toolkits remain subject to the EAR, but do not require review and classification by BXA and can be exported or reexported without further authorization.

(e) *Eligibility for License Exception ENC.* (1) *Review and classification.* You may initiate review and classification of your encryption commodities and software as required by paragraph (a) of this section by submitting a classification request in accordance with the provisions of § 748.3(b) and Supplement 6 to part 742 of the EAR. Indicate "License Exception ENC" in Block 9: Special purpose, on form BXA-748P. Submit the original request to BXA in accordance with § 748.3 of the EAR and send a copy of the request to ENC Encryption Request Coordinator (see paragraph (g)(5) of this section for mailing addresses). Thirty days after receipt of a complete classification request by BXA, unless otherwise notified by BXA, exporters may export and reexport to any non-government end-user any encryption product eligible under paragraphs (a)(2), (a)(4) and (a)(5) of this section. No exports to government end-users are allowed under this provision, and BXA reserves the right to suspend eligibility to export while a classification is pending.

(2) *Grandfathering.* Finance-specific and 56-bit products previously reviewed and classified by BXA can be exported or reexported to any end-user without further review. Other encryption commodities, software or components previously approved for export can be exported and reexported without further review to any non-government end-user under the provisions of § 740.17 (a). This includes products approved under a license, an Encryption Licensing Arrangement, or previously classified as eligible to use License Exception ENC (except for those products which were only authorized for export to U.S. subsidiaries). Exports to government

end-users require a license unless BXA has classified the product as a "retail" product under paragraph (a)(3) of this section.

(3) *Key Length Increases.* Exporters can increase the key lengths of previously classified products and continue to export without another review. No other change in the cryptographic functionality is allowed.

(i) Any product previously classified as 5A002 or 5D002 can, with any upgrade to the key length used for confidentiality or key exchange algorithms, be exported or reexported under provisions of License Exception ENC to any non-government end-user without an additional review. Another classification is necessary to determine eligibility as a "retail" product under paragraph (a)(3) of this section.

(ii) Exporters must certify to BXA in a letter from a corporate official that the only change to the encryption product is the key length for confidentiality or key exchange algorithms and there is no other change in cryptographic functionality. Certifications must include the original authorization number issued by BXA and the date of issuance. BXA must receive this certification prior to any export of an upgraded product. The certification should be sent to BXA, with a copy sent to the ENC Encryption Request Coordinator (see paragraph (g)(5) of this section for mailing addresses).

(f) *Open cryptographic interfaces.* License Exception ENC shall not apply to exports or reexports of encryption commodities, software and components (unless exported to a subsidiary of a U.S. company under paragraph (a)(1) of this section), if the encryption product provides an open cryptographic interface (as defined in part 772). This does not apply to source code that would be considered publicly available under § 734.3(b)(3).

(g) *Reporting requirements.* (1) No reporting is required for exports of:

(i) Any encryption to U.S. subsidiaries;

(ii) Finance-specific products;

(iii) Encryption commodities or software with a symmetric key length not exceeding 64 bits or otherwise classified as qualifying for mass market treatment;

(iv) Retail products exported to individual consumers;

(v) Any export made via free or anonymous download; and

(vi) Any export made from or to a U.S. bank, financial institution or their subsidiaries, affiliates, customers or contractors for banking or financial operations.

(2) Exporters must provide all available information as follows:

(i) For items exported to a distributor or other reseller, the name and address of the distributor or reseller and the quantity exported and, if collected in the normal course of business, the end-user's name and address;

(ii) For items exported through direct sale, the name and address of the recipient and the quantity exported (except for retail products if the end-user is an individual consumer); and

(3) For direct sales or transfers of encryption components, commercial source code described under § 740.17(a)(5) or general purpose encryption toolkits to foreign manufacturers, you must submit the names and addresses of the manufacturers using such encryption components, commercial source code or general purpose encryption toolkits and a non-proprietary technical description of the products for which the component, source code or toolkit 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).

(4) Exporters of encryption commodities, software and components which were previously classified under License Exception ENC, or which have been licensed for export under an Encryption Licensing Arrangement, must comply with the reporting requirements of this section.

(5) Beginning January 14, 2000, you must submit reports required under this section semi-annually to BXA, unless otherwise provided in this paragraph. For exports occurring between January 1 and June 30, a report is due no later than August 1. For exports occurring between July 1 and December 31, a report is due no later than February 1. For exports and reexports to Internet and telecommunications service providers of network infrastructure products (e.g., high-end routers or switches designed for large volume communications), reports are due by the time of export. Reports must include the classification or other authorization number. These reports must be provided in electronic form to BXA; suggested file formats for electronic submission include spreadsheets, tabular text or structured text. Exporters may request other reporting arrangements with BXA to better reflect their business models. Reports should be sent electronically to crypt@bxa.doc.gov, or disks and CDs

can be mailed to the following addresses:

(i) Department of Commerce, Bureau of Export Administration, Office of Strategic Trade and Foreign Policy Controls, 14th Street and Pennsylvania Ave., N.W., Room 2705, Washington, DC 20230, Attn: Encryption Reports.

(ii) A copy of the report should be sent to: Attn: ENC Encryption Request Coordinator, 9800 Savage Road, Suite 6131, Ft. Meade, MD 20755-6000.

(h) *Distributors and resellers.* 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 § 740.17.

PART 742—[AMENDED]

15. Section 742.15 is revised to read as follows:

§ 742.15 Encryption items.

Encryption items can be used to maintain the secrecy of information, and thereby may be used by persons abroad to harm national security, foreign policy and law enforcement interests. The U.S. has a critical interest in ensuring that important and sensitive information of the public and private sector is protected. Consistent with our international obligations as a member of the Wassenaar Arrangement, the U.S. has a responsibility to maintain control over the export of encryption items. As the President indicated in Executive Order 13026 and in his Memorandum of November 15, 1996, export of encryption software, like export of encryption hardware, is controlled because of this functional capacity to encrypt information on a computer system, and not because of any informational or theoretical value that such software may reflect, contain, or represent, or that its export may convey to others abroad. For this reason, export controls on encryption software are distinguished from controls on other software regulated under the EAR.

(a) *License requirements.* Licenses are required for exports and reexports to all destinations, except Canada, for items controlled under ECCNs having an "EI" (for "encryption items") under the "Control(s)" paragraph. Such items include: encryption commodities controlled under ECCN 5A002; encryption software controlled under ECCN 5D002; and encryption technology controlled under ECCN 5E002. Refer to part 772 of the EAR for the definition of "encryption items".

(b) *Licensing policy.* The following licensing policies apply to items identified in paragraph (a) of this section. Except as otherwise noted, applications will be reviewed on a case-by-case basis by BXA, in conjunction with other agencies, to determine whether the export or reexport is consistent with U.S. national security and foreign policy interests. For subsequent bundling and updates of these items see paragraph (n) of § 770.2 of the EAR.

(1) *Encryption commodities, software and technology under ECCNs 5A992, 5D992 and 5E992.* Certain encryption commodities, software and technology may, after classification by BXA as ECCNs 5A992, 5D992 or 5E992, be released from "EI" or "NS" controls. Items controlled under these ECCNs are eligible for export and reexport to all destinations except Cuba, Iran, Iraq, Libya, North Korea, Sudan or Syria. Refer to § 748.3(b)(3) of the EAR for additional information regarding classification requests. The following encryption items may be eligible for such treatment:

(i) *56-bit encryption commodities, software and technology.* Encryption commodities, software and technology up to and including 56-bits with an asymmetric key exchange algorithm not exceeding 512 bits may be classified under ECCNs 5A992, 5D992 or 5E992.

(ii) *Key management products.* Products which only provide key management with asymmetric key exchange algorithms not exceeding 512 bits may be eligible for classification under ECCNs 5A992 or 5D992.

(iii) *64-bit mass market encryption commodities and software.* (A) Mass market encryption commodities and software with key lengths not exceeding 64-bit for the symmetric algorithm may be eligible for classification by BXA under ECCNs 5A992 or 5D992.

Refer to the Cryptography Note (Note 3) to part 2 of Category 5 of the CCL for a definition of mass market encryption commodities and software. Key exchange mechanisms, proprietary key exchange mechanisms, or company proprietary commodities and software implementations may also be eligible for this treatment. Refer to Supplement No. 6 to part 742 and § 748.3(b)(3) of the EAR for additional information.

(B) Mass market encryption commodities and software (e.g., 40 and 56-bit DES or equivalent) previously eligible for License Exception TSU (or for hardware, ENC) may increase key lengths for the confidentiality algorithm up to 64 bits and still be exported as a mass market product without an additional review. Exporters must

certify to BXA in a letter from a corporate official the only change to the encryption product is the key length for confidentiality or key exchange algorithms and there is no other change in cryptographic functionality.

Certifications must include the original authorization number issued by BXA and the date of issuance. BXA must receive this certification prior to any export of upgraded products. The certification should be sent to BXA, with a copy to ENC Encryption Request Coordinator at the following addresses:

(1) Department of Commerce, Bureau of Export Administration, Office of Strategic Trade and Foreign Policy Controls, 14th Street and Pennsylvania Ave., N.W., Room 2705, Washington, DC 20230.

(2) A copy of the report should be sent to: Attn: ENC Encryption Request Coordinator, 9800 Savage Road, Suite 6131, Ft. Meade, MD 20755-6000.

(iv) For classification of these encryption items under these ECCNs, mark "NLR" in Block 9: Special purpose, on Form BXA-748P, of your classification request.

(2) *Encryption commodities and software eligible for classification under ECCNs 5A002, 5D002 and 5E002 and qualified for License Exception ENC.* Items classified by BXA as retail products under ECCNs 5A002 and 5D002 are permitted for export and reexport to any end-user. All other encryption commodities, software and components classified by BXA under ECCNs 5A002 and 5D002 may be exported to any individual, commercial firm or other non-government end-user. Any encryption item (including technology classified under 5E002) will be permitted for export or reexport to U.S. subsidiaries (as defined in part 772). Products developed using U.S. encryption items are subject to the EAR. No exports are authorized to Cuba, Iran, Iraq, Libya, North Korea, Sudan or Syria.

(3) *Encryption licensing.* Exporters may submit applications for licenses or Encryption Licensing Arrangements for exports and reexports of encryption items not eligible for license exception, including exports and reexports of encryption technology to strategic partners of U.S. companies (as defined in part 772). For Encryption Licensing Arrangements, the applicant must specify the sales territory and class of end-user. Encryption Licensing Arrangements granted for exports of unlimited quantities for all destinations except Cuba, Iran, Iraq, Libya, North Korea, Sudan or Syria, are valid for four years, and may require reporting.

Licenses are required for exports of encryption items to governments, or Internet and telecommunications service providers for the provision of services specific to governments, and may be favorably considered for civil uses, e.g., social or financial services to the public; civil justice; social insurance, pensions and retirement; taxes and communications between governments and their citizens.

16. Supplement No. 6 to Part 742 is revised to read as follows:

**Supplement No. 6 to Part 742—
Guidelines for Submitting a
Classification Request for Encryption
Items**

Classification requests for encryption items must be submitted on Form BXA-748P, in accordance with § 748.3 of the EAR. Insert in Block 9: Special Purpose of the Form BXA-748P, the phrase "License Exception ENC" or "NLR", based on your classification request. Failure to insert this phrase will delay processing. In addition, the Bureau of Export Administration recommends that such requests be delivered via courier service to: Bureau of Export Administration, Office of Exporter Services, Room 2705, 14th Street and Pennsylvania Ave., NW, Washington, DC 20230. In addition, you must send a copy of the request and all supporting documents to: Attn: ENC Encryption Request Coordinator, 9800 Savage Road, Suite 6131, Fort Meade, MD 20755-6000.

(a) Requests for encryption items will be processed in thirty (30) days from receipt of a properly completed request.

(b) To submit a classification request for a technical review of commodities and software, ensure that the information provided includes brochures or other documentation or specifications (to include applicable cryptographic source code) related to the technology, commodity or software, as well as any additional information which you believe would assist the review process. You must provide the following information in a cover letter to the classification request:

(1) Clearly state at the top of the page either "ENC" or "NLR"—"30 Day Technical Review Requested;"

(2) State that you have reviewed and determined that the commodity or software subject to the classification request meets the criteria of this Supplement;

(3) State the name of the commodity or software product being submitted for review;

(4) State how the commodity or software has been written to preclude user modification of the encryption

algorithm, key management mechanism, and key space;

(5) State that a duplicate copy has been sent to the ENC Encryption Request Coordinator;

(6) Provide the following information for the commodity or software product:

(i) Description of all encryption algorithms and key lengths, e.g. source code, and how the algorithms are used. If any combination of different algorithms are used in the same product, also state how each is applied to the data.

(ii) Pre-processing information of plaintext data before encryption (e.g. compression of the data).

(iii) Post-processing information of cipher text data after encryption (e.g. packetization of the encrypted data).

(iv) For classification requests regarding object code or Java byte code, describe what techniques (including obfuscation, private access modifiers, final classes) are used to protect against decompilation and misuse.

(v) For classification requests regarding components:

(A) Reference the application for the components if known;

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

(C) State whether the component is constrained by function;

(D) List any standards and protocols that the component adheres to;

(E) Include a complete description of all functionalities and their accessibility; and

(F) Encryption components need to be clearly identified to include the name of the manufacturer, component model number, or other identifier.

(vi) For classification requests regarding source code:

(A) If applicable, reference the executable product that has already received a technical review;

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

(C) Include a copy of the sections of the source code that contain the encryption algorithm, key management routines, and their related calls.

PART 770—[AMENDED]

17. Section 770.2 is amended by adding new paragraph (n) to read as follows:

§ 770.2 Item interpretations.

* * * * *

(n) *Interpretation 14: Encryption commodity and software reviews.* Classification of encryption

to the public; or (3) one-time encryption of copyright protected audio/video data; (e) cryptographic equipment specially designed and limited for banking use or money transactions; (f) cordless telephone equipment not capable of end-to-end encryption where the maximum effective range of unboosted cordless operation (e.g., a single, unrelayed hop between terminal and home basestation) is less than 400 meters according to the manufacturer's specifications.

Related Definitions: (1) The term *money transactions* in paragraph (e) of Related Controls includes the collection and settlement of fares or credit functions.

(2) For the control of global navigation satellite systems receiving equipment containing or employing decryption (e.g., GPS or GLONASS) see 7A005.

Items

Technical Note: Parity bits are not included in the key length.

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

a.1. Designed or modified to use "cryptography" employing digital techniques performing any cryptographic function other than authentication or digital signature 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 analogue 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 5A002a.1.b.2 in excess of 112 bits (e.g., Diffie-Hellman over an elliptic curve);

a.2. Designed or modified to perform crypto analytic functions;

a.3. [Reserved]

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

a.5. Designed or modified to use cryptographic techniques to generate the spreading code for "spread spectrum" or the hopping code for "frequency agility" systems;

a.6. Designed or modified to provide certified or certifiable "multilevel security" or user isolation at a level exceeding Class B2 of the Trusted Computer System Evaluation Criteria (TCSEC) or equivalent;

a.7. Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion.

* * * * *

5D002 Information Security—"Software".

License Requirements

Reason for Control: NS, AT, EI.

Control(s)	Country chart
NS applies to entire entry	NS Column 1
AT applies to entire entry	AT Column 1

EI applies to encryption items transferred from the U.S. Munitions List

to the Commerce Control List consistent with E.O. 13026 of November 15, 1996 (61 FR 58767) and pursuant to the Presidential Memorandum of that date. Refer to § 742.15 of the EAR.

Note: Encryption software is controlled because of its functional capacity, and not because of any informational value of such software; such software is not accorded the same treatment under the EAR as other "software"; and for export licensing purposes, encryption software is treated under the EAR in the same manner as a commodity included in ECCN 5A002.

Note: Encryption software controlled for "EI" reasons under this entry remains subject to the EAR even when made publicly available in accordance with part 734 of the EAR. See §§ 740.13(e) and 740.17(5)(i) of the EAR for information on releasing certain source code which may be considered publicly available from "EI" controls.

Note: After a technical review, 56-bit items, key management products not exceeding 512 bits and mass market encryption commodities and software eligible for the Cryptography Note (see § 742.15(b)(1) of the EAR) may be released from "EI" and "NS" controls.

License Exceptions: * * *

* * * * *

20. Supplement No. 2 to part 774 (General Technology and Software Notes) is amended by revising the Note at the end of the Supplement to read as follows:

Supplement No. 2 to Part 774—General Technology and Software Notes

* * * * *

Note: The General Software Note does not apply to "software" controlled by Category 5, Part 2 ("Information Security"). For "software" controlled by Category 5, Part 2, see Supplement No. 1 to Part 774, Category 5, Part 2, Note 3—Cryptography Note.

Dated: January 11, 2000.

R. Roger Majak,
Assistant Secretary for Export Administration.

[FR Doc. 00-983 Filed 1-12-00; 9:04 am]

BILLING CODE 3510-33-P

commodities or software is required to determine eligibility for all licensing mechanisms except source code (see §§ 740.13(e) and 740.17(a)(5)(i) of the EAR) and exports to subsidiaries of U.S. firms (see § 740.17(a)(1)). Note that subsequent bundling, patches, upgrades or releases, including name changes, may be exported or reexported under the applicable provisions of the EAR without further technical review as long as the functional encryption capacity of the originally reviewed encryption product has not been modified or enhanced. This does not extend to products controlled under a different category on the CCL.

18. Part 772 is amended by removing the definitions for "Health/medical end-user" and "On-line merchant" and adding definitions for "asymmetric algorithm", "encryption component", "government end-user", "open cryptographic interface", and "symmetric algorithm" in alphabetical order, to read as follows:

PART 772—DEFINITIONS OF TERMS

* * * * *

"Asymmetric algorithm". (Cat 5, Part II) A cryptographic algorithm using different, mathematically-related keys for encryption and decryption. A common use of "asymmetric algorithms" is key management.

* * * * *

"Encryption component". Any encryption commodity or software (except source code), including encryption chips, integrated circuits, application specific encryption toolkits, or executable or linkable modules that alone are incapable of performing complete cryptographic functions, and is designed or intended for use in or the production of another encryption item.

* * * * *

Government end-user (as applied to encryption items). A government end-user is any foreign central, regional or local government department, agency, or other entity performing governmental functions; including governmental research institutions, governmental corporations or their separate business units (as defined in part 772 of the EAR) which are engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List, and international governmental organizations. This term does not include: utilities (including telecommunications companies and internet service providers); banks and financial institutions; transportation; broadcast or entertainment; educational organizations; civil health and medical organizations; retail or wholesale firms;

and manufacturing or industrial entities not engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List.

* * * * *

"Open cryptographic interface". A mechanism which is designed to allow a customer or other party to insert cryptographic functionality without the intervention, help or assistance of the manufacturer or its agents, e.g., manufacturer's signing of cryptographic code or proprietary interfaces. If the cryptographic interface implements a fixed set of cryptographic algorithms, key lengths or key exchange management systems, that cannot be changed, it will not be considered an "open" cryptographic interface. All general application programming interfaces (e.g., those that accept either a cryptographic or non-cryptographic interface but do not themselves maintain any cryptographic functionality) will not be considered "open" cryptographic interfaces.

* * * * *

"Symmetric algorithm". (Cat 5, Part II) A cryptographic algorithm using an identical key for both encryption and decryption. A common use of "symmetric algorithms" is confidentiality of data.

PART 774—[AMENDED]

Supplement No. 1 to Part 774 [Amended]

19. Supplement No. 1 to Part 774, Category 5—Telecommunications and Information Security, is amended:

a. By revising, immediately following EAR 99, the heading for "Part 2—'Information Security,'" removing the Note, and inserting in its place three new Notes;

b. By revising the heading and the "List of Items Controlled" for ECCN 5A002; and

c. By revising the Licensing Requirements section of ECCN 5D002 to read as follows:

Category 15—Telecommunications and "Information Security"

* * * * *

II. "Information Security"

Note 1: The control status of "information security" equipment, "software", systems, application specific "electronic assemblies", modules, integrated circuits, components, or functions is determined in Category 5, Part 2 even if they are components or "electronic assemblies" of other equipment.

Note 2: Category 5, Part 2 encryption products, when accompanying their user for

the user's personal use, are eligible for License Exceptions TMP or BAG.

Note 3: Cryptography Note: ECCNs 5A002 and 5D002 do not control 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 be easily changed by the user;
- c. Designed for installation by the user without further substantial support by the supplier;
- d. Does not contain a "symmetric algorithm" employing a key length exceeding 64-bits; and
- 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) through (d) of this note. See § 742.15(b)(1) of the EAR.

* * * * *

5A002 Systems, equipment, application specific "electronic assemblies", modules and integrated circuits for "information security", and other specially designed components therefor.

List of Items Controlled

Unit: \$ value.

Related Controls: See also 5A992.

This entry does not control: (a) "Personalized smart cards" where the cryptographic capability is restricted for use in equipment or systems excluded from control paragraphs (b) through (f) of this note. Note that if a "personalized smart card" has multiple functions, the control status of each function is assessed individually; (b) receiving equipment for radio broadcast, pay television or similar restricted audience television of the consumer type, without digital encryption except that exclusively used for sending the billing or program-related information back to the broadcast providers; (c) portable or mobile radiotelephones for civil use (e.g., for use with commercial civil cellular radio communications systems) that are not capable of end-to-end encryption; (d) equipment where the cryptographic capability is not user-accessible and which is specially designed and limited to allow any of the following: (1) Execution of copy-protected "software"; (2) access to any of the following: (a) Copy-protected read-only media; or (b) information stored in encrypted form on media (e.g., in connection with the protection of intellectual property rights) where the media is offered for sale in identical sets

ENC 1
1 of 5

Ms. Kirsten Mortimer
Regulatory Policy Division
U.S. Department of Commerce
Bureau of Export Administration
P.O. Box 273
Washington, D.C. 20044

Subject: Comments to Revision to Encryption Items Regulation

Dated January 14, 2000

April 20, 2000

Dear Kirsten,

We would like to commend the BXA and other agencies for real breakthrough in the policy and regulatory areas of exports of encryption items. We understand the difficult decisions that had to be made, the efforts that went into this regulation and we are, overall very pleased with the results. For many of our products the regulation will enable us to compete with non-US companies and market our products within the established IBM business model. However, we would like to draw your attention to the fact that there are still 12 distinct product groups and that each has separate rules for which we have to have processes in place. We would suggest that the main effort in the follow up regulation goes into simplification of the rules and further streamlining of reporting. We are also requesting review of the requirement that non-retail products require individual license when sold to the Governments and restrictions on export of items with open cryptographic interface, i.e. we are requesting that all encryption products be eligible to be sold to all customers, in all countries, except embargoed, after a one time technical review. There is a sufficient foreign availability of cryptographic products as adequate alternatives to US solutions which largely negates the desired effect of the current policy.

We would like also to point out that the estimated times in the Rulemaking Requirements section are very underestimated for large multi-national companies. For example, while it may take only 5 minutes to complete the notification of a source code being made available on the Internet for export under License Exception TSU, it will take initially 1-2 hours of education, explanation and final determination as well as yearly one hour education refresher course for the developers. The estimate that it will take companies 4 hours to complete semi-annual reporting requirement are also not realistic for an overall effort of a large multi-national company. We estimate that it will take us over 1000 hours every 6 months to outline the requirements, educate the necessary personnel, set up systems where possible and consolidate the information for the submission to the BXA.

Specifically, our main concerns of the published regulation are as follows:

1. Reporting:

a. 740.17 (g)(1) (iv) Reporting of retail products when not exported to individual customers

To make a distinction between sales to individual customers and sales to dealers, distributors, etc. is difficult and time consuming. By their nature, these products are not controllable, can be transferred, and tracking of middle distributors does not appear to serve any purpose. In addition, pre-loaded software on PCs, workstations and servers sold as retail items changes frequently and tracking of new images is an administrative burden with significant cost. We are requesting that all reporting of retail products be eliminated.

b. 740.17(g)(3) Requirement to provide, for direct sales to foreign manufacturers, a non-proprietary technical description of the products that will result from using encryption components, commercial source code described under 740.17(a)(5) or general purpose toolkits

This is a cumbersome requirement which is difficult to implement. The exporter has to differentiate between direct sales to manufacturers and sales to third parties for re-sale. It requires a manual intervention for each sale and does not allow distribution in larger quantities, i.e. does not permit us to follow our normal business model. Foreign manufacturers will clearly not want to comply with this type of restriction and it will drive them to use foreign competitors code to the disadvantage of US companies. We are requesting that this requirement be eliminated.

2. Source Code

a. 740.13(e)(1) and 740.17(a)(5)(i) - Products developed using publicly available encryption source code (both subject and not subject to an express agreement for the payment of a licensing fee or royalty)

The regulation needs to clarify under what circumstances the above products require one time product review. We would like to point out that experienced exporters may know some of the answers below either through discussions with the BXA officials or through established practice; however, the clarifications need to be made in the regulation. The regulation needs to cover the following scenarios:

A. Products manufactured and exported from the US (when the product is developed by merely bundling or compiling of the source code)

3. Products up to and incl. 64 bit

742.15(b)(1) (i), (ii) and (iii) and 740.17 (a)(3)(vii) Products up to and including 64 bit

In order to streamline the process, all products up to and including 64 bit, without regard to key management, should be classified as 5A992/5D992. This change should be also brought forward to the Wassenaar Arrangement as soon as possible so that the control level for these products is uniform for all participating countries.

4. Key Length Increase for Retail Products

740.17(e)(3)(i) Key Length Increases

We were advised by the BXA that the intent of the regulation was that, once a product is classified as retail, changes to the key length made by a letter as specified in this section do not change the status of the product, i.e. it still remains retail. This intent needs to be incorporated into the regulation as today this section specifically requires another product review in order for the product to keep its retail status.

5. Change to the Retail Requirement

740.17(a)(3) - retail product distribution requirements

In addition to retail outlets, the regulation should add distributors and resellers as sources for sales in order to qualify a product as 'retail'. The regulation should also allow for 'anticipated sales and transfers', in addition to product sold or transferred. The reason for this change is that manufacturers may anticipate large sales which may not materialize.

6. Change to the CCL Entry 5A002

774 Category 5 - Telecommunications and Information Security - add additional language to include copy protection of DVD and MPEG data.

The regulation should be amended to add the following language to the List of Items Controlled by ECCN 5A002:

d.) 4.) Execution of algorithms (for audio/video data) restricted to performing decrypt and encrypt functions for tamper resistance purposes associated with the execution of copy-protected data.

7. Change to the CCL Entry 4D994

The regulation should be amended for ECCN 4D994 (non-communications

software) to Reason for Control to AT2 (from AT1) to reflect the same level of control as 5D992.b AT2 non-communication software controls.

In closing, we would like to thank the BXA for the opportunity to comment on the Regulation and we hope that the points made in this letter will receive favorable consideration.

Sincerely,

Vera A. Murray,
Manager, Encryption Exports
IBM Corporation, Export Regulation Office
Suite 1100, 1301 K Street, N.W. Washington, D.C. 20005
tel. (202) 515-5527, tie-line 8/622-5527; FAX (202) 515-5551; tl 8/622-5551
Internet: murray2@us.ibm.com

DEPARTMENT OF COMMERCE

BUREAU OF EXPORT ADMINISTRATION

Washington, DC

Revision to Encryption Items

15 C.F.R. Parts 734, 740, 742, 770, 772, and 774

Interim Rule

Comments of Lyndon D.S. Marquez

Lyndon D.S. Marquez
16 W. Montgomery Avenue #17
Ardmore, Pennsylvania 19003
April 26, 2000

B. Products manufactured and exported from the US (when the product is developed by other means beyond merely bundling or compiling of the source code)

C. Products manufactured from the source code outside the US and distributed outside the US. (The January 14, 2000 Federal Register regarding cryptography, Supplementary Information, Background, 4(e)(3), contains a Note that reads, "Neither review and classification nor re-export licensing requirements are required under this section for foreign finished products using U.S. origin source code, toolkits and components yet the foreign finished products remain subject to the EAR. Post-export reporting for foreign products developed for commercial sale with source code and general purpose encryption toolkits exported under this paragraph is limited to the name and address of the foreign manufacturer and certain non-proprietary technical information about the foreign product...."

The (official) regulation needs to clarify that such foreign products are exported/transferred/re-exported under either NLR or ENC retail and can be released to all end users including non-government end users without any further US Government review to obtain retail status. Likewise, Post-export reporting requirement is mentioned in the Background and pre-export reporting of these crypto items is specified in 740.17 (g)(3). For reasons already discussed above both pre-export and post-export reporting should be eliminated/avoided.

D. Is there a difference between a US and a non-US company for products in this category manufactured and distributed outside the US.

Both US subsidiaries and non-US companies outside the US should be treated the same. If there is a difference in treatment, though, it should be stated in the regulation. US subsidiaries should, at a minimum, have the same ability of exporting the code as non-US companies, if the product is developed by merely bundling or compiling of the software, there should be no US Government review. At most, a non-proprietary technical description could be provided to the US Government at, or shortly after, the time of export.

b. 740.13(e) Publicly available source code-not subject to licensing fee or royalty

If the source code is made publicly available as described in Part 740.13(e)(1), it is deemed TSPA and not subject to the EAR. To do otherwise and control such encryption source code under TSU is confusing - it introduces two different authorizations for the same method of distribution.

Table of Contents

- I. Summary of Points
- II. Do the New Rule Resolve the Differences?
 - A. Background
 - B. The New Rules
- III. Business and Industry Interest
 - A. How Previous Restrictions Effected Business
 - B. How the New Rule Will Effect Business
- IV. National Security and Law Enforcement Interest
 - A. How National Security Concerns Drove Strong Encryption Export Restriction
 - B. How the New Rules Impact National Security and Law Enforcement
- V. Free-Speech Interest
 - A. The Constitutional Argument
 - B. How the New Rules Impact Privacy Interest
- VI. Conclusion

I, Lyndon D.S. Marquez, respectfully submit comments on 15 CFR Parts 734, 740, 742, 770, 772, and 774, Revisions to Encryption Items. I am a third year student at the Villanova University School of Law.

I. Summary Points.

- A. The new rules implemented to relax the restrictions on strong encryption export were long overdue and satisfied the U.S. high-tech company interest and the national security / law enforcement interest to varying degrees.
- B. The new regulations allow U.S. high-tech companies the opportunity to maintain the lead in encryption technology and regain their lost market share that resulted from the previous regulations.
- C. National security interests are met by allowing for stronger encryption (to protect the large amount of electronic communication carried out daily by the military), while law enforcement interest have been appeased by the commitment of the Administration to measures that will protect the ability or law enforcement to gain access to electronic information.
- D. Free-speech interests pertaining to the export of encryption products will never be fully realized, but streamlining of the export procedures will minimize the negative impact of free-speech.

II. Do the New Rule Resolve the Disputes Between the Three Primary Interests?

The new rule provides breathing room for the U.S. high-tech business interest and national security / law enforcement interests, while being less intrusive on free-speech interests. First, national security / law enforcement interests are sufficiently satisfied, but future changes are necessary to address the issue of whether strong

or weak encryption is best for national security. Second, the interest of business seems to be the real driving force in improving the monitoring of encryption, and thus has made modest gains through this proposed rule. Nevertheless, business could benefit further by the complete elimination of restrictions on the encryption levels allowed by regulation. Third, free-speech continues to be impacted with this new rule amending Export Administration Regulations, even though the rules have eased up on the extent of government control. Considering the Appellate Courts in Bernstein v. Department of State, and more recently in Junger v. Daley, have ruled encryption to be speech, the new rule continues to infringe on the right of free-speech in requiring inspection and government access to encryption codes.

I believe that the system that has been developed to monitor encryption products is far from perfect. However, the latest amendments to the Export Administration Regulations have sought to appease the three primary interests in the debate. The proposed change still ensures that national security interests and law enforcement are given the ability to monitor cyberspace to prevent its use by criminals and terrorists. Additionally, the infringements of key access by governmental law enforcement agencies are reduced, thereby allowing for greater freedom in the exercise of speech. These two interests will always be at odds. With the current technology available, it seems unlikely that there will be any resolution in the near future completely resolving this dilemma. This being said, the business interest has been the one most able to make gains. With the removal, or subsiding of tight monitoring programs, business is able to provide foreign markets with strong encryption. American software and hardware companies will be able to maintain the edge they have in the technology and be able to sell to a variety of customers that have previously been scrutinized closely. This makes for good business for American companies.

A. Background

The administrative responsibility over cryptology falls to the Department of Commerce's Bureau of Export Administration. Before this, the U.S. Department of State

maintained control over the export of cryptology. The Arms Export Control Act of 1968 and the implementing International Traffic in Arms Regulations (ITAR) were enforced by the State Department.¹ A restricted-export Munitions List was created under ITAR for items that were determined a threat to the national security of the country - including encryption technology.² This explains why cryptology is regulated the way it is today.

The current limitations on the strength level of encryption was born out of the restrictions placed on cryptology when it was regulated by the State Department. At the time, the State Department required that a company apply for a license to export "cryptographic software with the capability of maintaining secrecy or confidentiality of information or information systems".³ The initial actions by the State Department in regulating cryptology exports has set the stage for the current controversy over the export restrictions. The restrictions on the export of strong encryption products were buffered with the granting of exceptions to this regimen based on certain classifications. Encryption that was considered "algorithm-neutral" were excepted from the restriction against export of strong encryption. There were nine exceptions, including cryptology utilized by the financial industry and broadcast encryption.⁴

The U.S. Department of Commerce, Bureau of Export Administration (BXA) currently administers the regulation and monitoring of cryptography exports. In November 1996, President Clinton issued an Executive Order that transferred control over encryption exports from the State Department to the Department of Commerce.⁵ With the change in controlling agencies came the change in the statutory and regulatory framework under which encryption products are managed. Instead of the Arms Export Control Act and the Munitions List, the Export Administration Act of 1979 and the Commerce Control List determines what non-military encryption products are exportable.⁶ Despite this change, the treatment of encryption exports has changed very little. The same mind-set still prevails over the extent and means of controlling the export of encryption products.

In the four years since President Clinton issued the Executive Order that placed encryption products under the control of the Department of Commerce, the developments in

encryption software and hardware, as well as the nature of the industry on the global scale has progressed beyond the strictures of the American regulatory regime. Where U.S. encryption vendors were virtually unrivaled in the development and supply of cryptology safeguards to the world, foreign software and hardware companies are becoming keen competitors for supplying these products around the world. This poses clear problems for U.S. high-tech business and national security / law enforcement if we continue on this strict regime of export controls on encryption products developed and manufactured by American businesses and intended for export. Diametrically opposed to these interests is that of the Constitutional right to free-speech that is argued to apply to encryption.

B. The New Rules

On September 16, 1999, a new approach to controlling the export of encryption items was announced. This new policy stands on three principles. First, a technical review of products completed before its sale.⁷ Second, a more efficient post-export reviewing process.⁸ Third, procedures providing for government review of strong encryption exports to foreign governments.⁹

The effect of this new regulation is to allow U.S. high-tech companies to export any encryption product overseas to commercial firms, individuals, and non-governmental users under a license exception. This includes an exemption from Internet download screening requirements. Along with this liberalization of restrictions is the new ability of U.S. encryption vendors to freely export, including to governmental end-users, encryption products that are readily available on the retail market.¹⁰ However, there still remains a one-time product review by the Bureau of Export Administration of these exports to foreign governments. The new rules have streamlined post-exporting reporting requirements. This was an effort to accommodate the business interest and appease the privacy advocates.

The changes reflected the commitment of the Clinton Administration to bring U.S. encryption export policy in line with the Wassenaar Arrangements. Cryptography products are now listed under the new Cryptography Note in Category 5 - Part 2 of the Commodity Control List. It decontrols mass

market encryption products up to and including 64-bits. Additionally, License Exception ENC was revised to allow export and re-export of encryption items to foreign subsidiaries of U.S. companies. However, the new rule did not change the restriction of encryption exports to countries listed as terrorists supporting states.

The remainder of this comment discusses the three primary interest in the debate over encryption export restrictions. The new rules reflect a pragmatic and realistic policy change that realized that U.S. high-tech companies were being harmed disproportionately to the stated purpose of these restrictions. National security and law enforcement are not harmed by the streamlining of the export procedures, so long as they are given the means of carrying out their criminal, terrorist, or espionage investigations. The privacy advocates must realize that the streamlining of encryption export improves the situation pertaining to prior restraint on free speech. Privacy interests will always be at odds with national security and law enforcement interests, and there will never be absolute privacy protection.

III. BUSINESS AND INDUSTRY INTEREST

There is no doubt that U.S. companies in the software and hardware industry are the primary beneficiaries of this new regulation. The question is, "How much have American companies benefitted?", or more importantly, "Does this new regulation benefit business enough to justify the diminished national security and law enforcement safeguards that previously existed?" In addressing these questions, it is important to analyze the issue by realizing that the rate of technological change and the regulatory actions of foreign countries on their domestic cryptology companies have an impact.

A. How Previous Restrictions Affected Business

Previous U.S. restrictions on cryptology exports have hurt U.S. companies. While the restrictions prevented U.S. suppliers from exporting strong encryption to foreign customers, it did not and could not stop foreign companies from selling their strong encryption products worldwide.¹¹

U.S. high-tech companies risked losing their technological lead, as well as their market share to foreign companies that were not hampered by their government. American companies that once had the lead in this technology were hindered from selling overseas, which allowed their foreign competitors to profit.

U.S. high-tech companies were further disadvantaged because they sold encryption products internationally that U.S. government agencies had access to through a trapdoor. This trapdoor allowed authorized wiretappers to use escrow keys to breach the privacy of encrypted electronic communications.¹² Moreover, since the strong encryption is already made available by foreign suppliers, the handicapping of U.S. companies does not appreciably increase national security or assist law enforcement. In fact, Semaphore Communications Corporation estimates that American companies are unable to export encryption products to 403 of the "Global 1000" multinational companies named by Fortune Magazine.¹³

The damage that past U.S. restrictions on the export of encryption has brought on the competitiveness of U.S. companies overseas is plain. The previous restrictions were difficult to change because of the adversarial stance taken between business interest and national security interest.¹⁴ However, U.S. high-tech businesses are aware of the problems that arise with strong encryption on national security. They argue that it is only U.S. companies that are being hurt by the restrictions on strong encryption exports. It is argued that, "no bad guys are being prevented from getting [128-bit] encryption by U.S. export controls."¹⁵ Again, U.S. encryption export restrictions only prevent American vendors from selling these strong encryption products overseas. There is nothing to stop the sale of strong encryption by non-U.S. vendors on the world market.

B. How the New Rule Will Affect Business

The question returns to whether the new rules benefit U.S. business enough to justify the detriment to national security and law enforcement. The new rules are a streamlining of the encryption export procedures. It will allow for the export of encryption products after a one-time review by the BXA. This relieves business of the cumbersome

license procedure that was required to sell the products to different buyers. Now, it is up to the U.S. vendor to track the encryption products it sells and report to the BXA. Additionally, commercial encryption source code, encryption tool kits, and associated hardware is exportable under a license exception for business and non-governmental users for their internal use and customization.¹⁶

The new rules generally will result in the increased competitiveness of U.S. vendors of encryption. Since the Wassenaar Arrangement was agreed upon in Vienna in 1998, the U.S. has done little to move toward standardization with other signators. On the flip side, the other signators have done little to abide by the agreement as well. However, the new rules bring the U.S. encryption export restrictions more in line with that Arrangement.

The liberalization of the export rules will be a boon for U.S. vendors. One forecast is that the relaxed restrictions will result in the widespread implementation of encryption on computer systems.¹⁷ This will make encryption more user-friendly, allowing for the further expansion of encryption use. Considering the speed of globalization, this will enhance both the U.S. and world economy. At the same time, it places U.S. high-tech companies in a position to remain at the cutting edge of encryption technology.

The policy change also establishes the resolve of the Clinton Administration to standardize encryption internationally. First, this move by the United States will send a signal that the U.S. is serious about standardizing encryption controls worldwide, in accordance with the Wassenaar Arrangement. Second, the United States, with the companies that arguably dominate the hardware and software industry, will lead the way in standardization by the mere mass of products and leading edge technology that it can thrust upon the market.

IV. NATIONAL SECURITY AND LAW ENFORCEMENT INTERESTS

Government agencies around the world have traditionally viewed strong encryption as being a military weapon. Even before the advent of the information age, government and military leaders recognized that information is power. The idea of coding and de-coding messages belonged to the far off world of government spies. Today, this act of coding

and de-coding, encryption, is one repeated everyday when we perform financial transactions at a bank's money machine or traverse the Internet. The use of encryption to provide security and privacy to these common, everyday activities has become increasingly important.

The technology exists today that can produce a near infinite number of possible coding solutions.¹⁸ This would make it extremely difficult, if not practically impossible, for unauthorized persons from breaking encryption and gaining access to the encrypted communications. Strong encryption instills confidence that our financial dealings, business communications, and everyday communications are secure from eavesdroppers who may use the information for their own benefit, and to the detriment of the authorized communicators. In a world of increasing globalization, where the Internet is becoming the primary means communication, maintaining secure electronic communications has become indispensable.

Although using strong encryption seems to be the proper means of securing communication, there is a down side to unbreakable codes. Testifying before the Senate subcommittee on Technology, Terrorism and Government Information in 1997, Louis J. Freeh, Director of the Federal Bureau of Investigation said that, "the widespread use of robust unbreakable encryption ultimately will devastate our ability to fight crime and prevent terrorism."¹⁹ Criminals, international terrorists, and spies will be able to communicate freely through cyberspace with the government and law enforcement incapable of discovering their plans. Espionage, criminal activity, and international terrorism will likely thrive in such a situation, because their plans will be better communicated to their conspirators, and in a more timely manner, and become more fully developed through the protection of strong encryption.

A. How National Security Concerns Drove Strong Encryption Export Restriction

National security and law enforcement interests have dominated U.S. policy on strong encryption export restrictions. Even with the end of the Cold War, the United States remains vigilant to the continuing espionage. Moreover, the espionage game has become more complex and

difficult to effectively track. The break-up of the Soviet Union and its system of satellite countries to help carry out their spying mission, has resulted in an marked increase in the number of players in espionage. In other words, the world has become more complex because of more individual an/or autonomous players. Thus, national security interests have continued to demand tight restrictions on the exports of encryption.

Moreover, the combination of cyberspace proliferation and the end of the Cold War has created a dangerous law enforcement dilemma. First, the Internet has created an opportunity for criminals and international terrorists to rapidly and more effectively plan and communicate their plan to their cohorts around the world. Second, strong encryption will prevent or hinder the ability of the National Security Agency and law enforcement from determining their plans and preventing their execution. Law enforcement needs to be able to easily break into the communications of suspected criminality, in order to prevent the commission of the crime. Strong encryption products exported to enhance security of communication between stateside business operations and their foreign subsidiaries also prevent law enforcement from thwarting economic and international terrorists.

Domestically, there were no bars to the use and distribution of strong encryption technology. The concern was with the distribution of strong encryption overseas. The National Security Agency and the military were primarily interested in preventing the exchange of sensitive and classified information in to and out of the country. Since 1968, the Arms Export Control Act (22 U.S.C. 2751-99) governed the overseas distribution of encryption systems. In relevant part, the statute states:

In furtherance of world peace and the security and foreign policy of the United States, the President is authorized to control the import and export of defense articles and defense services and to provide foreign policy guidance to persons of the United States involved in the export and import of such articles and services. The President is authorized to designate those items which shall be considered as defense articles and defense services

for the purposes of this section and to promulgate regulations for the import and export of such articles and services. The items so designated shall constitute the United States Munitions List.

As previously mentioned the Act was promulgated by ITAR through the State Department.²⁰ The State Department placed encryption technologies on the restricted-export Munitions List, treating it like any other military technology.²¹

The procedures under the auspices of the State Department required a license to export cryptographic material. Under ITAR, the license was required unless the cryptographic material fell into one of the nine exceptions. So, strong encryption was broadly restricted unless it fit into, among other categories, cryptology for financial transactions or broadcast signal scrambling. Although these two categories alone did comprise a large part of the encryption export on a daily basis, the procedures for exception approval was cumbersome and the discretion left to the controlling agency was dubious.

With the transfer of control over encryption to the Commerce Department and the Bureau of Export Administration in 1996, the regulations were altered only little. The statutory authority was transferred to the Export Administration Act of 1979.²² Accordingly, the initial Interim Regulations transferred non-military encryption technology from the Munitions List to the Commerce Control List.

The change of controlling agency allowed for a new perspective on the restrictions on encryption export. This move was partly in response to the realization of increased globalization, and that effective encryption is a key to insure confidence in this increased globalization. The Commerce Department is in a better position than the State Department to weigh the economic effect of the various restriction options. However, the Commerce Department has taken over a problem where the various interests are already firmly entrenched and hesitant to release whatever hold they may have from the previous policy.

In interpreting its intent with the initial Interim Regulations, the Commerce Department would permit the export of 56-bit key length DES or equivalent strength items under a License Exception if the vendor would commit to build

and/or market recoverable encryption items and assist in developing a supporting international infrastructure.²³ The Export Administration Regulations (EAR) amended immediately after the transfer to the Commerce Department, allowed licenses for three broad categories. First, mass market distribution permitted after a one-time review for technology that incorporates 40-bit or less key lengths.²⁴ Second, the exception allowed for products that incorporate key escrow and key recovery procedures that are approved by the Bureau of Export Administration. Third, it permitted encryption items that did not incorporate or use a key escrow system if its key length did not exceed 56-bits and a business plan was concurrently submitted outlining a plan to incorporate key recovery procedures within the next two years.

In issuing the Executive Order at that time, the Clinton Administration did not intend to consider whether comparable cryptography was available on the global market by foreign vendors. That Order stated:

I have determined that the export of encryption products . . . could harm national security and foreign policy interests even where comparable products are or appear to be available from sources outside the United States, and that facts and questions concerning the foreign availability of such encryption products cannot be made subject to public disclosure or judicial review without revealing or implicating classified information that could harm United States national security and foreign policy interests. [N]otwithstanding this, the Secretary of Commerce . . . may, in his discretion, consider the foreign availability of comparable encryption products in determining whether to issue a license in a particular case or to remove controls on particular products, but it is not required to issue licenses in particular cases or to remove controls on particular products based on such considerations . . .

As such, availability on the world market is not a factor the BXA is bound to weigh-in while determining the approval

of exception requests. This does not make sense. The result of such oversight is that U.S. vendors are harmed by being prevented from providing this cryptography abroad. At the same time, the foreign competitors of these U.S. companies are providing the technology to the world market with impunity.

The Clinton Administration took its case to the rest of the world. In December 1998, thirty countries convened a meeting in Vienna to discuss the encryption issue. The participating countries agreed to the Wassenaar Arrangement where the signatories assented to a standardization of encryption export rules. The goal was to embrace the idea of restricting the strength of exportable encryption items that coincided with the EAR. The Clinton Administration hoped to simplify their efforts to protect national security and law enforcement interests by having a majority the technologically advanced countries agree to keep the encryption strengths around the world at a weak level.

B. How the New Rules Impact National Security and Law Enforcement

The new rules are a long time in coming. The national security interest cannot hold on to the belief that weak encryption was the best way to ensure national security. The Department of Defense has changed its view. On the other hand, law enforcement still supports the old restrictions on exporting strong encryption.

The about face by the Defense Department resulted from events over the past few years that shook the old belief in weak encryption. There were a series of electronic attacks on defense facilities that would have been prevented by stronger encryption.²⁵ Although weak encryption would allow for easier monitoring against espionage and terrorists, the weak encryption makes the Department of Defense vulnerable to even the less sophisticated hacker. Strong encryption would protect the increasingly electronic dependent military, which is the largest single entity that operates in cyberspace.

Law enforcement still has its reservations about the wisdom of easing the restrictions. When the Administration announced the policy change last year, Attorney General Janet Reno was critical of the move. Although acknowledging

that the new rules will assist law-abiding persons in maintaining their security and privacy, she cautioned that "the policy the administration is announcing today will result in greater availability of encryption . . . criminals and terrorists will use encryption".

However, the new policy shift does not leave law enforcement completely in the cold. This relaxing of encryption export rules is part of a three-part proposal that will allocate more funds to the FBI-based Technical Support Center to aid in its cyberspace research and support new laws that will protect law enforcement procedures for gathering electronic information in their investigations.²⁶ Law enforcement interests on the encryption export issue were set aside by the Administration for the greater good that would result from supporting U.S. high-tech company interests. Fortunately, the Administration seems committed to lighten the negative impact on law enforcement.

V. FREE-SPEECH INTERESTS

The Constitutionality advocates on the issue of encryption restrictions have been vocal over the years. Where business interests lack cohesiveness and one strong voice, the privacy interest have been more successful in heading off the national security / law enforcement camp. There have been a line of federal cases that have touched on the unconstitutionality of prior restraint on encryption exports.

Most recently, the Court in Junger v. Daley reversed and remanded a District Court ruling that denied the right of Junger to post on the Internet an encryption program that exceeded the export limitations on encryption strength. The Court concluded that the computer language was considered speech that is protected under the First Amendment. This is the latest in the well-publicized efforts of privacy interests to challenge the encryption restrictions of the government.

The new encryption regulations announced by the Clinton Administration in September 1999 and implemented in January 2000 is applauded by U.S. high-tech companies, while still maintaining support of the National Security / Law Enforcement interests. However, the privacy community, the American Civil Liberties Union (ACLU) chief among them,

continue to cry "foul". The new rules still leave open the issue of researchers who want to publish their source code on the Internet.²⁷ The ACLU argues that the encryption rules treat encryption software and technology differently when it is posted on the Internet than when it is published in other media. Posting on the Internet is considered by the rules to be exporting. The rules require that electronic export of publicly available encryption source code be filtered through the BXA. Print media is not met with the same bars as when encryption software is made available on the Internet.

A. The Constitutional Argument

When authority over cryptology was transferred from the State Department to the Commerce Department and the BXA, the procedural changes were not substantial. The BXA still placed a limit on the strength of the encryption products that were exportable. The licensing requirement remained, with additions to the categorical exceptions. For example, there was the license exception for banks when they are dealing with financial software. The BXA also required a means of key recovery.

Non-military cryptology became the responsibility of the Department of Commerce. The cryptological products that were previously on the Munitions List were placed on the Commodity Control List. The items on this list are given an Export Control Classification Number that provides explanation for its placement on this control list. Encryption items are category 5D002, denoting placement on the control list for national security reasons.²⁸ The restriction placed on 5D002 items is the requirement of a license for export overseas. However, encryption items in printed form are not subject to this same restriction. Only encryption software in the electronic form is restricted by the rules. Moreover, consider the fact that the mere posting of encryption software on the Internet is considered exporting because of the ability of somebody overseas to download the software.

Constitutional issues arise under such a system of control. First, whether the encryption rules are a prior restraint on protected speech. Second, whether the encryption restrictions amount to content-based regulation

of speech. The second issue was addressed by the Sixth Circuit in Junger.

The Sixth Circuit reversed the District Court's granting of summary judgement in favor of the government. The District Court found that encryption source code does not amount to content-based restrictions and does not enjoy the protection of free speech.²⁹ Although it acknowledged that source code has an expressive feature, the District Court found that its functional feature was the more dominant characteristic of the source code. The functional feature of the source code being the means by which the software can interpret computer instructions. Computer programmers familiar with a particular computer programming language are able to read and understand source code.

This decision by the District Court does not comport to previous decisions by the Supreme Court on the content of speech. In Roth v. United States, the Court said that "all ideas having even the slightest redeeming social importance" are protected by the First Amendment.³⁰ In essence, the Court set the threshold for determining the applicability of the First Amendment low. Source code is a language known to programmers that is used to communicate instructions. There is clear redeeming value to communication through source code.

Constitutional protections are not reserved solely for expressive speech. The Supreme Court indicated the broad meaning attached to speech that is protected by the First Amendment in Hurley v. Irish-American Gay, Lesbian and Bisexual Group.³¹ The Court said that such things as artwork and music are "unquestionably shielded" by the First Amendment.³² Thus, symbolic speech has redeeming social value even if they exhibit both a functional and expressive nature. The Sixth Circuit concluded that source code is an expressive means for the exchange of ideas and information among programmers, and is constitutionally protected, reversing the lower court.

Now, the question turns to whether the intermediate scrutiny standard is met. In applying intermediate scrutiny, the court must determine if the regulation "furthers an important or substantial governmental interest".³³ In Turner Broadcasting System v. FCC, the Court said that the government must do more than hide behind the assertion of national security, and provide clear proof that

national security is directly affected.³⁴ With the end of the Cold War, the rally cry that national security is at risk no longer suffices. In order to meet the intermediate scrutiny standard, the government must show how national security is jeopardized and the extent of the risk.

B. How the New Rules Impact Privacy Interest

The new rules properly have the government changing its role in administering encryption. The realities of globalization and the essential role of cyberspace requires that the government permit stronger encryption exports to secure communications overseas. The Department of Defense and the Intelligence community now believe that strong encryption is essential. Unfortunately, with allowance of stronger encryption comes the need for governmental and law enforcement agencies to access the source codes.

The policy change streamlines export procedures and transforms the role of the BXA to initially reviewing then monitoring exported encryption. Marc Rotenberg, executive director of EPIC believes that the BXA is moving from a "gatekeeping" role to a surveillance role.³⁵ This may be due to several factors. First, national security interests have determined that in order to protect the sensitive information transmitted overseas, strong encryption is necessary to prevent spies or terrorists from intercepting the information. Second, the business interest has garnered enough support in Congress to threaten legislation that would sharply curtail the ability of the Administration to shape the encryption export rules the way it wants. Third, the Administration may have come to the realization that it cannot stem the tide, and would be better off with a system of monitoring versus that of controlling.

The new approach to export policy is based on three principles. First, the BXA will perform a technical review of encryption items before they are distributed. Second, the reporting system after the encryption products are sold has been made more amenable to U.S. high-tech companies. Third, the government still retains its authority to review strong encryption products to other governments. This new policy approach was intended to satisfy the needs of U.S. companies, while maintaining the national security interest.

The new rules, in essence, remove the previous system

of granting licenses or permitting products through license exceptions. The BXA will review encryption products initially. After this review, the companies themselves are responsible for tracking the products and reporting their sales.

Despite the streamlining, proponents of constitutional protection of free speech are not pleased with the changes. They point out that little was done to remove the barriers to free expression. The new regulations were geared to support the business interest, while government still maintains the prior restraint on speech. Prior restraint is illustrated by the requirement that encryption software still be reviewed by the BXA before export, especially if the product is strong encryption to foreign governments. Additionally, regulations still require that vendors track their exports and report to the BXA. These aspects of the new rules do not completely remove the infringement on free expression. The proponents of free-speech fail to realize that there will always be some restraint on encryption exports. The streamlining resulting from the new rules softened the blow of prior restraints, and is likely the best that can be hoped for at this point in time.

VI. CONCLUSION

The new rule amending the Export Administration Regulations shows the Clinton Administration's good faith in working out the dispute over the export of non-military encryption products. The three primary interests (national security/law enforcement, U.S. high-tech companies, and free-speech) have been at odds for several years on this issue. National security has been the dominant voice in the shaping of the export regulations. This is further illustrated by the initial placement of encryption under the State Department and on the Munitions List. Law enforcement would still prefer the tight restrictions on the export of strong encryption. However, there seems to be a change in thinking in the Defense establishment that shifts their advocacy to one that supports strong encryption. This has opened the door for business interest.

The once fragmented voice of the business interest has recently garnered the ear of Congress. Congress has applied pressure on the Administration to act. In 1999, the House

was pushing for legislation (SAFE) that liberalized the encryption export rules. At the same time, the Senate was seriously considering legislation (PROTECT) that also liberalized the export restrictions. The Clinton Administration's sudden policy change may be due to this legislative pressure. The new rule is definitely in the right direction for the sake of bolstering U.S. high-tech companies that are trying to compete with foreign suppliers of encryption products.

The advocates for privacy and free-speech have gained a little from the new rule. They have certainly won many battles in court over the issue of categorizing encryption codes as protected speech. Nevertheless, it is yet to be seen if the intermediate scrutiny burden of the government to show an important or substantial national security risk will go the way of free-speech advocates when dealing with encryption exports.

The new rule is just enough, just in time. Although the dispute between free-speech and national security/law enforcement will probably never be resolved, the rift between national security and the high-tech companies has been repaired. The new rule is a compromise position that should sufficiently support business interest in maintaining their position as leaders in the encryption field, while providing enough provisions to maintain national security. Privacy advocates should realize that the new rules have offered some benefit to their cause, and there will never be absolute privacy in the face of ever present national security and law enforcement risks.

1. 22 C.F.R. 120.1-130
2. See Exec. Order No. 13,026,61 *Fed Reg.* 58767 (1996).
3. John T. Soma, "Article: Encryption Key Recovery, and Commercial Trade Secret Assets: A Proposed Legislative Model", 25 *Rutgers Computer & Tech. L.J.* 97, 105 (1999) (citing 22 C.F.R. 121.1 cat. XIII(b).)

4. 22 C.F.R. 121.1 cat. XIII(b).
5. See Exec. Order No. 13,026, 61 *Fed. Reg.* 58,767 (1996).
6. Soma at 107.
7. Federal Register/Vol. 65, No. 10/Friday, January 14, 2000/Rules and Regulations, p. 2492.
8. *Id.*
9. *Id.*
10. U.S. Department of Commerce, "Commerce Announces Streamlined Encryption Export Regulations", January 12, 2000 (<http://204.193.246.62/public.nsf/docs/60D6B47456BB389F852568640078B6C0>).
11. Ellen Messmer, "Encryption Restriction Policy Hurts Users, Vendors", *Network World*, August 23, 1993.
12. Jack Robertson, "U.S. Still Dragging its feet", *Electronic Buyer's News*, August 17, 1998.
13. See Messer.
14. *Id.* (Ed O'Malley as Deputy Director of Corporate Security for MCI Communications, Inc., and former head of the FBI's national espionage program in electronic transmissions, argues that the strict encryption export controls damage U.S. competitiveness abroad.)
15. Alan Radding, "Encryption and You", *Computer World*, June 29, 1998 (quoting James Dempsey, senior staff counsel at the Center for Democracy and Technology in Washington).
16. See U.S. Department of Commerce.
17. Davis Wilson, "Attorney General Janet Reno Speaks Against Exporting Encryption", *San Jose Mercury News*, September 17, 1999.
18. See Security and Freedom Through Encryption (SAFE) Act. H.R. Rep. No. 105-108, pt. 1 at 28 (1997).
19. The Encryption Debate: Criminals, Terrorists, and the Secret Needs of Business and Industry, Hearing Before the Sub-Committee on Technology, Terrorism, and Government Information of the Senate Committee on the Judiciary, 105th Congress (1997).

20070

20. 22 C.F.R. 120.1.
21. Id. at 120.2.
22. 50 U.S.C. 2406 (1994).
23. Encryption Items Transferred from the U.S. Munitions List to the Commerce Control List, 61 Fed. Reg. 68,572-573 (1996).
24. 15 C.F.R. 742.15(b)(1) (1998).
25. See Wilson.
26. Scott Bradner, "Privacy and Security Enhancing Technology", Network World, September 27, 1999.
27. Jeri Clausing, "New Encryption Rules Leave Civil Libertarians Unhappy", New York Times on the Web, January 18, 2000.
28. 15 C.F.R. 742.
29. See Junger v. Daley, 2000 U.S. App. LEXIS 6161; 2000FED App. 0117P (6th Cir.).
30. See Roth v. United States, 354 U.S. 476, 484 (1957).
31. See Junger v. Daley.
32. Id.
33. See United States v. O'Brien, 391 U.S. 367, 377 (1968).
34. See Turner Broadcasting System v. FCC, 512 U.S. 622, 624 (1994).
35. Id.

May 10, 2000

To: BXA Hillary Hess
From: Bill Root
Subject: January 14 Encryption Regulation

Comments on the subject regulation follow:

EI

The designator EI serves no useful purpose and should be replaced by references to 5A002, 5D002, and/or 5E002.

EI applies only to encryption items transferred from the USML to the CCL consistent with EO 13026 of November 15, 1996, according to 5A002, 5D002, and 5E002 License Requirement Notes. This indicates that EI does not apply to encryption items which were on the CCL before the 1996 transfer. However, nowhere in the EAR is there an identification of which encryption items are EI and which are not. Even an exporter who researches pre-1996 and post-1996 State and Commerce control lists cannot determine which items are EI, because unpublished commodity jurisdiction determinations affect what was, or was not, transferred.

It is believed that, immediately prior to January 14, 2000, all items transferred in 1996 were controlled by ECCNs 5A002, 5D002, or 5E002 and the only encryption items on the CCL before the 1996 transfer were properly classified under ECCNs 5A992, 5D992, or 5E992. If that is correct, after January 14, 2000, some EI items are now properly classified under 5A992, 5D992, or 5E992, because 5A002 coverage was reduced and 5D002 and 5E002 coverage is related to 5A002. The statement in 15 CFR 742.15(a) that EI items "include" those controlled under 5A002, 5D002, and 5E002 implies that there are also EI items controlled elsewhere. However, there is nothing in the EAR to indicate an intent to have two control regimes for 5A992, 5D992, and 5E992, one for EI items and the other for non-EI items.

Other portions of the EAR indicate that EI applies to all encryption items, not just those transferred in 1996. 742.15(a) states that "EI" stands for "encryption items" and refers to part 772 for the definition of "encryption items." Part 772 defines "encryption items" as including "all encryption commodities, software, and technology that contain encryption features and are subject to the EAR."

Still other portions of the EAR are inconsistent as to whether EI covers all, or only some, encryption items. 734.3(b)(3) provides that only software controlled for EI reasons under ECCN 5D002 is excepted from the publicly available software exclusion from "subject to the EAR." However, the statement in the Note to 734.3(b)(2) and (b)(3) that encryption source code in electronic form remains subject to the EAR is not limited to EI items nor to ECCN 5D002, leaving in doubt whether publicly available non-EI or 5D992 source code in electronic form is

subject to the EAR.

Still other portions of the EAR are simply confusing as to the consequences of the use of the term EI. 770.2(m) states that software controlled for EI reasons under ECCN 5D002 is eligible for License Exceptions BAG and the tools of trade portion of TMP for laptop computers loaded with encryption software. 770.2(m) is silent as to whether non-EI items under ECCN 5D002 or EI or non-EI items under 5D992 are eligible. 5D992 is not an issue for TMP tools of trade to embargoed countries (740.9(a)(3)(i)(A)) but it is an issue for Syria. Both embargoed countries and Syria are generally eligible for BAG and the 770.14(f)(3) provision that EI items may not be exported to those countries indicates that non-EI items are eligible. 740.14(f)(3) does not mention 5D002; but reading it together with 770.2(m), which does mention 5D002, leads to the conclusion that the EI portion of 5D992 is also eligible.

740.14(f)(1) provides that only a U.S. citizen or permanent resident may permanently export EI items under BAG. This leaves open the possibilities that anyone (whether or not a U.S. citizen or permanent resident) may (1) temporarily export EI items under BAG (most baggage exports are temporary); (2) either permanently or temporarily export non-EI items under BAG; and (3) (if read together with 770.2(m)) either permanently or temporarily export 5D992 EI items under BAG.

5A992, 5D992, 5E992

Deletion of 5A992, 5D992, and 5E992 should be considered.

The definition of "export of encryption source code and object code software controlled for EI reasons under ECCN 5D002" in 734.2(b)(9)(ii) does not apply to exports to embargoed destinations or Syria of software controlled under ECCN 5D992. If none of the precautions in that definition need be taken with respect to 5D992 software, controls on 5D992 exports to Syria would probably be ineffective and there would be no reason to keep 5D992 on the Commerce Control List (EAR99 covers software not elsewhere specified for export to embargoed destinations).

The lack of a license requirement for 5A992 reexports to Iran and Sudan (742.8(a)(2) and 742.10(a)(2)) indicates that the need for 5A992 is also marginal.

The EAR statement in 15 CFR 734.4(b) that items classified ECCN 5A992, 5D992, or 5E992 "may be" eligible for *de minimis* is followed by "(refer to 742.15(b)(1))." However, there is nothing in 742.15(b)(1) which is relevant to the *de minimis* exclusion. Since only EI items controlled under 5A002, 5D002, or 5E002 are excepted from *de minimis*, items otherwise controlled under 5A992, 5D992, 5E992, or EAR99 are, not "may be", eligible for *de minimis*.

Silent License Exceptions

The EAR is silent as to encryption item eligibility for many License Exceptions. Encryption items are explicitly eligible for License Exceptions KMI, ENC, tools of trade portion of TMP, BAG, and the unrestricted encryption source code portion of TSU. Encryption items are explicitly ineligible for License Exceptions LVS, GBS, CIV, TSR, international safeguards and cooperating government portions of GOV, GFT, and mass market software portion of TSU. The EAR is silent as to whether encryption items are eligible for any of the other License Exceptions.

The silent ones which are reasonable candidates for encryption item eligibility include: remaining portions of TMP; RPL; U.S. Government and Chemical Weapons Convention portions of GOV; operation, sales, and software updates portions of TSU; equipment and spare parts for a vessel or aircraft portion of AVS; and APR.

One might conclude that License Exceptions do apply when they are silent. 736.1 states: "A person may undertake transactions subject to the EAR without a license or other authorization, unless the regulations affirmatively state such a requirement." On the other hand, it might be argued that this general rule is over-ridden, at least for software, by the 5D002 first Note statement that encryption software is not accorded the same treatment under the EAR as other software. However, perhaps all the intended differences have already been identified.

Publicly Available

It seems irrational that printed material setting forth encryption source code qualifies for the publicly available exclusion from "subject to the EAR," whereas the same information in electronic form does not (734.3(b)(2) and (b)(3) Note).

It is not apparent why embargoed countries and Syria are disqualified from the publicly available rules in 740.13(e) and 740.17(a)(5)(i), since the concept of "publicly available" is that such items cannot be controlled to any destination.

The EAR statement in 732.2(b)(1) that you may not proceed to export publicly available technology or software if you are a U.S. person and the export is subject to General Prohibition Seven (which includes an encryption provision in 744.9) does not appear as an exception in the operative rule in 734.3(b)(3) that publicly available technology and software is not subject to the EAR.

Deemed export

734.2(b)(2) removes EI encryption software from the deemed export rule for nationals of all countries. It may have been intended that this deemed export exception also apply to technology. If so, the exception for nationals of embargoed countries and Syria from the 740.17(a)(1) rule permitting U.S. firms to transfer encryption technology to their foreign employees in the United States could be removed..

De minimis

740.17(d) states: "Foreign products ... incorporating U.S.-origin encryption source code, components or toolkits remain subject to the EAR but do not require review and classification by BXA and can be exported or reexported without further authorization." This permits reexports to all destinations except embargoed destinations or Syria of the specified U.S.-origin encryption items when incorporated in foreign-made items even if the 25% *de minimis* limit in 734.4(d) is exceeded. Therefore, the statements that there is no *de minimis* level for 5A002, 5D002, and 5E002 (734.4(b)) and that U.S.-origin 5D002 software and 5E002 technology do not lose their U.S.-origin when commingled with items of any other origin (734.4(h)) are misleading. The only substantive consequence of the phrase "remain subject to the EAR" in 740.17(d) appears to be to provide a basis for requiring a license for trivial U.S. content in foreign products to embargoed or terrorist countries. This is illogical in the light of the liberal treatment of U.S. content in foreign products to other destinations.

734.4(h) states that software or technology controlled by 5D002 or 5E002 does not lose its U.S.-origin when commingled with software or technology of any other origin. This implies that software or technology controlled by other items, such as 5D992 or 5E992, does lose its U.S.-origin when commingled with foreign software or technology. However, this would be inconsistent with 734.3(a)(3) and (b)(4), which provide that commingled software or technology is subject to the EAR unless it is *de minimis*. The 734.4(h) rule is, therefore, confusing and serves no apparent useful purpose.

Other anomalies

740.17(a)(1) refers to "foreign subsidiaries of U.S. companies (as defined in part 772)." However, the term defined in part 772 is "U.S. subsidiary."

The terms used in (1) the Cryptography Note (774 Supplement 1 Category 5 Part 2 Note 3), (2) the description of "retail" (740.17(a)(3)), and (3) the mass market software portion of License Exception TSU (740.13(d) and 774 Supplement 2) are similar; but what appear to be needless differences are confusing. There are no apparent differences in meaning between:

- "retail selling points" vs. "retail outlets independent of the manufacturer" plus "sales directly by the manufacturer for consumer use";
- "from stock" vs. "not customized";
- "designed for installation by the user without further substantial support by the supplier" vs. "not require substantial support for installation and use"; and
- "electronic" vs. "intangible."

Different expressions should not be used to convey the same meaning. Conversely, if different meanings are intended, they should be apparent to the reader.

The Cryptography Note is used to condition a greater degree of liberalization than "retail." It, therefore, seems irrational to make "intangible" transfers ineligible for "retail" sales through outlets independent of the manufacturer whereas "electronic" transfers are eligible for Cryptographic Note sales through such outlets.

It is not apparent why intangible should be permitted for “retail” sales directly by the manufacturer but not for sales through outlets independent of the manufacturer.

The following revisions to 742.15(b)(1)(i,ii) are necessary to conform with ECCN 5A002.a.1:

- (i) ~~56-bit encryption commodities, software and technology~~ “Symmetric algorithm”. Encryption commodities, software and technology employing a key length up to and including 56-bits ~~with an asymmetric key exchange algorithm not exceeding 512 bits may be classified under ECCNs 5A992, 5D992 or 5E992~~
- (ii) ~~Key management products~~ “Asymmetric algorithm”. ~~Products which only provide key management with asymmetric key exchange algorithms not exceeding 512 bits may be eligible for classification under ECCNs 5A992 or 5D992. Where the security of the algorithm is based on any of the following:~~
 - (A) Factorization of integers in excess of 512 bits (e.g., RSA);
 - (B) 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
 - (C) Discrete logarithms in a group other than mentioned in (B) in excess of 112 bits (e.g., Diffie-Hellman over an elliptic curve).

742.15(b)(1)(i), (ii), and (iii)(A) are redundant. License requirements are defined on the Commerce Control List and do not belong under the heading of Licensing Policy.

742.15(b)(1)(iii)(B) concerns grandfathering as well as license requirements, rather than licensing policy, and would logically be moved to 740.17(e)(2).

The following revisions to 748 Supplement 2 (c) are necessary to conform with the “must also be evaluated” wording (emphasis added) in 774 Supplement 1 Category 4 Note 2:

Digital computers, telecommunications, and related equipment. If your license application involves items controlled by both Category 4 and Category 5, your license application ~~must be submitted according to the principal function of the equipment will be evaluated against the performance characteristics of both Categories.~~ License applications involving digital computers ~~controlled by Category 4~~ must identify a Composite Theoretical Performance (CTP) in Block 22(b). ~~If the principal function is telecommunications, a CTP is not required. Computers, related equipment, or software performing telecommunication or local area network functions will be evaluated against the telecommunications performance characteristics of Category 5, while cryptographic, cryptanalytic, certifiable multi-level security or certifiable user isolation functions, or systems that limit electromagnetic compatibility (EMC) will be evaluated against the information security performance characteristics of Category 5.~~

The first 5D002 Note states; “Encryption ... software is not accorded the same treatment

under the EAR as other “software”; and for export licensing purposes, encryption software is treated under the EAR in the same manner as a commodity included in ECCN 5A002.” However, in other parts of the EAR encryption software is treated as a subset of “software” and nowhere else in the EAR is 5D002 treated as a commodity included in 5A002.

ECCNs 5A002, 5B002, 5D002, and 5E002 contain License Requirement Notes referring to 743.1 for reporting requirements for exports under License Exceptions. However, there are no such reporting requirements in 743.1, nor should there be, since these items are not included in Wassenaar Annex 1, which is the basis for 743.1 reporting requirements.

The lists of items not controlled by ECCNs 5A002 and 5D002 irrationally appear in sections headed “Related Controls”



May 11, 2000

Frank J. Ruggiero
Room 2705
Regulatory Policy Division
Bureau of Export Administration
U.S. Department of Commerce
14th Street and Pennsylvania Avenue N.W.
Washington, DC 20230

Re: Comments on Revisions to Encryption Items (65 FR 2492)

Dear Mr. Ruggiero:

Sun Microsystems, Inc. (Sun) appreciates this opportunity to comment on the Revisions to Encryption Items published by the Bureau of Export Administration (BXA) on January 14, 2000 (65 FR 2492) amending the Export Administration Regulations (EAR, 15 CFR Part 730 et seq.).

Sun believes that the revisions to the encryption export controls published on January 14, 2000, are an important first step toward preserving the international competitiveness of American companies. However, a recent decision by the European Union to remove licensing for sales within the 15 member countries and 10 other countries, and to eliminate technical reviews by national security agencies, threaten to place American companies at a disadvantage again.

In the preamble to the interim rule, BXA promised:

5. A number of companies have expressed concern that the European Union (EU) may implement a general authorization permitting encryption items to be exported freely within the EU and other specified countries. If and when the EU implements such an authorization, the Administration will take the necessary steps to ensure U.S. exporters are not disadvantaged.

Sun believes that BXA should amend the EAR at the earliest opportunity, eliminating the technical reviews and creating a license free zone for exports to these countries, so that American companies are not disadvantaged by the EUs recent action.

In addition, Sun offers the following specific comments to the interim rule.

1) Technical Reviews

In Sun's experience, the technical reviews are taking very long, indeed. We have heard that the number of cases submitted has increased 200% while two licensing officers have been taken off the encryption area at BXA. (Meanwhile, NSA is also undergoing organizational and personnel changes.) We recommend that both BXA and NSA devote the resources required to complete technical reviews (including retail determinations) in a timely manner, preferably within 30 days of application.

2) Reporting

Sun respectfully submits that the reporting requirements be reduced or eliminated. Because of the different rules that apply depending on the product and/or customer, it is difficult to know how to deal with the reporting requirements. We believe that the special reporting requirement for the sale of network infrastructure products to telecommunications and Internet service providers is burdensome and should be eliminated, and other reporting requirements should be streamlined to require only information related to the initial export from the United States (where required).

3) Crypto APIs/Source Code

Because the regulations have been amended to allow the export of open and community crypto source code with notice to BXA, it seems redundant to require technical review of the executables of the same source code. Sun believes that the binary form of open or community source should be exportable under the same terms as the corresponding source code. In addition, it seems unlikely that effective control can be maintained with respect to compiled binaries with open cryptographic interfaces, once open or community source has been released on the Internet. Therefore, we recommend that the restrictions on binary code with open cryptographic interfaces be removed.

4) Definition of "Retail"

Sun remains concerned that products combining firewall and VPN capabilities in software may be considered network infrastructure products and therefore excluded from "retail" status. If these concerns are valid, then the government will be artificially forcing the market to move toward a model where these capabilities must be bundled into other products, such as operating systems. The government should not use export controls, even inadvertently, to create an uneven playing field among competing vendors.

5) Technology Transfer (Deemed Exports)


The regulations governing so-called deemed exports should be expanded. Currently, the EAR states that employees of U.S. companies are covered. The BXA web site suggests that this also includes self-employed natural persons, and this extension should be made explicit in the EAR. In addition, Sun believes that contractors and interns, who are employed directly or indirectly by U.S. companies, should be eligible to receive technology classified under ECCN 5E002 inside the United States.

6) Electronic Downloads of Non-Retail Products

Section 734.2(b)(9)(iii)(A) of the EAR states that companies may distribute non-retail encryption software via electronic downloads provided that they block downloads to .gov, .mil and similar addresses. Because this type of domain address verification is difficult to administer, we would like the EAR to authorize an alternative procedure based upon warnings and certifications by the parties requesting the download that they are not governments.

Thank you for this opportunity to comment on the interim final rule Revisions to Encryption Items.

Sincerely,



Hans Luemers
Director, Corporate Export Control

May 12, 2000

Mr. Frank J. Ruggiero
Regulatory Policy Division
Bureau of Export Administration
Department of Commerce
14th & Pennsylvania Ave., NW
Room 2705
Washington, DC 20030

Re: Comments on January 14, 2000 Interim Rule on Encryption Export Controls

Dear Mr. Ruggiero:

Mercantec, Inc. appreciates the opportunity to comment on the Department of Commerce, Bureau of Export Administration's January 14, 2000, Interim Rule which revises the controls on encryption items.¹ Mercantec is a leading provider of electronic commerce storefront software. Mercantec's SoftCart™ software enables merchants to expand their geographical reach by marketing and selling goods via the World Wide Web.

We appreciate that the Interim Rule makes many necessary changes that will support electronic commerce. However, the Rule does not go far enough to establish a level playing field for U.S. producers and marketers of products for online merchants, particularly in Europe, where the European Union has announced a "License Free Zone" for data-encryption products. Additional changes are necessary to prevent further erosion of U.S. market share worldwide, and to build trust for users and consumers in an electronic commerce environment. We urge the Department of Commerce to adopt the following changes.

Implement an immediate and corresponding response to the EU policy change.

We understand that the EU policy will allow unfettered distribution and sale of encryption products within the 15 EU countries, plus minimum regulatory requirements for export to 10 additional countries, including Japan and certain eastern European nations. These countries comprise approximately 80 percent of the world market. Mercantec's products are superior to any produced in the EU. Nevertheless, we will be at a competitive disadvantage unless corresponding changes are made in the U.S. policy.

¹ 65 Red. Reg. 2492, January 14, 2000

Internet Services Providers (ISPs), our direct channel of distribution to merchants, naturally prefer products that carry the highest level of security with the minimum level of regulatory control. The required technical reviews and reporting imposed by the Interim Rule, coupled with EU rumors that NSA tampers with codes of U.S. products to ensure they can tap into them, encourage ISP's to select non-U.S. products. Regardless of the superiority of our products, the United States will lose the world market, unless the Administration acts now to establish a license free zone for exports of encryption items to the EU and corresponding changes for exports to the additional countries included under the EU proposal.

Establish a sensible framework for reporting - eliminate reporting requirements on all retail products under 740.17(g).

All encryption products that are reviewed and classified as "retail products" under the Interim Rule should be exempt from reporting requirements.² The list of exemptions under 740.17(g) is confusing for the exporter and omits retail products that should be included, such as retail products for online merchants specifically designed to support electronic commerce. The current technical reviews and reporting system under the retail classification create a *de facto* licensing mechanism. This is not liberalization. To achieve the objective of the retail classification, all products that are reviewed and classified by the Bureau of Export Administration and the National Security Administration as "retail" should be exempt from reporting requirements. Alternatively, in order for the Administration to promote a strong electronic commerce infrastructure, the list of exemptions under 740.17(g) must be expanded to include exports to online merchants who use encryption products to support electronic commerce.

The Administration, in concurrence with our allies, has stated that strong encryption products will form the basis of the electronic commerce infrastructure and establish an environment of on-line trust. To realize the Administration's goal, exports to online merchants who use encryption products to support electronic commerce must be subject to minimal controls, free of burdensome and expensive reporting requirements.

Exports of encryption products for use by online merchants are sold through layers of distribution channels, e.g., producers sell to authorized distributors who in turn sell through ISPs, and ISPs generally make the products available to online merchants or individuals who want to establish a store on the Web. Under the Encryption Licensing Arrangement, product tracking and reporting have cost Mercantec approximately \$20.00 per unit sold. Under the Interim Rule, the reporting requirements for exports under License Exception ENC continue to place an expensive and unmanageable burden on our company.

Accordingly, it is imperative to reevaluate the reporting requirements under 740.17(g) of the Interim Rule and implement real reform under the retail classification.

² Section 740.17(g) exempts reports of retail products sold to individuals, but requires reports of retail products sold to businesses. This means that companies must establish additional screening procedures for business vs. individual uses, which makes little practical sense.

We appreciate the opportunity to comment on these regulations and urge the Commerce Department to adopt changes that will foster the growth of electronic commerce and preserve United States competitive position.

Sincerely,



Harriet Bury
VP Product Management

Cc: The Honorable J. Dennis Hastert, Speaker of the U.S. House of Representatives
The Honorable Judy Biggert, U.S. House of Representatives
Mr. James Lewis, Director of the Office of Strategic Trade

ENC 6
1013

Hewlett-Packard Company
Corporate Export Administration
900 17th Street, N.W., Suite 1100
Washington, D.C. 20006

202-884-7065
202-884-7070 fax

SENT VIA FAX TO 202-501-0784; 3 pages

May 12, 2000

Frank J. Ruggiero, Room 2706
Regulatory Policy Division
Bureau of Export Administration
U.S. Department of Commerce
14th Street and Pennsylvania Avenue N.W.
Washington, DC 20230

Re: Comments on Revisions to Encryption Items (65 FR 2492)

Dear Mr. Ruggiero:

Hewlett-Packard ("HP") Company appreciates this opportunity to provide comments on the interim final rule amending the Export Administration Regulations ("EAR", 15 CFR Part 730 *et seq.*) published by the Bureau of Export Administration ("BXA") on January 14, 2000 (65 FR 2492).

Historically, export controls on encryption have presented a significant impediment to international sales of products manufactured and sold by HP. Hence, the revisions to the encryption export controls published on January 14, 2000, are welcomed by HP and important to our international competitiveness.

Nevertheless, according to the Wall Street Journal of April 28, 2000, a recent decision by the European Union to remove licensing for sales within the 15 member countries and 10 other countries, and to eliminate technical reviews by national security agencies, threaten to place American companies at a disadvantage again, vis-à-vis our European competitors.

In the preamble to the interim rule, BXA promised:

5. A number of companies have expressed concern that the European Union (EU) may implement a general authorization permitting encryption items to be exported freely within the EU and other specified countries. If and when the EU implements such an authorization, the Administration will take the necessary steps to ensure U.S. exporters are not disadvantaged.

The appropriate response in our view would be to amend the EAR, eliminating the technical reviews and creating a license free zone for exports to these countries.

We have another, high level, concern, which is that the interim rule is too complex for practical administration.

For example, the interim rule sets forth at least one dozen different categories of encryption products within the affected Export Control Classification Numbers. The net result is that most cryptographic products may be exported to all destinations except the embargoed/terrorist countries, but subject to various review and reporting requirements that consume considerable time and effort within the company. We recommend that this complex classification system be collapsed into two, i.e. cryptography products with a variable key length less than or equal to 64 bits and products with a variable key length greater than 64 bits.

A second example is the reporting requirements which are unworkable in practice and seemingly unnecessary in light of the development of international standards. While HP appreciates the fact that the exemption from reporting for sales of "retail" products to individuals was introduced for the benefit of industry, in practice it

Frank J. Ruggiero
May 12, 2000
Page: 2

2 of 3

has proved difficult or impossible to determine whether a direct sale is to an individual or a company. Moreover, as international standards like SSL and S/MIME proliferate, every desktop computer, laptop and hand-held device will contain strong encryption and therefore be subject to the reporting requirements. Reporting should be streamlined and focused on those products that are primarily platforms for secure communications, as opposed to consumer goods.

Our further comments are divided into two categories.

The first set of comments focuses on items of specific concern. These include (1) the classification of certain networking products as "retail", (2) the sales of non-retail networking products to governments, and (3) the need for decontrol of network management encryption products.

The second set of comments focuses on simplification and clarification of the encryption export controls in the areas of open source software and controls on technical assistance.

Items of Specific Concern

HP respectfully recommends that BXA consider the following comments in its administration of the new encryption export control policy and its formulation of additional regulatory relief in this area.

1. Scalable Software Firewall-VPN Products Should be Afforded "Retail" Status

Products that combine firewall and virtual private network ("VPN") capabilities are important components of critical infrastructure protection. Indeed, one might argue that the U.S. government should promote, rather than restrict, the widespread deployment of firewall-VPN products, because of their crucial role in Internet security.

HP recommends that scalable software firewall-VPN products should be considered eligible for retail status and thus not considered network infrastructure products. These products typically are licensed for a number of concurrent users that would qualify for "small-office home-office", as that term is understood in the context of Section 740.17(a)(3)(iii). The mere fact that software-only products may scale better than competing hardware products should not provide a basis for exclusion of such products from retail treatment. Failure to afford retail status to scalable software firewall-VPN products will distort the market, by forcing developers to integrate firewall-VPN capabilities with other products, like operating systems, in order to compete effectively.

2. License Exception ENC Should be Extended to Governments for Civil Uses

HP welcomes the new Section 742.15(b)(3), which states that favorable consideration may be given to applications for licenses to "civil uses" by governments. Our expectation is that applications to export to governments for civil uses will rarely be denied. However, the licensing delays for these kinds of applications have historically been substantial, with potentially disastrous consequences in the form of lost sales. We suggest that License Exception ENC should be extended to governments for civil uses described in Section 742.15(b)(3).

3. Network Management Encryption Products Should Be Decontrolled

Products that merely allow a system administrator to configure devices on a network and obtain status reports on network devices and activity, securely and remotely, should be decontrolled provided that they do not allow encryption or decryption of user traffic. The ability to manage devices on a network securely and remotely is fundamental to sound and cost-effective deployment of networking products and protection of the nation's critical infrastructure. Furthermore, provided that such products do not encrypt user traffic, such network management products should not frustrate known intelligence gathering operations or law enforcement activities. Finally, it is worth noting that the leading product in this market segment is Open SSH, which is an open source product eligible for export under License Exception TSU. For these reasons, among others, we believe that network management products such as intrusion detection systems should be exempt from control

Frank J. Ruggiero
May 12, 2000
Page: 3

3 of 3

under ECCN 5A/D002, and classified without a one-time review under ECCN 5A/D992, regardless of cryptographic strength.

Items of General Concern

HP believes that the following suggestions will increase simplicity and transparency in the encryption export control regime.

1. Executable Code for Open Source Should Receive Similar Status

Open source is eligible for export under License Exception TSU pursuant to Section 740.13 of the EAR, even if it includes open cryptographic interfaces. However, the EAR is silent on how executable code derived from open source is treated in the cases where it (a) includes, or (b) does not include, open cryptographic interfaces. We believe that executable code derived from open source should be eligible for export under License Exception TSU, regardless of whether it includes open cryptographic interfaces. The reason is that any person who downloads the open source may compile and execute it. Therefore, the compiled executable code should be afforded similar treatment.

2. Section 744.9 Technical Assistance Controls Should Be Removed

The controls on technical assistance under Section 744.9 of the EAR appear to have been subsumed under the "operation technical data" provisions of License Exception TSU as set forth in Section 740.13(a) of the EAR. Because they appear to serve no useful purpose, beyond that which is authorized for export under License Exception TSU, we believe that they should be removed.

3. Clarification of No Reporting on Transfer of Technology

License exception ENC should be clarified to indicate in section 740.17(g)(1) that transfers of encryption technology to foreign employees in the U.S. are exempted from the ENC reporting requirement.

Conclusion

Thank you for this opportunity to comment on the interim final rule Revisions to Encryption Items. Please call me if you have any questions regarding the issues presented in this letter.

Sincerely,

HEWLETT-PACKARD COMPANY



Frederick F. Mailman

Export Manager



RIDER BENNETT
EGAN & ARUNDEL

Michael J. McGuire
(612) 340-7978

mjm McGuire@riderlaw.com
www.riderlaw.com

May 13, 2000

Frank J. Ruggiero
Regulatory Policy Division
Bureau of Export Administration
Department of Commerce
14th Street and Pennsylvania Ave, N.W.
Room 2705
Washington, DC 20230

Re: Comment on § 740.17(a)(3) of the Interim Final Rules

Dear Mr. Ruggiero:

I submit this comment to the Interim Final Rule published on January 14, 2000, which amended the Export Administration Regulations ("EAR"). This comment relates to the new § 740.17(a)(3) which creates an exemption for retail products. I submit this comment on behalf of a client in the United States, which sells software in "brick and mortar" locations and via the Internet.

The creation of the new exemption for products that have been classified as retail is a significant step forward in the effort to simplify for merchants the task of complying with the EAR, which is becoming increasingly complex. My goal in submitting this comment is to persuade the BXA to go one step further and create a simple mechanism to help merchants determine which products have been reviewed and classified as retail under ECCNs 5A002 and 5D002.

Pursuant to § 740.17(a)(3) of the Interim final rule, a party (most likely the manufacturer) may initiate the review and classification of an encryption product by submitting a classification request. *See* § 740.17(e). The rule states that:

Thirty days after receipt of a complete classification request by BXA, unless otherwise notified by BXA, exporters may export and reexport to any non-government end-user any encryption product eligible under paragraphs (a)(2), (a)(4) and (a)(5) of this section. No exports to government end-users are allowed under this provision, and BXA reserves the right to suspend eligibility to export while a classification is pending.

§ 740.17(c).

It is unlikely that retailers will be involved in the license application process. Therefore, retailers will not receive notification from BXA that a product has or has not been classified as retail or that a product's eligibility for export has been suspended.

Given this lack of a reliable means to verify the status of particular products, it is likely that U.S. retailers may not take advantage of the new "retail exemption." This will, of course, hinder the implementation of the Administration's new encryption policy announced on September 16, 1999.

May 13, 2000
Page 2

One solution to this problem would be to create a BXA "Seal of Approval" that manufacturers would be required to apply to the packaging of software products the BXA has classified as retail. The seal could be similar to the European Community symbol that is placed on products that are approved for import into the EC or the Underwriters Laboratories seal that can be placed on products that have been tested by that organization. This seal could also be used in conjunction with Internet Web sites where the software is made available for download.

The seal would make it a very simple matter to identify products that have been approved for export. Not only would this be a benefit to merchants trying to identify products that are appropriate for sale, it would also benefit postal workers, shipping companies, or even customs agents who need to ascertain the export status of a product. Given that the purpose of a "retail" classification is to facilitate sales to the public, it is likely that such products increasingly will be transported via common carriers. The seal requirement would also be of important benefit to consumers, given that retail products will also be exempt from Internet download screening requirements in 734.2(b)(9)(iii). By requiring the use of a seal, end-users who download the software from a Web site would not be left in doubt about the export status of the product they were downloading.

Another solution to this problem would be to create an online database listing all encryption products that have been reviewed and classified by the BXA as retail under ECCNs 5A002 and 5D002. The BXA Web site demonstrates several ways in which the BXA has implemented similar systems to ease compliance with the EAR.

For example, the BXA SNAP system allows exporters to use the Internet to apply for licenses, to track license requests and to receive notifications of final action. This system could be modified to allow retailers who want to export products classified as retail to check the status of a particular product. The system could also send merchants electronic notifications if BXA suspends the exemption for a product. The SNAP system could track products using either the product's retail UPC code or by referencing the software title and version information. The SNAP database may need to be modified to require applicants to provide this data when the initial application is filed or to update the database as necessary if this data is not available at the time the application is filed.

Regardless of the means chosen to implement this system, the rules should also provide that retail merchants shall not be liable for a violation of the EAR if the merchant exported a product based upon information in the BXA database or upon the presence of the "Seal of Approval."

Without methods such as these, retailers will be forced to rely upon manufacturers or their distributor's representations about the classification of a product. The methods outlined above would provide retailers with a simple and accurate means to verify *for themselves* that the export of a product will not violate the EAR. Thus, the suggested procedure would promote compliance with the EAR.

I also feel it is important to discuss whether Section 12(c) of the Export Administration Act would affect either of the methods outlined above. I do not believe that it would for several reasons. First, section 12(c), by its language, applies only to "information obtained for the purpose of consideration of, or concerning, license applications." The solutions described above would not involve the disclosure of application information. To the contrary, the solutions would merely disclose the BXA's classification decision.

Second, any manufacturer that sells outside of the United States a product containing encryption features necessarily discloses that the product has been reviewed by the BXA and has been approved for export or that it otherwise qualifies for an exemption. Posting the classification of the product on the BXA Web site or requiring a merchant to label its product would not involve any further disclosure of information.

RIDER, BENNETT, EGAN & ARUNDEL, LLP

May 13, 2000
Page 3

Finally, even if the suggestions outlined above could be construed as involving a disclosure of application information, this disclosure would be consistent with section 12 (c). Although section 12 (c) of the EAA limits disclosures of application information, it also provides that application information may be disclosed if the Secretary determines that the disclosure of the information is in the national interest. Providing an objectively verifiable means of determining whether a product has been classified as retail will promote the Administration's encryption policy and will reduce the likelihood that software which has not been classified as retail might be exported mistakenly. This clearly promotes the national interest.

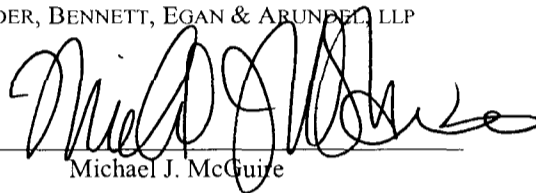
I strongly urge BXA to take amend the interim final rules as necessary to implement the systems described above or some other system that accomplishes the same goals. Doing so would remove the uncertainty and doubt that will likely limit the number of merchants that will take advantage of the retail classification created by the Interim final rules.

If you have questions, please feel free to contact me.

Very truly yours,

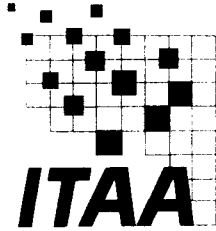
RIDER, BENNETT, EGAN & ARUNDEL, LLP

By



Michael J. McGuire

/jm
Enclosure



May 15, 2000

Frank J. Ruggiero
Regulatory Policy Division
Bureau of Export Administration
Department of Commerce
14th Street and Pennsylvania, Ave., NW
Room 2705
Washington, D.C. 20230

Via Hand

Dear Mr. Ruggiero:

On behalf of The Information Technology Association of America (ITAA) and our 400 direct and 26,000 affiliate corporate members throughout the U.S., and world-wide, we respectfully submit the following comments on Revisions to Encryption Items; Interim Final Rule, 15 CFR Parts 734, 740 et al.

Comments By ITAA on Revisions
to Encryption Items; Interim Final Rule

Summary.

ITAA recognizes and supports the substantial progress in reform and liberalization of export control mechanisms embodied in the "Revisions to Encryption Items; Interim Final Rule (the "Final Rule")". The Department of Commerce and other agencies involved are to be congratulated for undertaking reform on this important issue. The dynamic realities of high technology and markets compel all involved in this issue to cooperate to ensure the continued growth of unprecedented American prosperity.

ITAA believes, however, that additional progress remains. The Final Rule still imposes unnecessary complication and compliance burdens on industry. Industry daily strives to compete and to maintain American leadership in this important technology. As recognized in the Final Rule itself, the European Union's recent encryption export liberalization initiatives only underscore the

Information Technology Association of America

1616 N. Fort Myer Drive, Suite 1300, Arlington, Virginia 22209-3106 ■ Phone: (703) 522-5055 Fax: (703) 525-2279

need to further revise and streamline the U.S. regulatory framework to allow American industry to compete on a level playing field.

ITAA supports public comments by Under Secretary William Reinsch that the Department of Commerce recognizes the need to re-evaluate the Final Rule in light of developments in the European Union. ITAA and its member companies welcome an opportunity to collaborate in this re-evaluation to ensure that legitimate national security concerns are addressed while enhancing American competitiveness.

General Observations About The Final Rule.

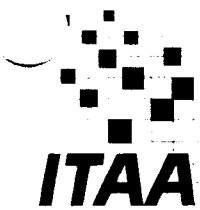
A. The Final Rule Demonstrates Change.

ITAA confirms that member companies have submitted products for technical review under the Final Regulations and have direct experience with the process. Reports from member companies indicate that the new framework represents improvement over past implementations.

Nonetheless, a reported trend is disturbing. ITAA notes that companies report, over time, that the requirements for technical reviews for products being submitted are growing much more complex, even when compared to reviews initiated earlier. For example, initially, technical review requirements may have required only the disclosure of the algorithm and key length. Now the process is become more baroque and burdensome. ITAA urges that the product review process under the Final Rule be one of notification rather than the previous regime of export approval.

A further issue that ITAA believes deserves clarification is the status of original equipment manufacturing ("OEM") collaboration under the Final Rule. Many of our members collaborate on a national and international basis regarding OEM arrangements. In many cases, under these arrangements, when an ITAA member has a product that has passed the review process on its own, that same product when embodied in the OEM product to other companies. Though a product has the ability to be shipped, once in an OEM product, that same product must be re-submitted for approval.

ITAA understands that there could be concern regarding alteration or changing of the product. But if the approved product is merely shipped overseas and then embedded by the OEM, ITAA believes that if a certificate or other formal declaration that the product has not been altered is tendered, the OEM product should not be re-submitted for re-examination. The Final Rule needs to reflect current realities of trans-national collaboration.



Finally, ITAA notes that the Final Rule still has twelve separate product categories, requiring a company to maintain rules, procedures and overhead for each one. This is again needlessly burdensome and a vestige of outmoded approaches. ITAA urges that consideration be given to a more streamlined and simplified approach to product classification that reflects current digital realities.

B. Deadline Issues.

ITAA considers the Final Rule to be an improvement regarding timeliness. A significant change is granting exporters the ability to export products 30 days after submission (unless advised otherwise) to non-government users, without receiving formal notification. The Final Rule also promises relief regarding the introduction of the retail classification. ITAA notes, however, that approvals for retail products, in some cases still require a reported sixty days or more. If these reports are accurate, ITAA notes that an avowed fundamental principle of the Final Rules – an alleged responsiveness to rapid technological and market evolution – is unfulfilled.

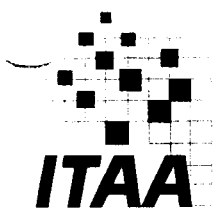
C. Reporting Requirements.

ITAA notes that it does not yet have significant feedback from member companies regarding the reporting requirements given the short amount of time between promulgation of the Final Rule in January 2000 and the date of these Comments. ITAA will continue to collect information on this subject and share it with appropriate agencies to ensure that the Final Rule in practice fulfills its promise.

Other specific concerns about the Final Rule's provision for reporting, however, are evident. Review of the Final Rule indicates that one interpretation is that exports to banks and financial institutions that are not subsidiaries of U.S.-based institutions have to be reported while previously they were exempted from reporting. If this is an accurate reading of the rules, ITAA requests that this provision be amended to provide relief for industry.

The Final Rule's requirements for reporting of any products classified as "retail" is needlessly burdensome and a vestige of outdated requirements. ITAA believes that there are no legitimate or compelling reasons for a company to provide reporting information for products classified as retail.

ITAA further commends the Final Rule for providing relief on some reporting by individual companies, provided that the company can demonstrate specific business reasons or alternative business models that differ from the requested reporting requirements. ITAA urges that such approved modifications of reporting be included in regulations for all companies and industry.



D. State-Owned Businesses.

ITAA members sell frequently foreign government and associated agencies. ITAA notes some minor inconsistencies between the previous regulations and the Final Rule. In general, ITAA believes that the effort should be pointed toward eliminating the need to differentiate between retail and non-retail products, i.e. prohibiting sales to the foreign governments under 'bulk' approvals (License Exceptions) for non-retail products. ITAA believes there is sufficient evidence of wide availability of cryptographic products, which seems to obviate the need for the current policy embodied in the Final Rule.

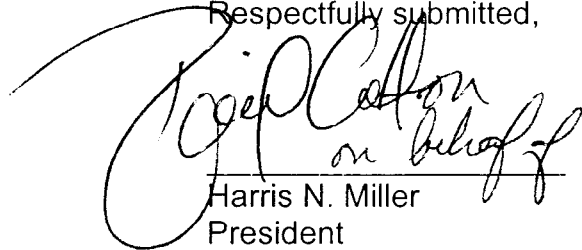
CONCLUSION

In summary, ITAA and its members support the important steps towards liberalization embodied in the Final Rule. The Final Rule represents substantial improvement over previously existing export control regulatory regimes.

Further work remains. Even absent an urgently needed response to the European Union initiative, additional effort now should be targeted toward greater simplification of the Final Rule. Implementation processes are still a matter of great concern and warrant careful scrutiny.

ITAA believes that the progress in the Final Rule holds out the promise of a solution without the need for congressional action. On behalf of its members, ITAA pledges to work constructively to explore all avenues to ensure that legitimate national security concerns are addressed while providing for the means of continued American technological leadership.

Respectfully submitted,



Harris N. Miller
President
ITAA
1616 N. Ft. Myer Drive
Suite 1300
Arlington, VA 22209-3106





Enc9
10 of 10

May 15, 2000

Mr. Frank J. Ruggiero
Regulatory Policy Division
Bureau of Export Administration
Department of Commerce
Room 2705
14th Street and Pennsylvania Avenue, NW
Washington, D.C. 20230

Re: Comments on January 14, 2000 Interim Final Rule on Encryption Items

Dear Mr. Ruggiero:

Americans for Computer Privacy (ACP) is pleased to offer these comments on the January 14, 2000 Interim Final Rule on Encryption Items, 64 Fed. Reg. 2492 (the "Regulations"). We wish to thank the Administration for issuing these Regulations, which dramatically revise U.S. encryption export control policy to permit U.S. companies to export strong encryption products worldwide. ACP appreciates the opportunity to comment on these Regulations, and we look forward to working with the Administration to refine and streamline them.

These Regulations represent a significant substantive improvement over the prior encryption export policy. For many products, the Regulations have permitted U.S. manufacturers to eliminate the costly practice of developing and supporting dual versions – one version with strong encryption for the domestic market and the other version with low encryption for export.

Nevertheless, ACP's member companies are still not allowed to compete on a truly level playing field against foreign competitors, particularly given the recently announced liberalization of the European Union's encryption export control rules. Needlessly complex and burdensome requirements still remain and continue to impose costs and delays that keep U.S. companies at a competitive disadvantage *vis-à-vis* foreign suppliers. Certain provisions favor particular business models over others. Moreover, ACP believes that there should be clear and enforceable guidelines to limit practices and interpretations that contravene the Regulations' spirit and language. Finally, ACP believes that there is sufficient foreign availability for cryptographic products to render

ineffective the restrictions remaining on widely-available commercial encryption products.

I. THE U.S. SHOULD MATCH THE EUROPEAN UNION'S RECENT RELAXATION OF ENCRYPTION EXPORT REGULATIONS BY TREATING EXPORTS TO THOSE COUNTRIES AS THE U.S. CURRENTLY TREATS EXPORTS TO CANADA

The U.S. should alter its Regulations to match the recent steps taken by the EU toward a significant relaxation of its encryption export rules. At the very least, the EU's bold steps should motivate the Administration to simplify and streamline its Regulations as much as possible.

We note that the EU's dramatic move comes in addition to the fact that there already are no reporting requirements for encryption exports within the EU. According to our information, the most significant elements of the EU's new rules are as follows:

- No export license or technical review is required for export within the EU.
- Companies can receive a general license for encryption exports to another 10 countries (including the U.S., Japan, Canada, Switzerland and several eastern European nations). Furthermore, for exports to these 10 countries:
 - no technical review is required;
 - there is no distinction between commercial and government purchasers; and
 - no technical review or license is required for open CAPIs.

These new rules are intended to assist EU companies to outstrip U.S. companies in encryption technology. As the EU's spokesman, Per Haugaard, stated regarding the new rules, "This is a big breakthrough and should help us build on our advantage over the United States in this field in order to become the world's leading supplier of encryption technology." BNA International Trade Reporter, May 4, 2000, at 693.

The Administration must act to ensure that U.S. companies are not at a competitive disadvantage *vis-a-vis* foreign companies. Indeed, the Regulations' Supplementary Information declares that, in the event of an EU liberalization of its encryption export regulations, the Administration will act to create a level playing field between U.S. and EU companies:

A number of companies have expressed concern that the European Union (EU) may implement a general authorization permitting encryption items to be exported freely within the EU and other specified countries. If and when the EU implements such an authorization, the Administration will take the necessary steps to ensure U.S. exporters are not disadvantaged.

65 Fed. Reg. 2494.

ACP believes that the broad territorial expanse of the EU's new liberalization lends itself to the Administration's extension of Canada-type treatment to the EU countries and to the eight other countries (leaving aside the U.S. and Canada) covered by the EU's new rules; such a policy removes complexity while facilitating U.S. companies' competition with their EU counterparts. We look forward to working with the Administration to prevent U.S. exporters from being disadvantaged by the EU's new policy.

II THE TECHNICAL REVIEW PROCESS SHOULD BE IMPROVED

While the Administration's January 14, 2000 policy announcement is a long stride toward fostering the competitiveness of U.S. companies, the Administration should ensure that the new Regulations are not frustrated "on the ground" by a lack of governmental resources or restrictive interpretations in implementing them.

A. Shorten Technical Reviews

The Administration should act to ensure that sufficient government resources and expertise are available to process the high volume of classification requests for encryption exports. ACP member companies have found that technical reviews are taking longer than the 30 days specified in Supplement 6 to Part 742. According to our member companies, the number of cases submitted has increased by 200% while the government has experienced personnel changes, including the transfer of licensing officers from the encryption area. The lack of government resources and expertise can, on a practical level, frustrate the Administration's policy decision to modernize U.S. encryption export regulations.

B. Prevent Restrictive Interpretations: The Case of Foreign-Produced Crypto Modules

The Administration should ensure that the Regulations are interpreted expansively, in accordance with their spirit. ACP's member companies report that the Administration has, on occasion, adopted restrictive interpretations of certain elements of the Regulations. For example, the Regulations are clear in not requiring review of foreign-produced cryptographic modules. See § 740.17(d). However, the Administration

continues to require the review and classification of all foreign-produced cryptographic modules that are designed to work with closed CAPIs and have been developed using U.S.-origin components. The Administration should remedy this restrictive interpretation of the Regulations regarding foreign-produced crypto modules and, in general, should act to make certain that the Regulations are interpreted in the spirit of their promulgation: leveling the playing field between U.S. and foreign companies.

C. Conduct Specification-Based Classification Reviews

The government should utilize where possible a generic, specification-based approach to one-time classification reviews. Currently, products that are based on the same overall encryption specification are individually subject to one-time reviews. For example, products built to the Bluetooth encryption specification for wireless IT products (1,800 companies have signed onto the Bluetooth standard, which uses a 128-bit Swedish algorithm that cannot be modified) each have to undergo product-by-product classification review.

Indeed, standard cryptographic protocols and algorithms are increasingly common in software products. For web security, the well-known SSL and TLS protocols using standard algorithms (128-bit RC2, 128-bit RC4, 56-bit DES, 3DES, and 1024-bit RSA) are widely used. For e-mail security, the S/MIME protocol – which uses the same set of standard algorithms – has become the industry standard. IPsec and Kerberos are other examples of cryptographic standards that are well understood and widely implemented in software products. There would seem to be little benefit from requiring time-consuming technical reviews of individual products that merely include these standard security implementations.

As a result, there should be a single one-time review involving the specification itself and the types of products/applications that would utilize that specification. The underlying encryption specification and its technical aspects provide sufficient information concerning a particular product's encryption capabilities, features, and technical constraints. This “spec-based” review could entail submission of the following:

1. technical descriptions of encryption design parameters that uniquely identify the design and adequately describe its functionality;
 2. the standard that is implemented (*e.g.*, Bluetooth 1.0);
 3. a description of both the electrical and programmatic interfaces;
 4. a list of the types of product applications likely to use this design;
- and

- 5. the kinds of sales channels through which products based on the specification would be sold, plus the extent to which the products would meet the definition of retail.

Providing the above information should meet the government's requirement for having technical data on encryption products that the government may confront in the field. Products built on an approved specification should therefore not have to undergo separate classification reviews. If an encryption product based on an approved specification is altered so as to exceed the outer parameters of the data provided in 1 through 5 above, it would of course become subject to a one-time review on its own merits.

D. Preventing Redundant Classification Reviews

Duplicative review is not necessary for items that have previously been classified as 'EI' items by the Administration but that clearly fall outside of EI-controls under the new Regulations. The grandfathering provision does not always clarify whether a company should pursue a second classification review. Accordingly, a new paragraph should be added to § 742.15(b) as follows:

Encryption commodities, software and technology up to and including 56-bits with an asymmetric key exchange algorithm not exceeding 512 bits that were reviewed and classified by BXA prior to January 14, 2000 under ECCNs 5A002, 5D002 or 5E002 may be classified and exported under ECCNs 5A992, 5D992 or 5E992, without further review by BXA.

III EI-CONTROLS ON SOURCE CODE, OPEN CAPIs, AND BROADLY AVAILABLE PRODUCTS SHOULD BE ELIMINATED

As the Administration recognized in its January 14, 2000 policy announcement, it is fruitless – if not counterproductive – to attempt to control the uncontrollable. The Administration should eliminate EI-controls from source code, open CAPIs, and encryption items that are widely available. At the very least, EI-controls should be eliminated from all “retail” encryption products.

A. End EI-Controls on Source Code and Open CAPIs

Now that the Regulations allow open or community crypto source code to be exported without a prior technical review, there should be no technical review of the executables of the same source code. The binary form of that source code should be decontrolled. Furthermore, the CAPIs contained in the source code should be decontrolled because anyone looking at the source code could write the modules that would plug into the open source code, listing the interfaces.

Indeed, releasing only “non-commercial” source code from EI-controls creates an unfair advantage to businesses that rely on an “open source” software development model over U.S. companies that rely on proprietary code. Even if object code software compiled from this released open source is not itself free from EI-controls (which is unclear in the Regulations), parallel independent compilation of common source code will certainly occur. Moreover, this exception, as written, would in effect release software containing open C APIs if the source code for those C APIs is available as open source. This seriously and specifically disadvantages those companies that have made the greatest effort to comply with U.S. export controls by developing products with closed C APIs because the review and licensing requirements still severely restrict the enabling of cryptographic code to work with those closed C APIs.

B. Reduce EI-Controls on Widely-Available Encryption Products

Even if EI-controls are not eliminated completely, the following steps should be taken to minimize the disruption caused by EI-controls.

1. Allow *De Minimis* Content for EI-Controlled Items

Because EI-controlled items currently are not eligible for *de minimis* exceptions, maintaining EI-controls on greater than 64-bit software and hardware encryption could make it impossible for U.S. manufacturers to supply their products to foreign manufacturers for incorporation into foreign products. If this exclusion is not removed, it will force some companies to continue to produce dual versions of products: one weak encryption version that can be free of EI-controls, and one strong encryption version. If this is the case, the cost savings and the ability to compete with foreign suppliers that were anticipated as a result of the new policy will not come to pass. Given the essentially unfettered exportability of retail encryption products, combined with the very broad exportability of the remaining non-retail products, the exclusion from *de minimis* treatment for EI-controlled items is outdated, unnecessary, and should be eliminated. Continuing the present policy of excluding EI-controlled items from *de minimis* treatment will only harm U.S. exporters without resulting in a security or other national benefit.

2. Extend the “Publicly Available” Exception to Software

The exclusion for EI-controlled software from the “publicly available” exception (§ 734.3(b)(3)) should be ended. Virtually all “publicly available” EI-controlled software would qualify as “retail” and is therefore exportable under the Regulations to virtually any end-user worldwide. Moreover, such software is normally distributed via free or anonymous Internet download and thus would be exempt from reporting requirements under the Regulations. Accordingly, it is reasonable to allow EI-controlled software to fall within the “publicly available” exception.

IV THE RETAIL EXCEPTION SHOULD BE IMPROVED

A. The Retail Classification Should Not Apply to Products Exported to the EU Plus Eight Countries

As we noted above, the EU has announced that it will no longer distinguish between commercial and government purchasers of encryption products. The difference between commercial and government purchasers is, in essence, equivalent to the dividing line in the Regulations between retail and non-retail. Accordingly, the retail classification should be eliminated for U.S. companies exporting to the same geographic area as covered by the EU's new rules, namely the EU countries plus eight others (leaving aside the U.S. and Canada). This will align the Regulations with the EU's new policy.

B. Modify the Current Retail Classification

The retail classification also should be modified in the following manner for those countries for which it is not eliminated.

a. Change the Retail Definition to a Mass-Market Definition

The retail definition should be changed to encompass mass-market sales, including high-volume sales, sales through normal yet non-retail commercial channels, and sales without substantial manufacturer support. This change is consonant with the Regulations' spirit, namely that the definition of retail is broader than sales to individual consumers. Indeed, even the substance of license exception ENC under § 740.17(a)(3) is broader than merely sales to individual consumers in that the license exception includes component devices and other items that are, in reality, mass-market. Accordingly, a mass-market definition is more appropriate for the substance of the retail classification and, on a practical level, would be less confusing for U.S. exporters.

b. Scalability Should Not Be a Proxy for Performance Restrictions

The government should assure the private sector that products that scale high, such as large web servers, will not be disqualified from retail classification only due to their large scalability. Scalable products that combine firewall and VPN capabilities in software should be considered retail and not classified as network infrastructure products. Otherwise, the government will be artificially forcing the market to move toward a model where these capabilities must be bundled into other products, such as operating systems. Indeed, the question of scalability is, in reality, not a question of encryption; rather, it is a question regarding the amalgamation of users and products and, ultimately, a question of a product's performance. Yet performance-based restrictions on the export of computers

are not the province of the encryption policy debate and thus not appropriate for inclusion in the Regulations.

V THE REPORTING REQUIREMENTS SHOULD BE CHANGED

A. Eliminate Reporting Requirements for Retail Products

As mentioned above, the EU has already eliminated reporting requirements for intra-EU exports and now is liberalizing its rules even further. The Administration should buttress U.S. companies' competitiveness by eliminating reporting requirements. Reporting is quite burdensome and costly for both mass-market software and hardware. Given that non-U.S. competitors – and especially EU companies – need not submit such reports, reporting requirements put U.S. companies at a competitive disadvantage.

Moreover, the Wassenaar Arrangement does not require reporting for any strong encryption exports. Prior to December 1998, the Wassenaar Arrangement included reporting requirements for the small segment of encryption products that did not meet the GSN definitions of mass-market or public domain. Yet in December 1998, encryption items were removed from the "Sensitive List", ending reporting requirements for even non-mass-market encryption products. In sum, the U.S. government agreed to eliminate all reporting requirements for our foreign competitors' encryption exports while maintaining burdensome reporting requirements for U.S. companies. The Administration should end reporting requirements in order to give U.S. companies a fair chance *vis-à-vis* foreign manufacturers of encryption products.

B. Streamline Reporting Requirements for Certain Products

Routine inventory commingling at companies can make it very difficult to distinguish between retail products sold directly to a consumer vs. a distributor/reseller. Retail sales to consumers, of course, are exempt from reporting, while sales to distributors/resellers are not. If inventory commingling prevents a company from distinguishing between the two, the logical compliance-related choice is to report on everything retail. Moreover, there does not appear to be any material benefit in retail reporting inasmuch as basic information on distributors/resellers and product quantities can be provided during the classification review itself.

Accordingly, the Regulations should clarify that reporting on retail products is not required when the exporter provides the following information in the course of the classification review process: (1) generic descriptions of retail channels and distributor/resellers applicable to an encryption product; and (2) a general indication of the quantities to be exported (e.g., thousands, tens of thousands, etc.).

The same principle should apply to KMI-eligible products, which, like retail items, can be shipped to government end-users.

It can also be very difficult, if not impossible, to provide non-proprietary technical descriptions for end-products using encryption components (e.g., mass-market chips). The Regulations should clarify that such reporting is not necessary where: (1) non-proprietary technical information is not readily available or collected in the ordinary course of business; or (2) the classification review process already takes account of generic descriptions of the kind of class of end-products in which the components are used.

Finally, the special reporting requirement for the sale of network infrastructure products to telecommunications and Internet service providers is burdensome and should be eliminated.

VI OTHER CLARIFICATIONS ARE NEEDED

A. Equivalent Treatment is Needed for Executable Code for Open or Community Source

Section 740.13 of the EAR permits export of open source – even including open cryptographic interfaces – under License Exception TSU. Yet the EAR does not specify treatment of executable code derived from open source when it either contains or does not contain open cryptographic interfaces. The Regulations should be clarified to allow export under License Exception TSU of executable code derived from open source even if open cryptographic interfaces are present. Indeed, the open source may be downloaded, compiled, and executed; accordingly, it seems reasonable that the compiled executable code should receive similar treatment.

The same argument is relevant to so-called "community" source eligible for export License Exception ENC pursuant to § 740.17(a)(5)(i) of the EAR. Given that the community source is eligible for License Exception ENC, the executable code should be eligible as well even if it contains an open cryptographic interface.

B. Permit Electronic Distribution of Non-Retail Software Products

The requirement to screen products posted on the web impedes the growth of companies' e-commerce business model. Currently, non-retail products can be posted on the web if accompanied by screening for government end-users. Specifically, § 734.2(b)(9)(iii)(A) allows reverse dns against .gov, .mil, and similar addresses. However, ACP's member companies lack an effective screening methodology, due in part to the complexity of making the "government" determination for any given end-user. In fact, most companies find that this determination is impracticable and thus, to be safe,

simply do not post any non-retail products on the web for electronic download. As many companies are currently trying to shift to a business model that makes use of electronic means of distribution, the Regulations impede this trend and should be changed to allow either less onerous screening requirements or to eliminate the screening requirement completely.

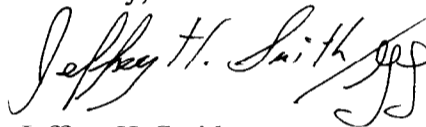
C. Technology Transfer

The Regulations should permit technology transfer not only to employees who are foreign nationals, but also to contractors and interns working for U.S. companies.

* * *

We appreciate the opportunity to comment on the new Regulations. The Administration's review of the Regulations is particularly timely in light of the EU's recent policy announcement, which has altered the status quo and tilted the playing field significantly. We look forward to working with the Administration to improve and streamline these Regulations and to create an equality of opportunity between U.S. companies and their international competitors in response to the EU's bold move.

Sincerely,



Jeffrey H. Smith

cc: Under Secretary of Commerce William Reinsch
Ms. Charlotte Knepper
Mr. Glenn Schlarman



May 15, 2000

Ms. Hillary Hess, Director
Regulatory Policy Division
Bureau of Export Administration
Department of Commerce
Room 2705
14th Street and Pennsylvania Avenue NW
Washington, D.C. 20230

VIA FAX: 202-482-3355

Re: Comments on January 14, 2000 Interim Final Rule on Encryption Items

Dear Ms. Hess:

Microsoft Corporation is pleased to offer these comments on the January 14, 2000 Interim Final Rule on Encryption Items (64 Fed. Reg. 2492).

These regulations represent a major substantive improvement over the prior regulations governing the export of items containing cryptographic capabilities. They have allowed Microsoft and other U.S. companies to finally compete for most of the customers worldwide that have been demanding products with strong encryption. For many products, the regulations have permitted manufacturers to eliminate the costly practice of developing and supporting dual versions – one with strong encryption for the domestic market and one with low encryption for export.

We are also very appreciative of the openness with which these regulations were drafted, and the ability of Microsoft and interested companies and organizations to respond to the discussion drafts that were made available throughout the process. The fact that the Interim Final Rule reflects many of the suggestions made during the drafting process makes it clear that the Administration took seriously the concerns that were raised.

Nevertheless, the regulations continue to present several serious problems for Microsoft and other U.S. companies. Despite the fact that almost all encryption items are exportable worldwide (except to the embargoed destinations), the regulations are still needlessly complex and contain burdensome requirements that impose costs and delays that keep U.S. companies at a competitive disadvantage vis-à-vis foreign suppliers.

Moreover, the current regulations contain several provisions that unfairly advantage certain business models over others. And in some cases, government practices and interpretations have been contrary to the spirit and language of the January 14 Rule.

These problems with the current regulations necessitate a thorough reexamination of the U.S. export rules with respect to encryption, with the goal of making the regulations simpler, less burdensome, and more equitable. The need for such changes are highlighted by the recent move by the European Union to create a license-free zone within the EU and 10 additional countries, which further highlights the need for a greater easing and simplification of the current U.S. export controls on encryption.¹

I. UNNECESSARY COMPLEXITY

The January 14, 2000 Interim Final Rule is far more complex than is necessary. The vast majority of all encryption products are now exportable to virtually any end-user worldwide. Millions of users worldwide have received strong encryption products in the months since the rule took effect. And as new versions of products containing strong encryption are globally released in the coming months, the worldwide ubiquity of strong encryption will be complete. There is no longer any justification for a complex regulatory regime that merely makes permissible exports far more difficult, confusing and costly than they need to be.

A clear example of the complexity of the rules is the large number of different categories of encryption items, each with its own set of rules. We have identified more than a dozen distinct categories (some with several subcategories): (1) authentication-only products; (2) mass-market products up to 64 bits; (3) non-mass-market products up to 56 bits, with key exchange up to 512 bits; (4) other cryptography products (over 64-bits for mass-market, or over 56-bits for non-mass-market) classified as "retail," which consists of any product that meets one of the criteria of 740.17(a)(3)(i) and all the criteria of 740.17(a)(3)(ii) – including general purpose operating systems and their associated user-interface client software or general purpose operating systems with embedded networking and server capabilities; non-programmable encryption chips and chips that are constrained by design for retail products; low-end routers, firewalls and networking or cable equipment designed for small office or home use; programmable database management systems and associated application servers; low-end servers and application-specific servers (including client-server applications, e.g., Secure Socket Layer (SSL)-based applications) that interface directly with the user; encryption products distributed without charge or through free or anonymous downloads; plus, finance-specific encryption items; non-mass-market products up to 56 bits, with key exchange greater than 512 and up to 1024 bits; any other encryption product that provides equivalent functionality to other products that have been classified as "retail"; (5) other cryptography products (over 64-bits for mass-market, or over 56-bits for non-mass-market) classified as "non-retail" – including network infrastructure products such as high end routers or switches designed for large volume communications; customized encryption products; encryption products that require substantial support for installation and use; products with encryption that is easily modified by the user; (6) key management products up to 512 bits; (7) key management products greater than 512 bits; (8) components (chips, toolkits) up to 56 bits; (9) components

¹ The European rule will reportedly permit the free export of cryptographic items within the license-free zone. For such exports there will be no technical reviews of products, no reporting requirements, and no restrictions on source code or open C APIs. When the current regulations were issued, it was anticipated that the EU may issue such a rule, and the commitment was made that "if and when the EU implements such an authorization, the Administration will take the necessary steps to ensure U.S. exporters are not disadvantaged." 65 Fed. Reg. 2494. The only way for the U.S. to meet this commitment to achieve equivalent treatment under the U.S. rules would be to extend the treatment currently available for encryption exports to Canada to include the EU and the 10 additional countries.

(chips, toolkits) greater than 56 bits; (10) general purpose toolkits; (11) publicly available, unrestricted source code; (12) publicly available, restricted source code; and (13) non-publicly available source code.

There are many other examples of complexity in the regulations. But the point is that since less than 5% of the encryption items currently available are subject to any meaningful controls, the regulations should be written to focus on those items. Everything else should be free of "EI-controls" and exportable under 5A992 or 5D992 (NLR) and the current rules applicable to those ECCNs.

II. ELIMINATION OR REDUCTION OF EI CONTROLS

One key to simplifying the regulations would be the elimination of EI-controls from encryption items that are generally exportable (at the very least, they should be eliminated from all "retail" and/or publicly available encryption items). EI-controls are a remnant of a very different policy that was in effect at the time encryption items were transferred from the State Department to the Commerce Department, and the ITAR-like restrictions were largely replicated in the EAR. These controls are entirely inappropriate and unnecessary under the current policy, especially when applied to products that are exportable worldwide.

The following steps should be taken either in conjunction with the elimination of EI-controls.

A. De Minimis Content

Because EI-controlled software currently is not eligible for de minimis exceptions, maintaining EI controls on greater than 64-bit software could make it impossible for U.S. manufacturers to supply their products to foreign manufacturers for incorporation into foreign products. If this exclusion is not removed, it will force some companies to continue to produce dual versions of products – one weak encryption version that can be free of EI-controls, and one strong encryption version. If this is the case, the cost savings and the ability to compete with foreign suppliers that were anticipated as a result of the new policy will not come to pass.

Moreover, since only EI-controlled items are ineligible for de minimis treatment, this creates an unfair advantage for companies that rely on "open source" software development over those with business models that rely on proprietary source. Foreign manufacturers will choose foreign supplies, or U.S. "open source" suppliers since their products are outside of EI controls and thus eligible for de minimis treatment. This discriminates against Microsoft and other U.S. companies with products based on proprietary code to give an artificial competitive advantage to "open source" suppliers. Export controls should not result in picking winners and losers among competitive U.S. products.

Given the essentially unfettered exportability of "retail" encryption products, and the very broad exportability of the remaining "non-retail" products, the exclusion from de minimis treatment for EI-controlled items is outdated, unfair and unnecessary. Thus, Section 734.4(b)(2) should be eliminated, and 734.4(h) should be amended to reflect that deletion. Or, at the very least, these paragraphs should be amended to apply only to products that are classified as "non-retail."

B. Publicly Available Software

Section 734.3(b)(3) – the exclusion for EI-controlled software from the “publicly available” exception – should be eliminated. Virtually all “publicly available” EI-controlled software would qualify as “retail” and is therefore exportable under the regulations to virtually any end-user worldwide. Moreover, such software is normally distributed via free or anonymous Internet download and thus would be exempt from reporting requirements under the draft regulations. So there seems to be little point in maintaining EI-controls and the exclusion from publicly available treatment for these products.

Additionally, under current interpretations of the regulations as stated in unpublished BXA advisory opinions, publicly available software compiled from “non-commercial” source code is released from EI controls, but publicly available software compiled from proprietary source code is not. But there is no rational basis for releasing one class of software while maintaining controls on another class, where the only difference between the two is the licensing model of the underlying source code. Such a distinction only gives an unfair advantage to companies that rely on an “open source” software development model over U.S. companies that rely on proprietary code (see the discussion of source code below). Thus, EI-controls should be eliminated from all publicly available software, regardless of the status of the underlying source code.

C. Published Software

Similarly, Section 734.7(c) – the exclusion for EI-controlled software from the “published information and software” rule – should be eliminated. This paragraph (c) was newly added by the January 14 Rule to make it clear that software controlled under ECCN 5D002 for “EI” reasons remains subject to the EAR even if it is “published” as defined in paragraphs (a) and (b) of that section (i.e. “available for general distribution either for free or at a price that does not exceed the cost of reproduction and distribution”). Paragraph (c) should be deleted and it should be made clear that “published” encryption software of any key length is not subject to the EAR.

D. Beta Test Software

Section 740.9(c)(3), relating to beta test software exportable under License Exception TMP, specifically excludes “encryption software controlled for EI reasons under ECCN 5D002.” Beta test software is distributed throughout the software development process, and subsequent versions of such software often need to be distributed quickly, before there is an opportunity to submit them for the technical reviews required for EI-controlled software to be exported under License Exception ENC. By the time a technical review is completed (or the 30-day period has run so that the software can be exported to non-governments), the test period for that version may be over or nearly over, with the next version of the software ready for distribution.

Of course, companies that rely on “open source” business models do not face this regulatory hurdle. Once again, certain U.S. companies are disadvantaged by the current regulations based solely on a difference among business models.

III. TREATMENT OF SOURCE CODE

The current export rules with respect to cryptographic source code are extremely complex and unclear. The regulations create three categories of source code, with a different set of rules for each. The current source code rules disadvantage U.S. companies vis-à-vis foreign competitors, plus they unfairly benefit certain U.S. companies at the expense of others.

Foreign companies do not face similar complex and restrictive rules. For example, under the European dual-use regulations, there is no distinction between “commercial” and “non-commercial” source code. Instead, any “publicly available” source code is outside the scope of the regulations and thus is freely exportable. Any other source code would, under the newly announced EU policy, be exportable at least within the EU and to 10 other countries without any formalities, and likely much more broadly with minimal requirements.

Releasing only “non-commercial” source code from “EI” controls creates an unfair advantage to businesses that rely on an “open source” software development model over U.S. companies that rely on proprietary code.² Even if object code software compiled from this released open source were not itself released from EI controls (which is unclear under the current regulations), parallel independent compilation of common source code will certainly occur.

Moreover, BXA has issued advisory opinions stating that publicly available object code compiled from “non-commercial” source code is also released from EI controls. Meanwhile, publicly available object code compiled from proprietary source code is still subject to EI controls. But whether or not licensing fees are collected for the use of source code has absolutely nothing to do with the controllability of the code or the software compiled from the code. This again demonstrates how the disparate treatment punishes U.S. companies with business models that include substantial investments in the development of their own intellectual property and desire to protect those investments.

The large disparity between the treatment of publicly available source code and that of proprietary code only creates a strong incentive for companies to release source code in order to achieve more favorable export treatment for their products. Currently, the rule penalizes companies that try to maintain some limitations on the dissemination and use of their cryptographic source code, which seems contrary to the intent of export controls on cryptography. It is hard to see how forcing the public release of cryptographic source code meets any U.S. national security or law enforcement interest.

Finally, this exception, as written, in effect releases software containing “open CAPIs” if the source code for those CAPIs is available as open source. This seriously and specifically disadvantages those companies that have made the greatest effort to comply with U.S. export controls by developing products with closed CAPIs, since the review and licensing requirements still severely restrict the enabling of cryptographic code to work with those closed CAPIs.³

² See also the discussion of how the rules governing source code create such disparities in the “de minimis,” “publicly available” and “beta test software” sections of Part II above.

³ See Part IV below for a discussion of how restrictive and unjustified interpretations of the current rules have also harmed U.S. companies that have developed closed CAPIs.

In order to remedy these disparities, all cryptographic source code should be released from EI controls. Or, at the very least, all publicly available source code (both commercial and non-commercial) should be released from EI-controls and made eligible for ECCN 5D992 / NLR.⁴ And if proprietary (non-publicly available) source code is not also released from EI-controls, it should at least be exportable in a way equivalent to how publicly available commercial source code currently is under Section 740.17(A)(5)(i) (i.e. exportable under a license exception without prior review, subject only to after-the-fact reporting).

IV. TREATMENT OF CLOSED CRYPTOGRAPHIC APIS (CAPIs)

Section 740.17(d) of the regulations states:

"Foreign products developed with or incorporating U.S.-origin encryption source code, components or toolkits remain subject to the EAR, but do not require review and classification by BXA and can be exported or reexported without further authorization."

The language of the regulations is very clear, and does not seem to be subject to any interpretation that would require the review of foreign produced cryptographic modules. In fact, the language excluding such products from review is not even limited to those items that would be classified as "retail" or those that are designed for non-government end-users. There is simply no requirement for the technical review of any foreign-produced cryptographic items.

Nevertheless, BXA continues to require the review and classification of all foreign produced cryptographic modules that are designed to work with closed CAPIs and have been developed using U.S.-origin components.⁵

⁴ We propose separately, in Part II above, that all publicly available software (object code) should also be released from EI controls, regardless of the status of the source code from which it is compiled.

⁵ Even the preamble to the regulations clearly states "foreign products developed from encryption components, while subject to the EAR, do not require review and classification prior to reexport." (page 2493, column 3 of the January 14, 2000 Federal Register).

Moreover, the communications from BXA (the agency that has the authority to interpret these regulations) are clear and consistent. BXA's "Questions and Answers" on the new regulations (<http://www.bxa.doc.gov/Encryption/qanda.htm>) contains the following:

9. Is there a review of the foreign product developed with U.S. encryption?

No, a review of the foreign product is not required, unless the encryption item was exported to a U.S. subsidiary.

The "Encryption Licensing Chart" (<http://www.bxa.doc.gov/Encryption/licchart.htm>) indicates for both "general purpose toolkits" and "encryption components / application specific toolkits" that a technical review is required for the toolkit itself, but makes it clear (in footnote 3) that there is "no review of foreign products."

Finally, the Commerce Department press release and fact sheet (<http://204.193.246.62/public.nsf/docs/60D6B47456BB389F852568640078B6C0>) states "foreign products developed using U.S.-origin source code or toolkits do not require a technical review."

It has been suggested that to exclude such foreign-produced modules from review would, in effect, make a closed CAPI an "open cryptographic interface." But that is not the case. "Open cryptographic interface" is defined in the regulations as:

"A mechanism which is designed to allow a customer or other party to insert cryptographic functionality without the intervention, help or assistance of the manufacturer or its agents, e.g., manufacturer's signing of cryptographic code or proprietary interfaces."

But regardless of whether the U.S. government reviews the cryptographic module, a closed CAPI is still a mechanism that requires the intervention of the manufacturer (e.g. digitally signing the code or a hash of the code).

So despite the fact that the January 14 regulations do not give the U.S. government the authority to review foreign developed cryptographic modules, BXA continues to require such review. While the language of the regulations is already clear on this issue, a further clarification is apparently necessary. Thus, section 740.17(d) of the regulations should be amended to state:

"Foreign products, including cryptographic modules designed to access closed or open CAPIs, developed with or incorporating U.S.-origin encryption source code, components or toolkits remain subject to the EAR, but do not require review and classification by BXA and can be exported or reexported without further authorization."

In the meantime, since there is no basis in the current regulations for requiring review of foreign produced cryptographic modules, BXA should immediately abandon this interpretation which contradicts the plain meaning of the regulations.

V. REPORTING REQUIREMENTS

The January 14, 2000 Interim Final Rule reduced in significant ways the reporting requirements on the export of encryption items. Nevertheless, the remaining reporting requirements are needlessly complex and burdensome, present difficult questions regarding actual practice, and do not appear to serve any government purpose.

The current rule states that:

- (2) Exporters must provide all available information as follows:
 - (i) For items exported to a distributor or other reseller, the name and address of the distributor or reseller and the quantity exported and, if collected in the normal course of business, the end-user's name and address;
 - (ii) For items exported through direct sale, the name and address of the recipient and the quantity exported (except for retail products if the end-user is an individual consumer)

There are several exceptions to these reporting requirements, but the sales that fall within these exceptions may be difficult if not impossible to differentiate. For example, there will frequently be no practical way for an exporter to determine whether a direct sale of a "retail" product is to an

“individual” or to a representative of a commercial entity or other organization. Thus, it is likely that most exporters will be forced to “over-report” their exports.

Reporting also appears to be unnecessary, given that it is hard to see where the value to government is.

The numerous exceptions (direct sales to individuals, anonymous or free downloads, retransfers by foreign distributors and resellers, etc.) will normally result in reported information that reflects a very small fraction of actual deployments. For example, a software company that uses overseas replicators and distributors could legitimately report an export of only one or two units, even where there are millions of foreign end-users.⁶

For products that are widely used, there does not seem to be any value to reporting specific end-users. For example, both the Netscape Navigator web browser and the Internet Explorer component of the Windows operating system have been distributed in quantities greater than the total number of Internet users – so it is safe to assume that virtually every user has both. But reporting will not reveal what software is actually being used by which user.

Similarly, many companies routinely purchase and use several competing products. For example, over 90% of the largest e-commerce companies run both Oracle and Microsoft SQL servers. The reporting, however, would not reveal how, and to what extent, each product is actually deployed. The reporting would tell the government that for any particular deployment, there would be either an Oracle server, a Microsoft SQL server, or both. But the same assumption could be made without any reporting whatsoever.

Furthermore, the vast majority of commercial products now use standard security protocols. So, it is unclear what is gained by the knowledge that Company X is using SSL for web security and S/MIME for secure e-mail, since virtually every company is using SSL for web security and S/MIME for secure e-mail.

Reporting is quite burdensome and costly, particularly for mass-market software exports. In the past, we have spent countless hours preparing semi-annual reports on encryption exports under individual export licenses. Under the new regulations, as many more exports are permitted, this burden will greatly increase. The burden and the cost of these reporting requirements will vary widely from company to company. For companies that sell lower volume / higher price items, it may be easier to comply with these reporting requirements - albeit at a substantial administrative cost. But for a mass market software company that relies on high volume and lower prices per product, there will be a huge amount of data to compile, and a lower margin per transaction to absorb the cost. Given that non-U.S. competitors do not need to make such reports, this requirement creates a substantial administrative cost that our foreign competitors do not bear, putting us at an automatic competitive disadvantage.

Moreover, the Wassenaar Arrangement – a multilateral export control regime based on national discretion licensing by each member country – does not require reporting for any strong

⁶ This example reveals why reporting requirements are especially inappropriate for software. In contrast to hardware, a customer can easily make an unlimited number of perfect copies of a software product. And licensing agreements for mass market software products frequently allow customers to do just that. Moreover, software can be easily distributed and redistributed over the Internet - not so with hardware.

encryption exports. Prior to December 1998, the Wassenaar Arrangement *did* include reporting requirements for the very small class of encryption products that did not meet the GSN definitions of mass-market or public domain. In December 1998, however, encryption items were removed from the "Sensitive List", thereby removing reporting requirements for even non-mass-market encryption products.⁷ It is particularly troubling that the U.S. Government agreed to eliminate all requirements for our foreign competitors to report exports of any encryption products, while maintaining burdensome reporting requirements on U.S. companies.

In sum, the reports that are required under the current regulations provide BXA with virtually no useful information about what, how, and the extent to which strong encryption software is actually being used around the world. Some basic assumptions, based on publicly available market data, can reveal nearly as much useful data to the government – without requiring US exporters to compile detailed reports.

These reporting requirements are needlessly burdensome for all U.S. exporters. They are a unilateral requirement of the United States which create significant disadvantages for U.S. exporters, and they provide the U.S. government with few if any benefits. We strongly urge that, at least for permitted exports of mass market or "retail" encryption software, regardless of key length, all reporting requirements be eliminated.

CONCLUSION

In a world where strong encryption is now freely available worldwide, and U.S. policy as reflected in the current regulations acknowledges and contributes to such availability, it is difficult to find any justification for the complexity of the regulations or the burdensome requirements that U.S. exporters must navigate merely to accomplish a permissible export. Rather than allowing U.S. exporters to freely compete in the global market for products containing encryption capabilities, the regulations add costs and delays to U.S. exports and create artificial advantages for certain business models over others.

We strongly urge the Administration to not only remedy the specific problems raised in these comments, but to also reexamine whether and to what extent the remaining controls and requirements make sense given the current broad exportability and worldwide availability of strong encryption.

Respectfully Submitted,



Michael Hintze
Corporate Attorney

⁷ The Arrangement imposes reporting requirements on exports from members countries of items on the so-called "Sensitive List" and "Very Sensitive List" of Annexes 1 and 2 to the Wassenaar list of controlled items. Reporting of exports of such items allows other Wassenaar members to know which of these items are exported to what countries, and allows members to monitor build up of sensitive items and to try to persuade other members not to export certain items to certain end-users. It provides the only useful enforcement mechanism of the Wassenaar Arrangement.



5/15/2000

Kirsten Mortimer
Regulatory Policy Division
Bureau of Export Administration
Department of Commerce
P.O. Box 373
Washington, DC 20044

Dear Ms. Mortimer:

Thank you for the opportunity to comment on the January 14, 2000 encryption regulation (F.R. Vol. 65, No. 10, pp. 2492-2502). I am submitting these comments on behalf of my company, iLink Global, which provides export consulting services to companies in the United States and abroad, including a number of software developers who incorporate encryption in their products.

Screening Downloads of "Retail" Encryption Software

Certain clarifications to §734.2 of the regulation would help the exporting community in their compliance efforts. As currently written, encryption source code eligible for export under §§ 740.13(e) and 740.17(a)(5)(i) are not "exported" when posted on the internet, or otherwise made available electronically. As a result, an exporter has a duty to check for "red flags" when allowing the download of this source code, but is not required to establish an access control system as described in §734.2(b)(9)(iii). The access control provision specifically states that it applies to encryption items eligible for export under §§ 740.17(a)(2), (a)(5)(ii), and (a)(5)(iii). Encryption items eligible for export under §740.17(a)(3) (so-called "retail" encryption products) are neither excluded from the definition of export (when made available electronically) nor are they included in the access control requirement. This causes confusion for companies who wish to make their software available on the Internet, because they are unsure of what the regulation requires in regard to screening. I suggest that BXA clarify this point, either in the final regulation, or on the BXA website, by advising companies of their screening requirement for "retail" encryption software made available for downloading on the Internet.

Access Control Systems

Section 734.2(b)(iii) requires exporters to establish an access control system to screen for foreign government end users. The regulation describes an access control

system that “checks the address of every system outside of the U.S. or Canada requesting or receiving a transfer and verifies such systems do not have a domain name or Internet address of a foreign government end-user (e.g., “.gov,” “.gouv,” “.mil” or similar addresses).” However, actual Internet domain names for government end-users do not follow simple and straightforward rules, and do not clearly identify the organization’s affiliation. For example, one of the Indian military’s domain names is “armedforces.nic.in.” This domain name does not include the terms “mil” or “gov” but suggests that internet screening mechanisms must look for terms that imply government or military affiliation, thus falling into the “similar addresses” language of the current regulation. It is not clear, however, how far an exporter is required to go with this line of reasoning. For instance, the term “mod” may stand for Ministry of Defense, or it may simply be embedded in the domain name of a commercial entity. The following list of domain names and their affiliations shows how difficult Internet download screening for military entities can be:

Domain Name	Affiliation
www.idf.il	Israeli Defense Forces official site
www.mnd.go.kr	Ministry of National Defense, South Korea
www.mta.ro	Military Technical Academy of Romania
www.mod.gr	Ministry of Defense, Greece
www.mod.uk	Ministry of Defense, United Kingdom
ncb.intnet.mu/pmo/dha.htm	Ministry of Defense and Home Affairs, Mauritius

None of these domain names includes any of the suggested screening terms in the current regulation. A screen should probably catch the two domain names that include “mod”. But it’s difficult to see how any screen would catch the others. If screening for government end users is truly a concern for the United States Government, then BXA should provide additional guidance to exporters on screening mechanisms, either in the final regulation or on its web site. On the other hand, if the United States Government believes that exporters cannot effectively screen for government end users, due to the lack of uniformity in domain names for these end-users, then I believe the screening requirement should be removed, because they do not further the purpose of the controls.

Status of Source Code Exported under License Exception TSU

The encryption regulation, as written, makes it unclear whether or not certain source code is subject to the EAR. Sections 734.7, 734.8, and 734.9 are clear in stating that their provisions do not apply to encryption software controlled for “EI” reasons under ECCN 5D002. In addition, they refer to §740.13(e) for release under License Exception TSU. However, this provision says that certain encryption source code “is released from “EI” controls and may be exported or reexported without review under License Exception TSU, provided [the exporter has] submitted written notification to BXA of the Internet location...”. If the source code is no longer controlled for “EI” reasons, as it states in the license exception, then it is not clear why the source code would be subject to the EAR at all, since the exclusion from the publicly available provisions in Part 734 only applies to software controlled for “EI” reasons.

Publicly available source code that is not controlled for “EI” reasons is not subject to the EAR, while publicly available source code that is controlled for “EI” reasons is subject to the EAR. Under the current construction of the regulation, however, publicly available encryption source code (without an express agreement for payment of a fee or royalty) is not controlled for “EI” reasons, yet remains subject to the EAR and is exportable under License Exception TSU. This situation is not consistent with the typical treatment of publicly available source code under the EAR, and makes encryption export controls, which are difficult to understand as it is, even more convoluted.

Reporting under License Exception ENC

The reporting provision of License Exception ENC, §740.17(g)(2), says that reporting is required for exports, but does not say that reporting is also required for reexports. The exporting community believes that this is intentional, and that the U.S. Government does not require reporting for reexports made using License Exception ENC. However, §740.17(g)(5) states “for exports **and reexports** to Internet and telecommunications service providers of network infrastructure products...reports are due by the time of export” [emphasis mine]. This statement is ambiguous as to whether it creates a reporting requirement for reexports in and of itself, or modifies a reporting requirement stated elsewhere. If it is a requirement that is not stated elsewhere, then it should be in its own paragraph immediately after §740.17(g)(3), and not embedded in a paragraph that is devoted to the time and method for reporting, as is currently the case. In addition, the final regulation should clarify when reporting of reexports is required under License Exception ENC, and when it is not.

Foreign Finished Products

Section 740.17(d) says that “Foreign products developed with or incorporating U.S.-origin encryption source code, components or toolkits remain subject to the EAR, but do not require review and classification by BXA and can be exported or reexported without further authorization.” Because the term “exported” is used, this provision would appear to create a situation in which a foreign product made with U.S.-origin source code, components or toolkits could be imported into the United States, and then further exported from the United States without an authorization. Such a circumstance would not apply to encryption items made in the United States or foreign products not made with U.S.-origin encryption and imported into the United States. This was probably an unintended effect of this provision.

Thirty-day Provision

Section 740.17(e) says that “thirty days after receipt of a complete classification request by BXA, unless otherwise notified by BXA, exporters may export and reexport to any non-government end-user any encryption product eligible under paragraphs (a)(2), (a)(4) and (a)(5) of this section.” BXA has advised exporters that this period begins on the date the classification request is registered into the BXA computer system (ECASS).

The only way for an exporter to know this date is through STELLA, which indicates the date on which the application was pending in a particular licensing division. However, if the classification request is reassigned to another licensing officer in the same division (which commonly occurs) STELLA indicates a new, and later, date. As a result, it is difficult for the exporter to know when the thirty-day period begins. I believe that the thirty-day period should begin on the date BXA receives the application, as evidenced by a signed courier receipt. If BXA continues to advise that this period begins when the application is registered into ECASS, then BXA should formalize a process for informing applicants of when this takes place. It is extremely important that this issue be clarified in some way, because exporters often want to use the authority to export under License Exception ENC on the earliest possible date, but also want to make sure they remain in compliance with the regulation.

Grand fathering

The regulation grand fathers into all provisions of the new License Exception ENC [except (a)(3)] products that were approved for export under the previous License Exception ENC. Yet it does not specifically state that 56-bit products with a key modulus of 512 bits or below, which were also previously made eligible for ENC, are grand fathered into ECCN 5A992 or 5D992. The final regulation should make clear whether or not BXA has grand fathered these 56-bit products.

Licensing Policy for 5A992 and 5D992 items

Section 742.15(b)(1) says the following:

Certain encryption commodities, software and technology may, after classification by BXA as ECCNs 5A992, 5D992 or 5E992, be released from "EI" or "NS" controls. Items controlled under these ECCNs are eligible for export and reexport to all destinations except Cuba, Iran, Iraq, Libya, North Korea, Sudan, or Syria.

This statement contradicts the Commerce Control List, which includes subparagraphs under these ECCNs that have an AT column 2 control. According to the country chart, these items may be exported to Syria without a license. Also, the word "or" between "EI" and "NS" should be "and," since items controlled under these ECCNs are not controlled for either EI or NS reasons.

Definition of Government End User

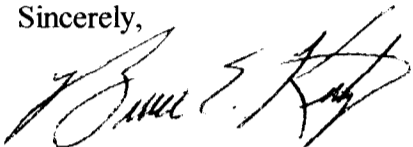
The definition of government end-user in Part 772 is unclear in regard to whether it covers certain partially- or wholly-owned government corporations. The phrase "performing governmental functions" is ambiguous, and it is not clear from whose perspective a particular activity is or is not a governmental function. For example, mail delivery in France is performed by the French PTT, and would certainly be considered a governmental function in France. However, mail delivery has been privatized in Germany, and may be performed by any entity, including private companies, licensed by the German government. Under the German Postal Act, such entities will be licensed,

unless they are determined to be unfit to perform mail delivery services. Thus, it would appear that mail delivery in Germany is not a governmental function under the law. Currently, the Deutsche Post delivers most of the mail in Germany, is a stock company whose shares are owned by the German government, and is planning an initial public offering for later this year. Given these facts, it is unclear whether the Deutsche Post meets the definition of government end-user in Part 772.

The phrase "governmental corporations or their separate business units... which are engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List" is also ambiguous. Does the clause beginning with "which are engaged" modify both "government corporations" and "separate business units" or just the latter? This should be clarified.

Again, thank you for the opportunity to comment on the regulation and for considering these comments in developing final regulations. Please do not hesitate to contact me at the number listed below if you have any questions about these comments.

Sincerely,



Bruce E. Kutz
Manager, Regulatory Affairs
iLink Global
10604 Tenbrook Drive
Silver Spring, MD 20901
(301) 681-7972

ENC 12
10f7



May 15, 2000

Frank J. Ruggiero
Regulatory Policy Division
Bureau of Export Administration
Department of Commerce
14 Street and Pennsylvania Ave., N.W.
Room 2705
Washington, DC 20230

Re: Comments on Interim Final Rule on Revisions to Encryption Items (65
Fed. Reg. 2492; Jan. 14, 2000)

Dear Mr. Ruggiero:

The Semiconductor Industry Association ("SIA") is submitting the following comments regarding the Commerce Department's January 2000 interim final rule on encryption exports. While the rule presents a host of important issues, SIA has limited its comments primarily to those issues with the greatest relevance to semiconductors.

SIA is the leading trade association representing the U.S. semiconductor industry and its members comprise 90 percent of U.S.-based semiconductor production.

Summary

The interim final rule represents an important and overdue change in the U.S. government's treatment of encryption exports. Foreign production and sale of robust encryption continues unabated and no level of U.S. controls will impede foreign access to the most powerful commercial encryption products. In these circumstances, the new rules properly permit license-free exports of unlimited strength encryption to all non-terrorist nations. This approach, implemented through license exception ENC, removes a significant burden on the ability of U.S. companies to compete in the growing area of electronic privacy and security.

At the same time, most U.S. encryption commodities, software and technology remain subject to special encryption controls and face a variety of requirements and restrictions both before and after an export sale. License exception ENC, the heart of this reform effort, requires further improvement. Changes are needed to the provision's "retail" approach, the classification review process, the treatment of open cryptographic interfaces, and reporting requirements.

Separately, restrictive EI controls - those controls specific to encryption items - should no longer apply to products that receive global, license-free treatment under the new rules. In addition, a de minimis standard should be made available for all encryption items. Restrictions on encryption should not be extended beyond hardware, software and technical data, i.e. not to technical assistance. The control status of encryption technology should always correspond to the status of the underlying commodity or software. Lastly, the United States must act swiftly to address pending policy changes by the European Union (EU) that would place U.S. exporters of encryption at a clear competitive disadvantage.

Overall, the interim rule serves to bring U.S. export control policy more in line with the realities of the information age and global markets. SIA agrees with the general direction of the January rule changes, but suggests that the Administration further refine these rules and ensure that U.S. companies competing in the global market for encryption are not needlessly disadvantaged.

License Exception ENC

License exception ENC is the primary means by which this rule's reforms are implemented. It provides a regulatory framework for permitting the license-free export of unlimited strength encryption worldwide. Several specific changes are needed to ensure that ENC functions appropriately and is responsive to technological and market realities.

Mass Market Benchmark - The greatest liberalization under ENC is reserved for items categorized as "retail". By definition, this category includes not only items sold through retail outlets, but also high volume items sold, without restriction, by mail, e-commerce, or telephone, such as encryption chips. SIA believes "retail" is an inadequate and misleading characterization for encryption commodities and software eligible for license exception ENC under § 740.17(a)(3). This section should be reconstituted as a "mass market" provision, thereby encompassing those items that are sold - whether to consumers or intermediaries - in high volume through normal commercial channels and without substantial manufacturer support.

The current ENC retail formulation essentially achieves this result, but with needless confusion. Despite the substance of the provision, the retail label perpetuates the faulty notion that only items sold to individual consumers are unworthy of control. The drafters of the regulation fully recognized that this is not the case, thereby including components, devices and other ostensibly non-retail items that are mass market in nature. The ultimate test under § 740.17(a)(3) must be whether an item is unsusceptible and unworthy of controls, regardless of means of distribution. Mass market serves as the correct standard.

Beyond just changing a label, replacing retail with mass market would bring greater clarity and logic to the ENC provision and make the provision more understandable for exporters.

Specification-Based One-Time Reviews - SIA believes the new rules should provide the opportunity for an encryption item to forego the one-time classification review if the item's underlying encryption specification has already been reviewed and authorized for export. This would avoid subjecting to one-time reviews thousands of items that, while differing in product type and use, offer essentially the same cryptographic functionality and performance.

By relying on a prior technical review of the underlying encryption specification (e.g., the Bluetooth standard), the government would have a sufficient indicator of an individual item's encryption capabilities and attributes. This is possible because most hardware products running on a particular encryption specification will have inherent technical constraints. This can be due, for example, to necessary electrical and programmatic interfaces that can limit an end-item's cryptographic functionality.

Therefore, SIA proposes that a one-time review of encryption specifications be instituted and that end-items utilizing an approved specification be authorized for export under ENC based on the underlying specification's review. It would not be necessary to submit these individual products to separate one-time reviews.

Under this arrangement, the government could maintain information about the types of items being shipped under this approach by requiring certain information during the initial review of the underlying specification. This information should include:

1. technical descriptions of encryption hardware design parameters that uniquely identify the design and describe its functionality;
2. the relevant encryption standard;
3. a description of the electrical and programmatic interfaces;
4. likely types of product applications; and
5. likely sales channels and customer types.

Such an analysis would capture the type of information and descriptions that would otherwise be gathered during individual product reviews. This would also be sufficient for determining up-front an item's retail, or more appropriately "mass market", status. Individual product reviews would be required only to the extent that an item's technical or marketing parameters varied from those laid out in the original specification review. Lastly, export reporting would be unnecessary for items shipped under a specification-based review to the extent that the original review provided representative sales and marketing data.

Specification-based reviews would offer the same basic information and market intelligence that the government would garner under a pure item-by-item review process. It would, however, cut out significant and unnecessary work on the part of both government and industry without jeopardizing the principle of the existing one-time technical review.

Open Cryptographic Interfaces - With the exception of exports to foreign subsidiaries, encryption items providing open cryptographic interfaces are entirely excluded from eligibility under all provisions of ENC. By definition, an open cryptographic interface implements no fixed set of algorithms or key attributes and permits a user to insert cryptographic functionality into an item. The regulations hold that such a mechanism is without discernable bounds and must therefore be licensed.

The problem with such an approach is that the means for creating and utilizing open cryptographic interfaces are already freely accessible. Public source code capable of implementing these open mechanisms is exportable license-free under license exception TSU, as are publicly available products compiled from such source code. In addition, open cryptographic interfaces are readily available from non-U.S. sources. It is therefore of little value to the government but potentially a large cost to U.S. companies to summarily exclude open cryptographic interfaces from ENC treatment. This exclusion should therefore be removed from the regulations.

Reporting - While retail encryption items exported to individual consumers do not have to be reported, other items qualifying as retail remain subject to ENC semiannual reporting requirements. These requirements apply to items such as mass market parts and components, including "retail" semiconductors which are exported to thousands of OEMs, distributors, and other intermediaries. Under the current rules, for example, U.S. semiconductor exporters must provide a range of data on potentially thousands of sales, including customer identities, quantities, and technical descriptions of end-products incorporating their devices.

There is no value or justification to requiring export reporting of such mass-produced items. As a rule, by virtue of qualifying under the retail provision, an item should be exempt from any reporting requirements. Information as to customer-type, probable sales quantities, and the like can be provided up-front during the one-time technical review.

For encryption components that are not classified as retail (as well as for retail components to the extent that they remain subject to reporting), the rules should state with greater clarity the extent to which reporting on components can be adjusted or reduced by providing relevant information during the one-time review. As an initial step, the current reference to the potential for reduced reporting for components should be moved from the interim rule's preamble into the body of the regulations.

One of the more onerous reporting requirements for components is the need to provide non-proprietary technical descriptions of the products incorporating such items. A new provision on the availability of reduced reporting for components should state that such technical descriptions are not required when: (1) such information is not readily available or collected in the ordinary course of business, or (2) generic descriptions of the likely

type of class of end-product that will incorporate such a component are provided during the one-time review.

No Duplicative Reviews for 56-bit Items - A new paragraph should be added to § 742.15(b) of the regulations as follows:

Encryption commodities, software and technology up to and including 56-bits with an asymmetric key exchange algorithm not exceeding 512 bits that were reviewed and classified by BXA prior to January 14, 2000 under ECCNs 5A002, 5D002 or 5E002 may be classified and exported under ECCNs 5A992, 5D992 or 5E992, without further review by BXA.

This change makes clear that duplicative technical reviews are not necessary for items that have previously been classified as EI items by the Commerce Department but that clearly now fall outside of EI controls under the new regulations. The interim final regulations are ambiguous on this point.

EI Controls

EI controls are the primary means within the Export Administration Regulations (EAR) for controlling the export of encryption items. These controls are specific to encryption items and impose added controls and restrictions on such products. These restrictions include ineligibility for the de minimis, public availability and foreign availability rules within the EAR.

Removal for retail items. To the extent that an encryption item is classified as retail, or more properly mass market, that item and related re-exports should no longer be subject to restrictive EI controls. Products classified as retail receive nearly unlimited exportability. To nevertheless maintain EI controls on these items is unreasonable and makes little sense. The types of restrictions and requirements under EI controls should be lifted concurrent with the broad licensing exemption granted under a retail determination.

De minimis treatment for EI items. To the extent that encryption items remain under EI controls, these items should be made eligible for de minimis treatment. The de minimis rule essentially holds that a controlled component item can comprise such a small or negligible percentage of an overall end product that the end product does not merit controls. This principle should hold regardless of the type of item or the reason for its control. In effect, de minimis content is immaterial in all cases. Continuing the present policy of excluding EI items from de minimis treatment will only harm U.S. exporters of component parts and systems, without resulting in a security or other national benefit.

Treatment of Technical Assistance and Technology

Technical Assistance. Controls on encryption items should be restricted to commodities, software and technical data. This is in line with the fundamental approach of the EAR. There is no demonstrated need for the existing encryption-specific prohibition on the provision of technical assistance to foreign persons (EAR § 744.9). This expansion of control authority is confusing and redundant and should be removed from the regulations. Controlling the export of commodities, software and technical data is fully adequate for covering encryption products and technology.

Technology. With respect to encryption technology, the level of control, as well as eligibility under license exceptions, should always directly correspond to that of the underlying encryption commodity or software. In other words, if particular encryption hardware or software is controlled only for anti-terrorism reasons under 5A992 or 5D992, then the related technology should be controlled to exactly the same extent (under 5E992) with no additional restrictions. Similarly, if an encryption item receives eligibility under license exception ENC, related technology should receive precisely the same license exception treatment.

Such a classification policy is logical, sensible and should already be in place under the EAR. Unfortunately, in practice this approach does not always appear to be followed by regulators. It is of particular concern that technology related to essentially decontrolled encryption items (those classified as 5A992 and 5D992) continues to be controlled at times as an EI item, thereby incurring license requirements and other restrictions above and beyond those applicable to the underlying commodity. The regulations should explicitly and clearly state that the export status of encryption technology always derives from the status of the underlying commodity or software.

EU Encryption Policy

The interim rule anticipated the recent move by the EU to permit license-free, review-free encryption exports to EU and 10 other major markets. This policy change would in effect create an encryption "free-zone" for EU exporters. They would be free to ship practically any encryption product without authorizations or reviews of any kind. The countries involved in the yet-to-be announced EU rule would collectively comprise the vast majority of the global encryption market.

U.S. suppliers of encryption stand to be significantly disadvantaged by this disparity between EU and U.S. policies. Despite broad new licensing exemptions under ENC, U.S. exporters would continue to face mandatory one-time technical reviews, a variety of EI-based restrictions, including continued U.S. regulation of re-exports, and certain other requirements which provide nothing approaching a "free-zone" for U.S. suppliers. U.S. makers of component items, such as semiconductors, are particularly at risk given the likelihood that foreign OEMs would quickly shift to more reliable and timely non-U.S. suppliers.

As a result, the U.S. government should expeditiously meet the commitment it made in the interim rule to "take the necessary steps to ensure U.S. exporters are not disadvantaged" by the new EU policy. This would require treatment similar to that now available within the EU. Unlimited strength U.S. encryption products should be made freely exportable, without reviews or any other requirements or restrictions, to the "EU-plus 10" countries on the same basis that sales to Canada currently enjoy. The U.S. gains nothing by maintaining a stricter encryption policy than the EU or any other major encryption supplier. The only notable result will be loss of business and market leadership for U.S. companies. The U.S. government has stated it will remedy this issue and SIA urges it to act quickly.

* * * *

SIA appreciates the opportunity to submit these comments and would be happy to elaborate on any of its suggestions. Please feel free to contact me or SIA counsel W. Clark McFadden II.

Sincerely,

David Rose
wcm

David Rose
Chairman
SIA Export Controls Committee

ENC 13

1212 Avenue of the Americas, New York, NY 10036-1689
tel: 212-354-4480 - fax: 212-575-0327
e-mail: info@uscib.org - Internet: www.uscib.org

Serving American Business as U.S. affiliate of:

International Chamber of Commerce (ICC)
International Organisation of Employers (IOE)
Business and Industry Advisory Committee (BIAC) to the OECD
ATA Carnet System



United States Council for International Business

May 15, 2000

Mr. Frank J. Ruggiero
Regulatory Policy Division
Bureau of Export Administration
Department of Commerce
14th Street and Pennsylvania Avenue, N.W.
Room 2705
Washington, D.C. 20230

Dear Mr. Ruggiero:

The United States Council for International Business (USCIB)¹ appreciates the opportunity to comment on the Interim Rule, Encryption Regulations published on January 14, 2000. The USCIB is encouraged by the trend toward a more liberal policy for the export of encryption technologies. The access to robust cryptography to ensure the security of business information and information that relates to a business' customers is essential to the continued growth of electronic commerce and its resulting benefits to society and the global economy.

As expressed in previous submissions, USCIB members believe that the marketplace should define the types and strengths of encryption technologies that users access; business and end-users should be able to choose the cryptographic systems and products that best suit their needs. The Interim Rule is a significant step forward in achieving that objective.

However, USCIB members would like to address several outstanding issues in the Interim Rule that may put U.S. companies at a competitive disadvantage vis-à-vis their foreign counterparts. Most notably, the costs that businesses will incur to comply with the often complex procedures set forth in the Interim Rule will decrease the competitiveness of U.S. suppliers.

More specific are set forth below.

I. COMPLEXITY

The January 14, 2000 Interim Final Rule adds unnecessary layers of complexity. The unnecessary complexity is confusing, costly, more difficult than need be, and is inconsistent with the general objective of the revisions namely, to make 'retail,' 'mass market' and other forms of encryption products

¹ The United States Council for International Business (USCIB) advances the global interests of American business both at home and abroad. The USCIB has a membership of over 300 global corporations, professional firms, and business associations. It is the American affiliate of the International Chamber of Commerce (ICC), the Business and Industry Advisory Committee (BIAC) to the OECD, and the International Organisation of Employers (IOE). As such, it officially represents U.S. business positions in the main intergovernmental bodies, and vis-à-vis foreign business communities and their governments.

uniformly exportable to almost all end-users in all destinations, save restrictions on terrorist supporting states. An example of the unnecessary complexity is that there are at least thirteen categories of encryption items, some with sub-categories and each having unique rules.²

II. ENCRYPTION ITEM (EI) CONTROLS

The Interim Rule makes progress by releasing certain categories of encryption products from EI controls including:

- mass market encryption commodities, software up to and including 64-bits after review and classification;
- unrestricted encryption source code not subject to an express agreement for the payment of a licensing fee or royalty for commercial production or sale of any product developed using the source code without review; and
- certain encryption items exported and reexported to foreign subsidiaries of U.S. companies without technical review and classification;

As stated, this is good progress. Nevertheless, USCIB members believe that this progress could be greatly improved and the regulations could be simplified if EI-controls from encryption items that are generally exportable were eliminated. At a minimum, USCIB members urge the Department of Commerce to eliminate all EI-controls on all "retail" encryption products. Again, such controls are unrealistic and inconsistent with the general intent of the revised regulations and other provisions of the revised regulations that permit the export of retail encryption items to most destinations.

USCIB members encourage the U.S. Government to take the following steps in conjunction with the elimination of certain EI controls:

A. De Minimis Content

Under the Interim Rule, EI-controlled software is not eligible for de minimis exceptions. Maintaining EI controls on greater than 64-bit software could make it impossible for U.S. manufacturers to supply their products to foreign manufacturers for incorporation into foreign products. This will force companies to continue to produce dual versions of products – one weak encryption version that can be free of EI-controls and one strong encryption version. This will likely lead foreign manufacturers to "design out" U.S. origin components where an EI control creates risk to the foreign manufacturer due to licensing or other review requirements or where the foreign manufacturer is unwilling to accept a weaker version of the product to comply with U.S. rules. Such "design outs" would significantly impair the competitiveness of U.S. providers in foreign markets. Therefore, USCIB members recommend that Section 734.4(b)(2) be eliminated, and 734.4(h) be amended to reflect that deletion. At a minimum, these paragraphs should be amended to apply only to "non-retail" EI controlled items.

² Our members have identified the following categories: (1) authentication-only products; (2) mass-market products up to 64 bits; (3) non-mass-market products up to 56 bits, with key exchange up to 512 bits; (4) other cryptography products (over 64-bits for mass-market, or over 56-bits for non-mass-market) classified as "retail"; (5) other cryptography products (over 64-bits for mass-market, or over 56-bits for non-mass-market) classified as "non-retail" – including network infrastructure products such as high end routers or switches designed for large volume communications; customized encryption products; encryption products that require substantial support for installation and use; products with encryption that is easily modified by the user; (6) key management products up to 512 bits; (7) key management products greater than 512 bits; (8) components (chips, toolkits) up to 56 bits; (9) components (chips, toolkits) greater than 56 bits; (10) general purpose toolkits; (11) publicly available, unrestricted source code; (12) publicly available, restricted source code; and (13) non-publicly available source code.

B. Publicly Available Software

Section 734.3(b)(3) – Virtually all "publicly available software" qualifies as "retail commodities software" and, therefore, is exportable to virtually any end-user in all destinations. Moreover, such software is normally distributed via free or anonymous Internet download and would be exempt from reporting requirements under the draft regulations. The exclusion for EI-controlled software from the "publicly available" exception is inconsistent with other provisions of the Interim Rule and with actual practice and should therefore be eliminated.

C. Published Software

Similarly, Section 734.7(c) – the exclusion for EI-controlled software from the "published information and software" rule – should be eliminated. This paragraph (c) was newly added by the January 14 Rule to make it clear that software controlled under ECCN 5D002 for "EI" reasons remains subject to the EAR even if it is "published" as defined in paragraphs (a) and (b) of that section. This paragraph should be deleted and it should be made clear that "published" encryption software of any key length is not subject to the EAR.

III. RULE INTERPRETATION

The Interim Rule has been effective since January 14, 2000. This has given industry approximately 4 months to assess the application of the Rule by government agencies in actual practice. Our members have raised several concerns about the application of the Interim Rule in practice. Classification requests for retail encryption products are routinely taking much longer than the 30 days specified in Supplement 6 to Part 742. More importantly, restrictive interpretations of the regulations are contrary to the spirit of the promised liberalization and the understanding that industry had with respect to the new rules. And, in some cases, such interpretations are contrary to the black letter of the regulations.

For example, Section 740.17(d) of the regulations states:

"Foreign products developed with or incorporating U.S.-origin encryption source code, components or toolkits remain subject to the EAR, but do not require review and classification by BXA and can be exported or reexported without further authorization."

This clear statement, which on its face exempts review and classification, is being applied in a way that continues to require such review and classification of all foreign produced cryptographic modules that are designed to work with closed CAPIs and that have been developed using U.S. origin components.

It has been suggested that to exclude such foreign-produced modules from review would, in effect, make a closed CAPI an "open cryptographic interface." But that is not the case. "Open cryptographic interface" is defined in the regulations as:

"A mechanism which is designed to allow a customer or other party to insert cryptographic functionality without the intervention, help or assistance of the manufacturer or its agents, e.g., manufacturer's signing of cryptographic code or proprietary interfaces."

But regardless of whether the U.S. government reviews the cryptographic module, a closed CAPI is still a mechanism that requires the intervention of the manufacturer (e.g. digitally signing the code or a hash of the code). So despite the fact that the January 14 regulations do not give the U.S. government the authority to review foreign developed cryptographic modules, BXA continues to require such review.

IV. REPORTING

One of the stated goals of the Interim Final Rule is to streamline reporting requirements and in fact, it has made significant progress toward achieving that goal. Nevertheless, our members have noted with concern that the reporting requirements as set forth in the Interim Rule remain overly complex and burdensome, present difficult questions regarding actual practice, and do not appear to serve any government purpose. Several particular concerns expressed by our members are set forth below.

The Interim Rule requires reporting of sales of 'retail' products to non-individuals. "Retail" products are sold to both individuals and non-individuals/businesses. Often, a U.S. merchant that electronically transmits "retail" products will not know if the end-user is selling the product to the purchaser in his/her individual or non-individual/business capacity. Therefore, to ensure compliance with this requirement, U.S. merchants will, in practice, "over-report" their exports. Given the requirement of one-time review, reporting of retail type products seems to add no value. For example, both the Netscape Navigator web browser and the Internet Explorer component of the Windows operating system have been distributed in quantities greater than the total number of Internet users – so it is safe to assume that virtually every user has both. However, reporting will not reveal what software is actually being used by which user.

Similarly, many companies routinely purchase and use several competing products. For example, over 90% of the largest e-commerce companies run both Oracle and Microsoft SQL servers. The reporting, however, would not reveal how, and to what extent, each product is actually deployed. The reporting would tell the government, that for any particular deployment, there would be either an Oracle server, a Microsoft SQL server, or both. But the same assumption could be made without any reporting whatsoever.

Furthermore, the vast majority of commercial products now use standard security protocols. So, it is unclear what is gained by the knowledge that Company X is using SSL for web security and S/MIME for secure e-mail, since virtually every company is using SSL for web security and S/MIME for secure e-mail.

Moreover, the Wassenaar Arrangement – a multilateral export control regime based on national discretion licensing by each member country – does not require reporting for any strong encryption exports. Prior to December 1998, the Wassenaar Arrangement *did* include reporting requirements for the very small class of encryption products that did not meet the GSN definitions of mass-market or public domain. In December 1998, however, encryption items were removed from the "Sensitive List", thereby removing reporting requirements for even non-mass-market encryption products.³ It is particularly troubling that the U.S. Government agreed to eliminate all requirements for our foreign competitors to report exports of any encryption products, while maintaining burdensome reporting requirements on U.S. companies.

In sum, the reporting requirements are overly burdensome; offer the U.S. Government little, if any, useful information about what, how, and the extent to which strong encryption software is actually being

³ The Arrangement imposes reporting requirements on exports from members countries of items on the so-called "Sensitive List" and "Very Sensitive List" of Annexes 1 and 2 to the Wassenaar list of controlled items. Reporting of exports of such items allows other Wassenaar members to know which of these items are exported to what countries, and allows members to monitor build up of sensitive items and to try to persuade other members not to export certain items to certain end-users. It provides the only useful enforcement mechanism of the Wassenaar Arrangement.

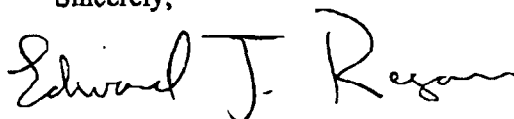
used around the world; and will put U.S. companies at a competitive disadvantage in relation to their foreign competitors.

V. CONCLUSION

The Interim Rule is a significant step forward in implementing the Clinton Administration's encryption policy announced on September 16, 1999 and USCIB members appreciate that progress. Nevertheless, the comments above clearly demonstrate that the Interim Rule will continue to place U.S. merchants at a competitive disadvantage vis-à-vis their foreign counterparts.

Again, thank you for the opportunity to comment on the Interim Rule. We look forward to continuing our dialogue with you on this important issue.

Sincerely,



Edward J. Regan
Chairman, Information Policy Committee



Alliance for
Network
Security

ENC 14
10 f 5

May 15, 2000

Frank J. Ruggiero, Room 2705
Regulatory Policy Division
Bureau of Export Administration
U.S. Department of Commerce
14th Street and Pennsylvania Avenue N.W.
Washington, DC 20230

Re: Comments on Revisions to Encryption Items (65 FR 2492)

Dear Mr. Ruggiero:

Members of the Alliance for Network Security ("ANS") appreciate this opportunity to provide comments on the interim final rule amending the Export Administration Regulations ("EAR", 15 CFR Part 730 *et seq.*) published by the Bureau of Export Administration ("BXA") on January 14, 2000 (65 FR 2492).

ANS members include 3Com, Cisco, Hewlett-Packard, Intel, Lucent Technologies, Microsoft, NetScreen, Network Associates, Novell, RedCreek and Sun Microsystems.

Historically, export controls on encryption have presented a significant impediment to international sales of products produced by the ANS members. Hence, the revisions to the encryption export controls published on January 14, 2000, are important to the international competitiveness of, and are welcomed by, the ANS member companies.

Nevertheless, according to the Wall Street Journal of April 28, 2000, a recent decision by the European Union to remove licensing for sales within the 15 member countries and 10 other countries, and to eliminate technical reviews by national security agencies, threaten to place American companies at a disadvantage again, vis-à-vis our European competitors.

In the preamble to the interim rule, BXA promised:

5. A number of companies have expressed concern that the European Union (EU) may implement a general authorization permitting encryption items to be exported freely within the EU and other specified countries. If and when the EU implements such an authorization, the Administration will take the necessary steps to ensure U.S. exporters are not disadvantaged.

The appropriate response in our view would be to amend the EAR, eliminating the technical reviews and creating a license free zone for exports to these countries.

We have another, high level, concern, which is that the interim rule is too complex for practical administration in member companies.

For example, the interim rule sets forth approximately one dozen different categories of encryption products within the affected Export Control Classification Numbers. The net result is that most cryptographic products may be exported to all destinations except the embargoed/terrorist countries, but subject to various review and reporting requirements that consume considerable time and effort within member companies. We recommend that this complex classification system be collapsed into two items (for weak and strong encryption).

A second example is the reporting requirements which are unworkable in practice and seemingly unnecessary in light of the development of international standards. While ANS member companies appreciate the fact that the exemption from reporting for sales of "retail" products to individuals was introduced for our benefit, in practice it has proved difficult or impossible to determine whether a direct sale is to an individual or a company. Moreover, as international standards like SSL, S/MIME and Bluetooth proliferate, every desktop computer, keyboard, mouse and hand-held device will contain strong encryption and therefore be subject to the reporting requirements. Reporting should be streamlined and focused on those products that are primarily platforms for secure communications, as opposed to consumer goods.

Our further comments are divided into two categories.

The first set of comments focuses on items of specific concern to ANS members. These include (1) the classification of certain networking products as "retail", (2) the sales of non-retail networking products to governments, and (3) reporting requirements for network infrastructure products.

The second set of comments focuses on simplification and clarification of the encryption export controls in the areas of open source software, controls on encryption technology, and controls on technical assistance. As such, they reflect concerns not only of ANS members, but also industry at large.

Items of Specific Concern to ANS Members

We respectfully recommend that BXA consider the following comments in its administration of the new encryption export control policy and its formulation of additional regulatory relief in this area.

1. Scalable Software Firewall-VPN Products Should be Afforded "Retail" Status

Products that combine firewall and virtual private network ("VPN") capabilities are important components of critical infrastructure protection. Indeed, one might argue that the U.S. government should promote, rather than restrict, the widespread deployment of firewall-VPN products, because of their crucial role in Internet security.

ANS members have received conflicting guidance from representatives of BXA and other agencies involved in the implementation of the new encryption export control policy on two important questions. First, may scalable software firewall-VPN products qualify as "retail"? Second, if scalable software firewall-VPN products do not qualify as "retail", are the properly classified as "network infrastructure products" for purposes of the reporting requirements?

We submit that scalable software firewall-VPN products should be considered eligible for retail status and thus are not network infrastructure products. Such products typically are licensed for a number of concurrent users that would qualify for "small-office/home-office", as that term is understood in the context of Section 740.17(a)(3)(iii). The mere fact that software-only products may scale better than competing hardware products should not provide a basis for exclusion of such products from retail treatment. Failure to afford retail status to scalable software firewall-VPN products will distort the market, by forcing developers to integrate firewall-VPN capabilities with other products, like operating systems, in order to compete effectively.

2. License Exception ENC Should be Extended to Governments for Civil Uses

ANS members welcome the new Section 742.15(b)(3), which states that favorable consideration may be given to applications for licenses to "civil uses" by governments. Our review of applications to export to governments for civil uses suggests that none of these applications have been denied since the new policy was implemented. However, the licensing delays for these kinds of applications have been substantial, with potentially disastrous consequences in the form of lost sales. We submit that License Exception ENC should be extended to governments for civil uses described in Section 742.15(b)(3).

3. Special Reporting for Network Infrastructure Products Should be Eliminated

ANS members believe that the special reporting requirements for sales of network infrastructure products to telecommunications and Internet service providers should be eliminated, consistent with the objectives of simplicity and transparency. Let us take as an example a typical "turnkey" export by a systems integrator setting up a new ISP in a Tier 3 country. If that systems integrator were to export one high performance computer (e.g., a server from Sun or HP), one network infrastructure product (e.g., a router from 3Com, Cisco or Lucent), and one "retail" encryption product (e.g., a network interface card from Intel, a web server from Microsoft, Novell's NetWare or Network Associates' Gauntlet GVPN, or a network appliance from RedCreek or NetScreen), then that systems integrator would have to file four different reports at three different times under Sections 740.17(a)(5), 742.12(b)(3)(iv) and 743.1 of the EAR.

4. Network Management Encryption Products Should Be Decontrolled

Products that merely allow a system administrator to configure devices on a network and obtain status reports on network devices, securely and remotely, should be decontrolled provided that they do not allow encryption or decryption of user traffic. The ability to manage devices on a

network securely and remotely is fundamental to sound and cost-effective deployment of networking products and protection of the nation's critical infrastructure. Furthermore, provided that such products do not encrypt user traffic, such network management products should not frustrate known intelligence gathering operations or law enforcement activities. Finally, it is worth noting that the leading product in this market segment is Open SSH, which is an open source product eligible for export under License Exception TSU. For these reasons, among others, we believe that network management products should be exempt from control under ECCN 5A/D002, and classified without a one-time review under ECCN 5A/D992, regardless of cryptographic strength.

Items of General Concern

ANS members have three suggestions that are designed to increase simplicity and transparency in the encryption export control regime.

1. Executable Code for Open or Community Source Should Receive Similar Status

Open source is eligible for export under License Exception TSU pursuant to Section 740.13 of the EAR, even if it includes open cryptographic interfaces. However, the EAR is silent on how executable code derived from open source is treated in the cases where it (a) includes, or (b) does not include, open cryptographic interfaces. We believe that executable code derived from open source should be eligible for export under License Exception TSU, regardless of whether it includes open cryptographic interfaces. The reason is that any person who downloads the open source may compile and execute it. Therefore, the compiled executable code should be afforded similar treatment.

The same principles should apply to so-called "community" source eligible for export License Exception ENC pursuant to Section 740.17(a)(5)(i) of the EAR. If the community source is eligible for License Exception ENC, then the executable code should be, too, regardless of whether it includes an open cryptographic interface.

2. ECCN 5E002 Should Be Removed

Export Control Classification Number ("ECCN") 5E002 on the Commerce Control List ("CCL") of the EAR should be removed, for two reasons. First, we note that almost all encryption technology is publicly available within the definition set forth in Section 734.7 of the EAR. Second, we note that, to the extent the technology may be proprietary, it is common to encryption classified under ECCN 5E992 on the CCL of the EAR.

The only kind of technology we can think of that is neither publicly available nor common to ECCN 5E992 is masks and similar technology that may be specially designed for products controlled under ECCN 5A002. We submit that, because the end-item that is the products of U.S.-origin technology, remains subject to the EAR, there is no benefit to retaining ECCN 5E002

To: Mr. Frank J. Ruggiero
Date: May 15, 2000
Page No.: 5

merely to create a licensing requirement for the offshore manufacture of items controlled under 5A002.

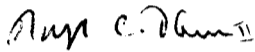
3. Section 744.9 Technical Assistance Controls Should Be Removed

The controls on technical assistance under Section 744.9 of the EAR appear to have been subsumed under the "operation technical data" provisions of License Exception TSU as set forth in Section 740.13(a) of the EAR. Because they appear to serve no useful purpose, beyond that which is authorized for export under License Exception TSU, we believe that they should be removed.

Conclusion

Thank you for this opportunity to comment on the interim final rule Revisions to Encryption Items. Please call me if you have any questions regarding the issues presented in this letter.

Sincerely,



Roszel C. Thomsen II
Counsel
Alliance for Network Security
(410) 539-2595 Ext. 111
E-mail: roz@t-b.com

ENC 15

Hillary Hess, Director
Regulatory Policy Division
Bureau of Export Administration
Department of Commerce
14th Street and Pennsylvania Ave, N.W., Room 2705
Washington DC 20044

Re: CitiGroup Comments on Encryption Regulation of January 14, 2000

Dear Ms. Hess:

Citigroup is pleased to offer comments on the Interim Rule, Revisions to Encryption Items, published January 14, 2000 in 64 *Fed. Reg.* 2492 (Jan. 14, 2000) (the "Rule"), amending the Export Administration Regulations ("EAR"). As you know, Citicorp has previously submitted comments on prior revisions to encryption regulations in 1996, 1997, 1998, and 1999 ever since jurisdiction was transferred from the State Department to the Commerce Department's Bureau of Export Administration ("BXA").

Citigroup companies increasingly rely on products with encryption functions not only for internal and interbank transactions but more and more for secure communication with customers. The nature of our business requires the strongest encryption capabilities available. We appreciate the extent to which the Rule has implemented some of the changes recommended by our earlier comments and how the Administration improved this rule over earlier drafts. We especially appreciate the removal of reporting requirements for exports to and from U.S. banks and financial institutions" as reporting had imposed a major burden on our compliance program. While we note that our concerns have, in part, been addressed, encryption controls are still complex, making compliance by even the most expert difficult. We and our affiliates still devote substantial resources to compliance with export control rules over encryption products. (Please see our November 6, 1998 comments on the September 22 rule, many of which are yet to be addressed.) We hope that the following additional suggestions will help you to make this Rule more workable for exporters.

1. General Comments

We are generally very happy that this Rule has changed the export controls over commercial encryption items in a way that is far more consistent with commercial realities than prior revisions. This Rule represents the most realistic step forward of the Administration's annual changes to encryption regulations. It enables us to export many if not most finished commercial products. We believe however that encryption export regulations can be improved

Citicorp Comments on Encryption Rule
May 15, 2000
Page 2

and streamlined much further. There is sufficient foreign availability (and now U.S. availability) of cryptographic products to render ineffective the restrictions remaining on commercial encryption products. We are describing below the most important changes, and providing more specific comments in Part Two.

1.1 Need to Simplify and Streamline. We remain concerned that the structure of the regulations is overly complex. The regulations apply to at least twelve distinct product groups with separate rules for each for which exporters must adopt compliance procedures. This is unnecessarily confusing. For example, the definition for mass market products eligible for export under License Exception TSU should apply instead of the new term "retail"; there should be only one set of rules for all products with encryption key lengths of 64-bit or less, and rules for publicly available source code and object code should apply to encryption items in the same way as for non-encryption products (putting them outside the scope of the EAR instead of TSU or ENC).

The estimated times in the Rulemaking Requirements section of this Rule grossly underestimate exporters' burdens to learn these rules and comply with them in their current form. For example, while it may take only 5 minutes to complete a notification of source code being made available on the Internet for export under License Exception TSU, that short time only comes after hours of education and work to apply the rules to particular products to determine that one may make such a notification. The real burden is at least two hours per product. We were surprised that BXA stated that it would only take four hours to complete semi-annual reporting requirements, because Citicorp comments in the past have advised you that it took two persons working two full man-weeks plus many others working part time to gather data to make reports. We thus appreciate that the Administration did not eliminate the exemptions from such reporting for U.S. banks and financial institutions. However, those who still have to make reports (and those shipping to non-U.S. banks who must now make reports that previously had not been required) will likely bear a similar burden.

1.2. Need to Eliminate Restrictions on Non-Retail Products. The structure for non-retail encryption items allows exports to commercial end-users in all but nine countries, but prohibits transfers to governments in any country whatsoever. This is an extraordinarily broad and difficult to administer end-user and end-use export control. As an exporter Citigroup does its best to make sure that it does not export or facilitate exports of such products to governments. However, it is unrealistic to expect that governments will never obtain these products or equivalent products, particularly since the encryption components are often exactly the same as those for retail products. We retain broader authority to export some non-retail products under our ELAs to customers, regardless of whether they are governments. So, in some ways, the Rule is more restrictive as to our exports to customers. At a minimum, we still need to obtain either ENC Retail classifications or ELAs to export to all of our customers, but there is no longer a

Citicorp Comments on Encryption Rule
May 15, 2000
Page 3

specific provision for ELAs for banks and financial institutions and their customers. BXA should revise the rules so that all commercial encryption products are exportable under the same rules as for ENC retail products. Remove from Section 740.17(a) the phrase "to any individual, commercial firm, or non-government end-user . . ."; and strike the remainder through to 740.17(b) so that it simply reads to any end-user other than those in the nine embargoed and terrorist supporting countries. That would substantially streamline the Rule and eliminate a lot of confusion and wasted resources.

1.3. Delete Technical Assistance Provisions. We recommend that you eliminate the ITAR-type controls on technical assistance that apply even when there is no controlled export or reexport. Those provisions no longer serve a useful purpose and inhibit U.S. programmers and other U.S. persons who are aware of them from operating on a level playing field with their counterparts around the world. U.S. users of encryption products should freely be able to tell non-U.S. suppliers of such products how to design their encryption products to meet the U.S. users' needs just as the Commerce Department's NIST has been doing with the non-U.S. bidders to supply the U.S. with its Advanced Encryption Standard that will replace DES for U.S. Government use. Now, as NIST has discovered, the EAR requires the U.S. user to obtain a license to provide "technical assistance" to non-U.S. persons. It is helpful that the preamble provides that exporters of unrestricted source code are not prohibited from providing technical assistance to foreign customers, but exporters of commercial products should not be inhibited from helping their customers either. These restrictions do far more harm than good, and we recommend that BXA eliminate them. At a minimum, the Administration should clearly identify what purpose the rules prohibiting technical assistance continue to serve (beyond the export control rules) and justify the continuation of these unusual restrictions in a more reasonably restrictive manner to address the need.

1.4 Incorporate ENC Finance Specific Provisions under the Money and Banking Decontrols to Conform with Long-Standing Interpretations. Citicorp has pointed out consistently that the License Exceptions for finance specific encryption products now set out in Section 740.17(a)(3)(vi) are confusing and redundant. They cover products that the State Department and the NSA long ago advised exporters of financial products were decontrolled under provisions now set out in the "Related Controls" paragraph under ECCN 5A002 "cryptographic equipment [and software] specially designed and limited for banking use or money transactions". No other nation has a separate overlapping general license provision. BXA should move the provision in Section 740.17(a)(3)(vi) to the Interpretation provision of EAR 770.2(n), and make clear that such products are classified under ECCNs 5A992 and 5D992 per the decontrol note. It would be important to make clear in the definition that the concept of "securing financial communications/transactions" includes all forms of communication, such as e-mail.

Citicorp Comments on Encryption Rule
May 15, 2000
Page 4

1.5 Drop Restrictions on Open Cryptographic Interfaces. Open cryptographic interfaces are not permitted for exports under License Exception ENC, but public source code products to build products with open cryptographic interfaces are freely exportable under TSU, as are publicly available products compiled from such source code. Likewise, non-U.S. source and object code products with open APIs are freely available around the world. It serves no useful purpose to restrict U.S. exporters from providing such products and thus to require U.S. software developers to undertake more cumbersome and expensive programming than non-U.S. competitors. BXA should eliminate this restriction by deleting Section 740.17(f).

1.6 Reporting. The Administration agreed in December 1998 to eliminate all reporting requirements for exports of encryption items under the multilateral export control rules of the Wassenaar Arrangement. The Administration dropped all requirements for reporting exports of encryption products to BFIs in an amendment to the Export Administration Regulations effective December 31, 1998. There is thus no increased risk that would justify requiring reporting now, particularly to non-U.S. banks and financial institutions, which is a rollback over prior controls. We do not believe that we have to report such exports, but the rules are confusing in this regard. The cumbersome and confusing reporting requirements in this Rule are unilateral export controls that burden and thus add costs to U.S. encryption exporters that are not borne by any non-U.S. persons. We submit that there is no clear benefit to reporting, merely a clear and unwarranted burden. All reporting should be eliminated to put U.S. exporters on a level playing field with their competitors. At a minimum, as an alternative the Administration should delete any requirement for reporting exports of retail encryption items and eliminate the rollback in reporting required for exports to non-U.S. banks and financial institutions.

1.7 Delete EI Restrictions from Retail Encryption Products. The "EI Controls" imposed when commercial encryption products were moved from the International Traffic in Arms Control Regulations in 1996 to the EAR deny the application to those products of protections against excessive controls such as *de minimis*, "publicly available", and foreign availability rules. At this point, it is counterproductive to continue to treat "retail" products as subject to EI controls. Retail products are decontrolled for export to all but seven countries, and reexport controls are almost nonexistent. Section 740.17(d) says that foreign products incorporating U.S. encryption content do not require further review and can be exported without further authorization. But, this provision is confusing because the EAR elsewhere says that these products remain subject to EI controls of the EAR. The EI controls are an anachronism. They remain important collateral burdens with no remaining benefit. These restrictions are not enforceable, but they do inhibit U.S. sales and undermine respect for the regulations. Maintaining EI controls on retail Encryption Items inhibit sales by U.S. manufacturers for incorporation into many foreign products because the EI controls subject the foreign product to U.S. reexport controls regardless of the minimal level of the U.S. EI-product incorporated into it. The EI controls thus mean that one function in basic operation software that is one percent of the

Citicorp Comments on Encryption Rule
May 15, 2000
Page 5

value of the end item would theoretically be controlled. The reality is that non-U.S. companies who actually care will not buy such products if they are subject to U.S. unilateral reexport controls that cost more than the product.

For example, those European and Japanese manufacturers who treat U.S. reexport controls seriously will buy from non-U.S. suppliers the operating system for a bank machine rather than subject their \$10,000 ATM to U.S. reexport controls. It is not that U.S. exporters want their products to be sold to U.S. embargoed countries, but that customers with worldwide sales in fact design out small U.S. components to avoid reexport restrictions that cost them far more than the U.S. components themselves. (To encourage them to ignore these controls undermines respect for the regulations.) If this exclusion is not removed, it will force many U.S. companies either to lose significant worldwide sales or to continue to produce dual versions of products - one weak encryption version that can be free of EI-controls (but will have little market), and one strong encryption version (the market for which will also remain restricted). If this is the case, the cost savings and the ability to compete with foreign suppliers that were anticipated as a result of the new policy will be retarded.

Given the essentially unfettered exportability of "retail" encryption products, and the very broad exportability of the remaining "non-retail" products, the exclusion from de minimis treatment for EI-controlled items is outdated and unnecessary. Existing reexport controls on U.S.-origin products, products with U.S.-origin content, and direct products of U.S.-origin technology and software protect the Administration's concerns adequately and realistically without creating the level of distrust and anticompetitiveness that the EI controls do. The effect of the current control is to inhibit only those who meticulously try to comply with U.S. reexport controls (or force them to buy foreign) but allow such ubiquitous products free reign that they arrive at the destination in ATMs, car navigation aids, computers, etc. anyway. Thus, the impact on U.S. national security of this change will be minimal, but can result in millions of sales by U.S. companies to Europeans and others who make worldwide sales. We urge you to remove EI controls from retail encryption products. We recommend that you drop all EI controls entirely by deleting the last sentence of 734.8(a) and making corresponding changes. Short of that, BXA can remove EI controls from retail items by (1) adding a provision after the first sentence in Part 740.17(a)(3) stating that "Encryption items reviewed and classified as retail will be released from EI controls."; (2) revising the last amended sentence to Section 734.4(b) and the last sentence of 740.13(d)(2) to refer also to "740.17(a)(3) and (e)"; and (3) deleting 734.7(c).

2. Additional Specific Comments

For convenience, these comments are set forth in the order of the draft regulation rather than in order of priority. We would be pleased to provide further specific language to drafters upon request.

Citicorp Comments on Encryption Rule
May 15, 2000
Page 6

2.1 Put Substantive Provisions of the Preamble in the Regulation. Substantive provisions and interpretations that exporters will look for in the regulation as it is applied during the next year should be included in the regulation, not left to the preamble. This includes provisions stating that exporters of unrestricted encryption source code are not restrained from providing technical assistance to foreign persons working with such source code, and the provision stating that distributors and resellers can export and reexport under ELAs as long as they comply with the requirements (particularly since that interpretation is at odds with other parts of the EAR that say only the license holder can export under a license and had previously been included in EAR 742.15, and it is less necessary to provide as in EAR 740.17(h) that distributors and resellers may use License Exception ENC as any classification and license exception can be used by anyone but special permission is needed to use a license of another party).

2.2 Clarify That Download Restrictions Do Not Apply to Retail Products, at Least Not to Anonymous Downloads. Like other companies, Citigroup would like to post to the web client products with encryption capabilities for download by customers. Exporters of retail encryption software working with Administration officials on the draft for this Rule were surprised when, at the last minute, BXA dropped "retail encryption software" from the list of products in Section 734.2(b)(9)(ii) that were not considered exports when posted to, e.g., web sites for download. At a minimum, BXA should revise ENC provisions to say that posting of retail encryption software to the web for anonymous downloads would not establish "knowledge" of a prohibited export or reexport and does not trigger a duty to inquire under Know Your Customer Guidance, as is provided explicitly in Section 740.13(e)(3) for public source code and, by interpretation, object code compiled from it. Retail software "exporters" had understood that this same safe harbor would apply to them.

2.3 Move Public Availability Provisions from TSU to Section 734.7 for Both Source and Object Code Software that is Published and Unrestricted and Clarify Ability to Use TSU Provisions Other than the General Software Note for Encryption Items. We appreciate the provisions allowing unrestricted source code that is published to be exported freely after notification. We also appreciate that BXA has provided to those who request it advisory opinions stating that object code compiled from such source code that is made publicly available without royalty also is released from EI controls and may be exported freely after notification. That provision should be published in the EAR as it is not apparent from the regulations. Likewise, other publicly available object code should receive the same treatment regardless of whether it is compiled from Open Source Code. Publicly available object code software should be eligible for this treatment just like non-EI controlled publicly available object code and EI-controlled publicly available source code software are.

Citicorp Comments on Encryption Rule
May 15, 2000
Page 7

As a structural matter, this new Section 740.13(e) belongs in Section 734.7, which applies to all other published software and information and which would otherwise apply when EI controls are lifted on such items. It contradicts the EAR structure for this Rule to release such items from EI controls, meaning that they are excluded from the EAR, then say that TSU applies. That treatment undermines the standard structure of the EAR. The provision in 740.17(f) should then cross reference to 734.7. The embargoed and terrorist supporting countries are not excluded from the "publicly available" rule, since that concept is premised on the assumption that publicly available information and software cannot be controlled to any destination. The Berman Amendment to IEEPA compels release from controls.

In addition, BXA should revise the initial phrase of Section 740.13(d)(2) "This provision of License Exception TSU" to clarify that other provisions for bug-fixes, sales technical data, etc., may still be used for encryption software and technology.

2.4 Clarify Provisions Regarding Exports to U.S. Subsidiaries, Particularly Deemed Export -- Section 740.17(a)(1). The Rule has effectively eliminated application of the deemed export rule to EI technology, but in a way that remains more cumbersome than it should. There has never been an EAR deemed export rule for encryption software or source code, so it should be dropped cleanly for technology. It would be clearer if Section 734.2(b)(2) referred to Section 734.2(b)(9) for encryption technology as well as encryption source and object code software. From discussions with the drafters, it appears to have been an oversight in 1996 that the deemed export rule was intentionally dropped for encryption source code but not for encryption technology.

At a minimum, the present Rule should be clarified further. For example, BXA has provided helpful verbal interpretations that the Provisions of Section 740.17(a)(1) that allow deemed exports to employees of U.S. firms for internal use to apply to all types of employees, including student interns and contractors, and to other U.S. companies that employ foreign nationals. The regulations should make this clear. This section of the regulations should use "U.S. persons" (a defined term) instead of "U.S. firms" to cover individuals, etc., and make clear the scope. Change "their foreign national employees" to "foreign nationals" to make clear that the deemed export rule does not apply even when working with consultants, nationals of other companies, students, etc.

Also, it would be helpful to insert at the end of the last sentence of 740.17(a)(1) "unless specifically authorized by other provisions of the EAR (e.g., key upgrades, subsequent bundling interpretation)". Some U.S. subsidiaries believe they are at a disadvantage in having to obtain classifications that other companies do not. The provision does not make such a distinction, because it only applies to items "exported under this paragraph", but as written that subtlety has been lost even on BXA experts discussing the matter at special seminars.

Citicorp Comments on Encryption Rule
May 15, 2000
Page 8

Finally, the defined term "U.S. Subsidiary" should replace the undefined "subsidiary of U.S. firm" in initial paragraph and paragraph (1) of Part 740.17(a).

2.5 If the Retail Distinction is Retained, Clarify Application of Retail. As described in Part 1 above, we strongly prefer that all encryption products be treated the same as retail. Alternatively, the definition of "retail" should be revised to be the same as the general cryptography note (with the exception of key length limitations). If the first major change is not made, Section 740.17(a)(3) needs clarification. Insert in subsection (iv) after "Encryption products" the phrase "not meeting provisions of (i) and (ii) above but" to clarify the application of this helpful provision to allow companies with functionally equivalent products to meet competition. Delete the term "low end" from "servers in subsection (iii) and otherwise clarify that nothing in this illustrative list restricts products that meet criteria of (i) and (ii) from being classified as retail. Further, replace the term "sold" in subsection (i) in all cases with "transferred or anticipated to be transferred" for consistency and to allow for classifications of products being brought to market. The Administration has clearly applied "anticipated to be transferred" in some of its applications approving new products, but certain exporters have been advised that this is not possible, giving the appearance of different treatment.

Insert the terms "distributors, or resellers" after "retail outlets" in subsection (i) to level the playing field for different distribution methods and nomenclature. Subsection (ii) of the definition would be clearer if it deleted the word "specifically" before "designed".

We were advised by the BXA that the intent of Section 740.17(e)(3)(i) on key length increases was that, once a product is classified as retail, changes to the key length made by a letter as specified in this section do not change the status of the product, i.e., it still remains retail. This intent needs to be made explicit as this section otherwise appears to require another product review in order for the product to keep its retail status.

Delete Restrictions on Network Infrastructure Products. Section 740.17(a)(3)(D) should be eliminated. Certain high end products have been classified as retail, but agencies have said for others that there is a school of thought that any product that runs on a LAN is network infrastructure, giving the appearance that the application of this provision may be subjective from one product to another. Because most low end retail products have the same encryption that scales to high end infrastructure products, the distinction only serves to keep U.S. exporters from competing in the high end market with non-U.S. companies. Likewise, the provision in (C) serves no useful purpose.

The Provisions Applicable to Internet and Telecommunications Service Providers Should Apply to Any Civil End-User. Provisions in Section 740.17(a)(4) allow specified civil end-users

Citicorp Comments on Encryption Rule
May 15, 2000
Page 9

to provide non-retail products as services to governments, but do not allow other companies to do so on the same basis. This provision should apply to any civil user.

2.6 Reduce and Streamline Reporting Provisions 740.17(g). The following comments supplement those in Part 1.

No reports should be required for exports of any retail products. Delete "exported to individual consumers" from 740.17(g)(1)(iv) and (2)(ii). Reporting of retail exports is a waste of resources, private and government. These products are eligible for export everywhere except to embargoed countries and are now exported in the millions, making reporting information meaningless. For direct distribution, distinguishing between individual consumers and others is usually impossible. A less preferable amendment to relieve the burden here would be to add in Section 740.17(g)(1)(iv) and (2)(ii) "in single units with no license for multiple use copies (other than for backup), or when loaded onto or accompanying personal computers and workstations" so that only multiple product shipments would be reported and so that PCs which have numerous types of software, more and more often with encryption, do not need to be reported. It is an impossible task for exporters of such products to keep track of such minor software programs, often provided free of charge.

Reduce burden of reporting for indirect sales. Likewise, the requirement of subsection (2)(i) to report "if collected, the end user name and address" even when selling via distributors seems potentially to call for reporting of registration cards, again, voluminous and largely inaccurate. We appreciate that this provision requires only reports of information "collected", but "systematically collected" would be a better term as the term "collected" by itself could reasonably be construed to cover anyone in the company actually obtaining the information, which is a broader net than we understand you intend to cast.

Clarify Reporting for Components, Commercial Source Code, and General Purpose Toolkits. The requirement to provide technical descriptions under 740.17(g)(3) is very problematic for exports of components, commercial source code, and general purpose toolkits that are sold directly to hundreds or thousands of OEMs. If exporters of such items must provide a technical description of a final product for each OEM, the burden would be enormous for both exporters and the government. We appreciate that Part 4.h of the Preamble provides that such reporting requirements can be adjusted on a case by case basis to waive such reporting requirements when enough information is provided during the initial technical review to enable the U.S. Government to understand the types of products that will result. This provision should be included in Section 740.17(g)(3) of the regulation itself and should apply to commercial source code and general purpose tool kits as well (provided of course that the sufficient showing can be made).

Citicorp Comments on Encryption Rule
May 15, 2000
Page 10

"The requirement to provide non-proprietary descriptions of final products will be waived for components constrained by function for use in a particular class of end products. Reporting is not required for products covered by the subsequent bundling interpretation in Section 770.2(n)."

Remove rollback for reporting to banks and financial institutions and their customers. We particularly appreciate the changes from earlier drafts made for exports from U.S. banks and financial institutions, and interpret the term "for banking and financial operations" to cover communications by banks and financial institutions with their customers. Nevertheless, no justification has been demonstrated for adding this burden and rolling back a provision of the 1998 policy that eliminated reporting for exports of the same encryption items to non-U.S. banks and financial institutions. Reports that did not need to be provided for such exports during 1999 are no more necessary for the proper functioning of the law and have no more practical utility now than when they were not required. We recommend that the word "operations" be changed to "matters", that the qualifier "U.S." be deleted. Exporters who sell largely to the financial industry have to report for some of their exports and not others, a burdensome and wasteful requirement.

Allow for an extra 30 day grace period to prepare reports. The reporting burden is grossly underestimated in the preamble and will take immense time and effort given the increasing proliferation of encryption products. One month after the close of a period is not sufficient time to gather all of the data required to report multitude of exports of products through many different channels and compile it and report it.

The requirement for electronic reporting in certain formats should be changed to an option. This provision imposed a new burden on exporters, though it is obviously beneficial for government. Prior to this Rule, BXA had refrained from requiring that reporting be done in any specific format. Exporters should be able to submit reports in whatever format is most convenient, as they do now for other types of exports pursuant to Section 743. Moreover, the draft rule seems to require companies to compile a complete and detailed report of their business activity (including customer names/addresses and volumes) in a single electronic file with no security provisions. BXA should not even encourage submission of electronic reports unless it has a secure methods of transmission such as encrypted files or separate hand deliveries to a trusted official of each of the two agencies.

2.7 Clean Up Technical Review Provisions. Technical review requirements still impose a major burden on companies like hours, for whom time to market for new products is critical. We suggest the following improvements:

Citicorp Comments on Encryption Rule

May 15, 2000

Page 11

Comply with the 30 Calendar Day Limit. The addition of the right to export to non-government entities 30 days after submission at first blush seems to be a remarkable improvement, but the fact that there are no controls on exports of any encryption products to non-government entities indicates that no review should be required or that this time period be amended to ten days. If BXA can do normal classifications and NDAA reviews in ten days, surely the agency can tell if enough information to understand the product was submitted in that time period. For non-retail products, the ability to export to non-governments should commence on submission of the classification application. For retail products, BXA and NSA must honor the normal 14-day time period for classifications, at minimum the 30 day time period that the Administration extended to itself in this Rule. As a practical matter, exporters cannot effectively discriminate between governments and other end-users for retail products, so they have to wait for the classification to export. Supplement 6 to EAR Part 742 extends from the current statutory and regulatory requirement of 14 calendar days to process a classification to 30 calendar days, which is over twice the prior time limit. Yet, most classifications are taking around 60 days. It is unacceptable that the Administration does not find itself bound by these regulations and routinely exceeds even this extended time limit.

Eliminate Mandatory Classification Request for ECCNs 5X992 Items. We continue to object to a requirement that exporters obtain a classification for items under ECCNs 5X992. Exporters are not required to seek classifications for any other ECCNs, but they may do so if they have questions. (See EAR Part 748.) The provisions of Category 5, Part 2 of the CCL set out objective criteria that exporters can apply themselves. We know of no classification of 64-bit items that has been denied. It is time to eliminate the requirement for this review.

Clarify Provisions for Exports to Syria for ECCNs 5X992. Section 742.15(b)(1) provides that items classified under ECCNs 5A992, 5D992, or 5E992 may not be exported to certain countries, including Syria. But, those ECCNs allow export of encryption items (not telecommunications items) to Syria. Insert the following sentence after the word Syria: "(Exports of items controlled under these ECCNs require a license for Syria only if subject to AT Column 1 controls.)" Given the ongoing Middle East Peace Talks, we question whether this is the time to tighten controls on exports to Syria inadvertently.

Ensure that Supplement 6 to Part 742 Correctly Specifies Information that Needs to Be Provided. (A) Exporters need to provide information on distribution methods to obtain the coveted "retail" classification, but Supplement 6 does not say so. Supplement 6 should be revised to add that exporters seeking a retail classification should provide information as to why the product meets the provisions of 740.17(a)(3)(i) and (ii) or (iii), (vi), or (vii). (B) Supplement 6 should also clarify whether or when any source code will be required to be submitted. Companies obviously control proprietary source code very tightly, and will typically not release

Citicorp Comments on Encryption Rule
May 15, 2000
Page 12

it to any party without a Non-Disclosure Agreement. It is currently hard to predict when source code will be required.

2.8 Simplify Confusing Inconsistencies Regarding Key Length Limits and Product Classification. The Rule is unclear and confusing regarding the classification of products with various symmetric / asymmetric key length combinations, especially with respect to 64-bit products. We understand that the Wassenaar Arrangement creates many of these problems by setting decontrol levels at 56-bit and 512 bit, but allowing mass market decontrol at 64-bit with no asymmetric limit. A chart to supplement the regulations is helpful. Nevertheless, there should be a way to simplify the classifications and, ultimately, the Wassenaar rules. Because virtually all of these products are effectively decontrolled, and the real problem is one of "labelling," it would be much simpler and cleaner to remove EI controls and allow exports under, preferably, NLR, but at minimum under License Exception ENC as retail authority of all encryption products with a symmetric key length of 64-bit regardless of the key exchange mechanism (or at least to 1024). That way, exporters would have a simple option to apply rather than having to decide which of several complex classifications and shipping options applies to substantially similar products.

The simple option (using ENC if the Administration feels constrained by Wassenaar obligations) can be established via the following changes. Revise Section 740.17(a)(3)(vii) to state: "Any encryption products with a symmetric key of 64-bit or below and a key exchange mechanism of 1024-bit or below is released from EI controls and may be exported under License Exception ENC. See Section 742.15(b)(1) and Category 5, Part 2 of the CCL for options to classify some such products under ECCNs 5A992, 5D992, or 5E992." Also, add the following sentence at the end of Section 740.15(b)(1): "Note that exporters have the option of exporting any encryption products with a symmetric key of 64-bit or below and a key exchange mechanism of 1024-bit or below under License Exception ENC (see Section 740.17(a)(3)(vii))."

In any case, in Section 740.17(e)(3)(i), insert "or non-mass market software" to the parenthetical "(or for hardware [INSERT], ENC)" to cover upgrades to non-mass market software as well. It would be preferable simply to say in this section "Any 56-bit product previously classified as eligible for export under License Exceptions TSU or ENC may increase key lengths . . . to 64 . . . 1024 . . . and still be eligible for export under NLR or ENC as retail without an additional review." Also, make clear in Section 740.17(e)(2) and 742.15(b)(1) that 56-bit products previously approved as eligible for export under TSU or ENC qualify for ECCN 5A992 or 5D992 or ENC without further review.

2.9 Put Finance Specific Restrictions under the Money and Banking Decontrols to Conform with Long-Standing Interpretations. As discussed in Part 1, the provisions for finance specific encryption products now set out in Section 740.17(a)(3)(vi) have long been an

Citicorp Comments on Encryption Rule
May 15, 2000
Page 13

empty box as they apply to products that the State Department and the NSA long ago advised exporters of financial products were decontrolled under provisions now set out in the "Related Controls" paragraph under ECCN 5A002 "cryptographic equipment [and software] specially designed and limited for banking use or money transactions". The overlapping provisions are confusing and unnecessary. The provision in Section 740.17(a)(3)(vi) should be moved to the Interpretation provision of EAR 770.2(n), which should make clear that such products are classified under ECCNs 5A992 and 5D992 per the decontrol note. Citicorp has consistently pointed out this issue since 1996, when the regulations moved to the jurisdiction of the EAR.

2.10 Section 742.15 Still Needs to Be Cleaned Up to Clarify Certain Issues. First, Section 742.15(b)(1) should be moved to subsection (a) because it reflects decontrol rather than licensing policy for controlled items. Subsection (b) starts by describing licensing policies for ECCN 5A/D/E002 items identified under paragraph (a), but subsection (b)(1) addresses items that can be classified under ECCNs 5A/D/E992. This section should also make clear that classification requests are optional (even if recommended) for anything that can be classified under ECCNs 5A/D/E992.

Second, as noted previously, this section should explicitly describe the differences between 56-bit and 64-bit products and the key exchange limits affecting each (1024 for 56-bit and 512 for 64), and why those distinctions exist to answer the obvious questions raised. Again, we recommend simple NLR or ENC classification for all such products.

Third, subsection (b)(2) needs a cross reference to License Exception ENC provisions under Section 740.17(a).

Fourth, the Administration could ameliorate a lot of concerns if Section 742.15(b)(3) would specify additional licensing policy for exports to government end-users, such as whether ELAs would likely be approved for export to government end-users in countries listed in Country Group A:1 (or Computer Tier 1 or Supplement 3, for that matter). The International Traffic in Arms Regulations allow for reexport of most Munitions List components to Governments of NATO, Australia, and Japan without a license. (22 C.F.R. § 123.9(e).) The EAR should do so as well. The provisions added are helpful, but do not go as far as the ITAR.

Fifth, the licensing provisions should make clear that distributors and resellers can also make exports under ELAs if they comply with the restrictions thereunder. This provision was in the prior regulation and should not be relegated to a preamble since it contradicts other provisions that state that only license holders may export under a license. Also, this section should provide that ELA licensees are only liable for violations by others that they "knew" would occur.

Citicorp Comments on Encryption Rule
May 15, 2000
Page 14

2.11 Technical Assistance Provisions in Section 744.9 Should Be Eliminated. As discussed in Section 1, the provisions of Section 744.9 are now anachronistic and no longer useful. They should be eliminated entirely as no longer serving a useful purpose. At a minimum, they should be revised to reflect that technical assistance regarding use of lawfully exported U.S. items is not prohibited. Most companies must provide technical assistance for their exportable products. U.S. exporters will also need to compete to provide assistance in developing products overseas. And, users must provide technical assistance to non-U.S. suppliers to ensure that products meet quality control standards, just as NIST has done with potential non-U.S. suppliers for AES. Without revision, the prohibitions in Section 744.9 would prohibit normal activities related to authorized exports and even imports. This is particularly true for exports of encryption source code, toolkits, and encryption components. These services, like encryption products, should be exportable under license exception to commercial users. Otherwise the U.S. Government will continue to provide foreign competitors with significant market advantages, as they can supply identical technical services to the same customers without first obtaining a U.S. license. This is too important to leave to a one line provision in the preamble.

2.12 The Interpretation Section 770.2(n) Should Be Expanded to:

Insert the following descriptor after the phrase "functional encryption capacity": "(j.e., confidentiality algorithm or key exchange mechanism)". This provision should also cross reference the ability to increase key lengths in Section 740.17(e)(3).

Include a Statement re Crypto Aware Products. Add: "Products that do not include encryption functions but that make encryption calls to products already classified may be classified under the same category as the product which they call for encryption functions." Few exporters realize that NSA interprets the regulations as requiring such "crypto aware" products to be reviewed, even though they classify them according to the product that they call. Principal among these are products making calls to the Microsoft CAPI, which allegedly must be reviewed and are routinely classified as eligible for TSU export. The vast majority of exporters of such products have no idea that they need to be reviewed. This duplication of effort and trap for the unwary should be eliminated.

Clarify the Restriction Regarding Other CCL Entries. Revise the last sentence to read "This does not relieve exporters from more restrictive controls that may apply if the item is also covered by another ECCN.

Clarify MAC Decontrol in the Interpretations or a Note to Category 5, Part 2. We appreciate the clarification in the Preamble that it was not the intent of the new Wassenaar language to be more restrictive regarding "data authentication equipment that calculates a

Citicorp Comments on Encryption Rule
May 15, 2000
Page 15

Message Authentication Code (MAC) or similar result to ensure that no alteration of text has taken place . . ." and that such items (including software) continue to be excluded from control under ECCN 5A002. This important provision needs to be included as a Note to Category 5, Part 2, or in the Interpretations Section 770.2(n) rather than left to the preamble.

Clarify that the "related control" decontrol provision d. under ECCN 5A002 applies to DVD and MPEG type functions by stating: The decontrol provisions in Category 5, Part 2 also place under ECCNs 5A002 or 5D002 the execution of algorithms for audio/video data restricted to performing decrypt and encrypt functions for tamper resistance purposes associated with the execution of copy protected data (e.g., DVD and MPEG).

2.13 The Definition of "Government End-User" Has Been Improved, but can be Improved Further. We recommend that the civil end-uses described as likely to be favorably considered for license applications in Section 742.15(b)(3) be moved to paragraph (b) of the definition of Government (which lists what is not considered "government" for these purposes) so that licenses do not even need to be filed for such end-uses. Delete from Section 742.15(b)(3) the phrase "social or financial services to the public, civil justice, social insurance, pensions and retirement, taxes and communications between governments and their citizens". Insert in part (b) of the definition of "Government End-user (as applied to encryption items)" the phrase "and other entities engaged in civil uses, e.g., the provision of social or financial service to the public, civil justice, social insurance, pensions and retirement, taxes and communications between governments and their citizens."

2.14 BXA Should Consolidate Decontrol Provisions in Category 5, Part 2, Section 774, Supplement 1. Presumably, drafting is somewhat constrained by the structure of the Wassenaar Arrangement, but the format is confusing even for experts in export control. The **decontrol provisions now appear in three places**, the Cryptography Note 3, the Related Controls paragraph to ECCN 5D002, and technical notes under ECCN 5A002.a.1. The "related controls" paragraph is not a logical place for decontrol provisions. It would be helpful to move the decontrol provisions from the "Related Controls" paragraph into a new Note 4 up front, and add there a cross reference to the exclusions from controls in the technical notes to ECCN 5A002.a.1. This section should also cross reference Section 742.15, particularly any requirement (if retained against our advice) that products be reviewed before they can be decontrolled. Most experienced exporters who classify their products look to the CCL and will not be aware from those provisions that in this rare case some products decontrolled by the CCL must be formally classified for the decontrol to apply.

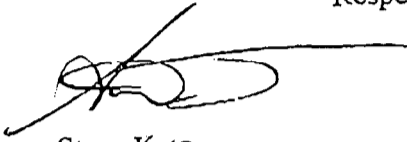
2.15 References to the "T-7" Countries Should Also include "and (if applicable) embargoed destinations (See Part 746)" in all cases to avoid confusion. This is lost in the preamble.

16 of 16

Citicorp Comments on Encryption Rule
May 15, 2000
Page 16

We appreciate the opportunity to provide these comments. We would be happy to discuss them at your request.

Respectfully submitted,



Steve Katz

Under Secretary William Reinsch
Ms. Charlotte Knepper
Mr. Bruce McConnell

ENC 16
10/12

REGULATIONS AND PROCEDURES TECHNICAL ADVISORY COMMITTEE

Hillary Hess, Director
Regulatory Policy Division
Bureau of Export Administration
Department of Commerce
14th Street and Pennsylvania Ave, N.W., Room 2705
Washington DC 20044

Re: Comments on Encryption Regulation of January 14, 2000

Dear Ms. Hess:

The Regulations and Procedures Technical Advisory Committee ("RPTAC") is pleased to offer the following comments on the Interim Rule, Revisions to Encryption Items, published January 14, 2000 in 64 *Fed. Reg.* 2492 (Jan. 14, 2000) (the "Rule"). As you know, we have previously submitted comments on draft versions of these regulations and on prior revisions to encryption regulations since jurisdiction was transferred from the State Department to the Commerce Department's Bureau of Export Administration ("BXA"). Due to time constraints, you were able to incorporate some, but not most, of our comments of December 31, 1999 on the last draft, so we are repeating them for convenience as well as offering fresh comments.

1. General Comments

We are generally very happy that this Rule has changed the export controls over commercial encryption items in a way that is far more consistent with commercial realities than prior revisions. This Rule represents the most realistic step forward of the Administration's annual changes to encryption regulations. It enables many if not most finished commercial products to compete with non-U.S. companies. We also appreciate the web site guidance that BXA has published, and how BXA and NSA and other officials have been open to comment and suggestions throughout the regulatory revision process.

We do believe that encryption export regulations can be improved and streamlined much further, particularly in light of the recent EU decontrol announcement. There is sufficient foreign availability (and now uncontrolled U.S. availability) of cryptographic products to render ineffective the restrictions remaining on commercial encryption products. We are describing below the most important changes, and then providing more specific comments in a second section.

1.1. Need to Eliminate Restrictions on Non-Retail Products at Least for EU Plus Ten Countries. The structure for non-retail encryption items allows exports to commercial end-users in all but nine countries, but prohibits transfers to governments in any country whatsoever. This is the broadest and most difficult to administer end-user and end-use export control ever created. Exporters are doing their best to make sure that they do not export or facilitate exports of such products to governments, but it is unrealistic to expect that governments will never obtain these products or equivalent products, particularly since the encryption components are often exactly the same as those for retail products. Some exporters retain somewhat broader authority to export some non-retail products under ELAs to favored sectors, regardless of whether they are governments. So, in some ways, the Rule is more restrictive as to exports under prior policy. All commercial encryption products should be exportable under the same rules as for ENC retail products. BXA should revise Section 740.17(a) to remove the phrase "to any individual, commercial firm, or non-government end-user. . . ."; and strike the remainder through to 740.17(b) so that it simply reads to any end-user other than those in the nine embargoed and terrorist supporting countries. That would substantially streamline the Rule and eliminate a lot of confusion and wasted resources.

At a bare minimum, BXA should allow unlimited exports to a license free zone of the fifteen member European Union countries plus ten to meet their recent decision to eliminate export licensing requirements to those countries. Otherwise, U.S. companies will be at a severe disadvantage vis-à-vis European competitors. The preamble to the Rule anticipated this change and promised that the Administration will take necessary steps to

ensure that U.S. exporters are not disadvantaged by this development. We request that you at least take this step at once.

Also, at a minimum, the Administration should use the "mass market" terminology employed in the General Cryptography Note (without bit length limitations) and in the General Software Note, instead of the confusing term "retail". The two are now nearly the same, and any remaining distinction is more cumbersome than useful. In so doing, however, the Administration should not exclude from eligibility non-programmable chips for retail items that are widely distributed, but may not have qualified as "mass market" in the past.

1.2 Need to Simplify and Streamline. We remain concerned that the structure of the regulations is overly complex and in many ways unrealistic. The regulations apply to twelve distinct product groups with separate rules for each for which exporters must adopt procedures to comply. This is unnecessarily confusing for even the most expert compliance personnel of major multinational companies, much less for small businesses.

For example, the definition for mass market products eligible for export under License Exception TSU should apply instead of the new term "retail", there should be only one set of rules for all products with encryption key lengths of 64-bit or less, and rules for publicly available source code and object code should apply to encryption items in the same way as for non-encryption products (putting them outside the scope of the EAR instead of TSU or ENC).

The estimated times in the Rulemaking Requirements section of this Rule grossly underestimate exporters' burdens to learn these rules and complying with them in their current form. For example, while it may take only 5 minutes to complete a notification of source code being made available on the Internet for export under License Exception TSU, that short time only comes after hours of education and application of the rules to particular products. We were surprised at your low estimates of the burden for reporting given our prior submissions that reporting would be far more burdensome. For example, rather than four hours to complete semi-annual reporting requirements, one multinational estimates that it will take over 1000 hours every six months to outline the requirements, educate the necessary personnel, determine which products will require which type of reports, set up systems where possible, and gather and consolidate the information for the submission to the BXA. Citicorp previously advised that it took them four man weeks (160 hours) every six months just by the two persons who were principally responsible for reporting before the 1998 changes effectively eliminated their reporting requirements. This time could be spent far more productively.

1.3. Delete Technical Assistance Provisions. It is also high time to eliminate the ITAR type controls on technical assistance that apply even when there is no controlled export or reexport. Those provisions no longer serve a useful purpose. They simply inhibit U.S. programmers and other U.S. persons who are aware of them from operating on a level playing field with their counterparts around the world. It is helpful that the preamble provides that exporters of unrestricted source code are not prohibited from providing technical assistance to foreign customers, but exporters of commercial products should not be inhibited from helping their customers either. Likewise, U.S. users of encryption products should freely be able to tell non-U.S. suppliers of such products how to design their encryption products to meet the U.S. users' needs just as the Commerce Department's NIST has been doing with the non-U.S. bidders to supply the U.S. with its Advanced Encryption Standard that will replace DES for U.S. Government use. Now, as NIST found out the hard way, the EAR requires the U.S. user to obtain a license to provide "technical assistance" to non-U.S. persons. The Administration should clearly identify what, if any, purpose the rules prohibiting technical assistance continue to serve (beyond the export control rules) and justify the continuation of these unusual restrictions or, if as we submit they do more harm than good, eliminate them.

1.4 Drop Restrictions on Open Cryptographic Interfaces. Open cryptographic interfaces are not permitted for exports under License Exception ENC, but public source code products to build products with open cryptographic interfaces are freely exportable under TSU, as are publicly available products compiled from such source code. Likewise, non-U.S. source and object code products with open CAPIs are freely available around the world. It serves no useful purpose to restrict U.S. exporters from providing such products and thus to require U.S. software developers to undertake more cumbersome and expensive programming than non-U.S. competitors. BXA should eliminate this restriction by deleting Section 740.17(f).

The Administration Should Also Cease Imposing Unwritten Restrictions on Closed CAPIs.

Restrictive interpretations of the regulations are contrary to the spirit of the promised liberalization and the understanding that industry had with respect to the new rules. Section 740.17(d) of the regulations states:

"Foreign products developed with or incorporating U.S.-origin encryption source code, components or toolkits remain subject to the EAR, but do not require review and classification by BXA and can be exported or reexported without further authorization."

The statements in the regulations are very clear, and do not seem to be subject to any interpretation that would require the review of foreign produced cryptographic modules. There is no requirement for the technical review of any foreign-produced cryptographic items. Nevertheless, BXA continues to require the review and classification of all foreign produced cryptographic modules that are designed to work with closed CAPIs and have been developed using U.S.-origin components.

It has been suggested that to exclude such foreign-produced modules from review would, in effect, make a closed CAPI an "open cryptographic interface." But that is not the case. "Open cryptographic interface" is defined in the regulations as:

"A mechanism which is designed to allow a customer or other party to insert cryptographic functionality without the intervention, help or assistance of the manufacturer or its agents, e.g., manufacturer's signing of cryptographic code or proprietary interfaces."

But regardless of whether the U.S. government reviews the cryptographic module, a closed CAPI is still a mechanism that requires the intervention of the manufacturer (e.g. digitally signing the code or a hash of the code). So despite the fact that the January 14 regulations do not give the U.S. government the authority to review foreign developed cryptographic modules, BXA continues to require such review.

1.5 Reporting. The Administration agreed in December 1998 to eliminate all reporting requirements for exports of encryption items under the multilateral export control rules of the Wassenaar Arrangement. Thus, the cumbersome and confusing reporting requirements in this Rule are unilateral export controls that burden and thus add costs to U.S. encryption exporters that are not borne by our non-U.S. competitors. The Administration has not even attempted to explain why there is some benefit to the United States as a whole that justifies this burden, opting instead to require U.S. industry to justify why it should not be required to report such encryption exports. We submit that there is no clear benefit to reporting, merely a clear and unwarranted burden. All reporting should be eliminated to put U.S. exporters on a level playing field with their competitors. At a minimum, as an alternative, the Administration should (a) delete any requirement for reporting exports of retail encryption items, (b) delete the special reporting requirements for sales of network infrastructure products to telecommunications and Internet service providers, and (c) eliminate the rollback in reporting required for exports to non-U.S. banks and financial institutions (which was not required prior to this rule).

1.6 Delete EI Restrictions from Retail Encryption Products. The "EI Controls" imposed when commercial encryption products were moved from the International Traffic in Arms Control Regulations in 1996 to the EAR deny the application to those products of protections against excessive controls such as *de minimis*, "publicly available", and foreign availability rules. At this point, it is counterproductive to continue to treat "retail" products as subject to EI controls. Retail products are decontrolled for export to all but embargoed or terrorist countries, and reexport controls are almost nonexistent. Section 740.17(d) says that foreign products incorporating U.S. encryption content do not require further review and can be exported without further authorization. But, this provision is at best confusing because the EAR elsewhere still says that these products remain subject to EI controls of the EAR. The EI controls are an anachronism that has outlived their usefulness. They remain important collateral burdens with no remaining benefit. These restrictions are not enforceable, but they do inhibit U.S. sales and undermine respect for the regulations. Maintaining EI controls on retail Encryption Items inhibit sales by U.S. manufacturers for incorporation into many foreign products because the EI controls subject the foreign product to U.S. reexport controls regardless of the minimal level of the U.S. EI-product incorporated into it.

For example, those European and Japanese automobile manufacturers who treat U.S. reexport controls seriously will buy from non-U.S. suppliers the \$30 operating system for a navigation aid rather than subject their \$50,000 cars to U.S. reexport controls. It is not that U.S. exporters want their products to be sold to U.S. embargoed

countries, but that customers with worldwide sales in fact design out small U.S. components to avoid reexport restrictions that cost them far more than the U.S. components themselves. (To encourage them to ignore these controls undermines respect for the regulations.) If this exclusion is not removed, it will force many U.S. companies either to lose significant worldwide sales or to continue to produce dual versions of products - one weak encryption version that can be free of EI-controls (but will have little market), and one strong encryption version (the market for which will also remain restricted). If this is the case, the cost savings and the ability to compete with foreign suppliers that were anticipated as a result of the new policy will be retarded.

Current rules do release from EI controls open source source code, and by interpretation any publicly available products compiled from such source code. Thus, the effect of the *de minimis* rules is felt by makers of proprietary object code for operating software, putting them at a competitive disadvantage with U.S. open source exporters as well as non-U.S. companies that apply such open source products and non-U.S. products. This disadvantage accomplishes nothing for national security, but does harm the U.S. businesses and non-U.S. companies who are trying their utmost to comply with U.S. reexport controls.

Given the essentially unfettered exportability of open source and "retail" encryption products, and the very broad exportability of the remaining "non-retail" proprietary products, the exclusion from *de minimis* treatment for EI-controlled items is outdated and unnecessary. Existing reexport controls on U.S.-origin products, products with U.S.-origin content, and direct products of U.S.-origin technology and software protect the Administration's concerns adequately and realistically without creating the level of distrust and anticompetitiveness that the EI controls do. We urge you to remove EI controls from retail encryption products. We recommend that you drop all EI controls entirely by deleting the last sentence of 734.8(a) and making corresponding changes. Short of that, BXA can remove EI controls from retail items by (1) adding a provision after the first sentence in Part 740.17(a)(3) stating that "Encryption items reviewed and classified as retail will be released from EI controls."; (2) revising the last amended sentence to Section 734.4(b) and the last sentence of 740.13(d)(2) to refer also to "740.17(a)(3) and (e)"; and (3) deleting 734.7(c).

2. Additional Specific Comments

For convenience, these comments are set forth in the order of the draft regulation rather than in order of priority. We would be pleased to provide further specific language to drafters upon request.

2.1 Put Substantive Provisions of the Preamble in the Regulation. Substantive provisions and interpretations that exporters will look for in the regulation as it is applied during the next year should be included in the regulation, not left to the preamble. This includes provisions stating that exporters of unrestricted encryption source code are not restrained from providing technical assistance to foreign persons working with such source code. the provision stating that distributors and resellers can export and reexport under ELAs as long as they comply with the requirements (particularly since that interpretation is at odds with other parts of the EAR that say only the license holder can export under a license and had previously been included in EAR 742.15, and it is less necessary to provide as in EAR 740.17(h) that distributors and resellers may use License Exception ENC as any classification and license exception can be used by anyone but special permission is needed to use a license of another party), and the provision that exporters of components, tool kits, and networking products can negotiate for relief from special reporting requirements during one time reviews.

2.2 Clarify That Download Restrictions Do Not Apply to Retail Products, at Least Not to Anonymous Downloads. Exporters of retail encryption software working with Administration officials on the draft for this Rule were surprised when, at the last minute, BXA dropped "retail encryption software" from the list of products in Section 734.2(b)(9)(ii) that were not considered exports when posted to, e.g., web sites for download. At a minimum, BXA should revise the ENC provisions to say that posting of retail encryption software to the web for anonymous downloads would not establish "knowledge" of a prohibited export or reexport and does not trigger a duty to inquire under Know Your Customer Guidance, as is provided explicitly in Section 740.13(e)(3) for public source code and, by interpretation, object code compiled from it. Other software should also be provided this safe harbor as the retail software manufacturers understood the regulations were going to provide.

2.3 Move Public Availability Provisions from TSU to Section 734.7 for Both Source and Object Code Software that is Published and Unrestricted and Clarify Ability to Use TSU Provisions Other than the

General Software Note for Encryption Items. We appreciate the provisions allowing unrestricted source code that is published to be exported freely after notification. We also appreciate that BXA has provided to those who request it advisory opinions stating that object code compiled from such source code that is made publicly available without royalty also is released from EI controls and may be exported freely after notification. That provision should be published in the EAR as it is not apparent from the regulations. Likewise, other publicly available object code should receive the same treatment regardless of whether it is compiled from Open Source Code. There is no utility in treating object code more strictly. It should be eligible for publicly available treatment just like any other object code software, publicly available source code, and object code compiled from the latter.

As a structural matter, this new Section 740.13(e) belongs in Section 734.7, which applies to all other published software and information and which will apply when EI controls are lifted on such items. It is confusing to release such items from EI controls, meaning that they are excluded from the EAR, then say that TSU applies. That undermines the structure of the EAR. The provision in 740.17(f) should then cross reference to 734.7. There is no reason to treat published object code more restrictively than source code. Further, the embargoed and terrorist supporting countries are not excluded from the "publicly available" rule, since that concept is premised on the assumption that publicly available information and software cannot be controlled to any destination. **The Berman Amendment to IEEPA compels release of publicly available software from controls just as for other "informational materials".**

In addition, the initial phrase of Section 740.13(d)(2) should be revised to "This provision of License Exception TSU" to clarify that other provisions for bug-fixes, sales technical data, etc., may still be used for encryption software and technology.

2.4 Clarify Provisions Regarding Exports to U.S. Subsidiaries, Particularly Deemed Export -- Section 740.17(a)(1). BXA has provided helpful verbal interpretations that the Provisions of Section 740.17(a)(1) that allow deemed exports to employees of U.S. firms for internal use apply to all types of employees, including student interns and contractors. The regulations should make this clear. For example, this section of the regulations should use "U.S. persons" (a defined term) instead of "U.S. firms" to cover individuals, etc., and make clear the scope. Change "their foreign national employees" to "foreign nationals" to make clear that deemed export rule does not apply even when working with consultants, nationals of other companies, students, etc. This rule should be even simpler. There has never been an EAR deemed export rule for encryption software or source code, so we should just drop it cleanly for technology. It would be cleaner if Section 734.2(b)(2) referred to Section 734.2(b)(9) for encryption technology as well as encryption source and object code software. From discussions with the drafters, it appears to have been an oversight in 1996 that the deemed export rule was intentionally dropped for encryption source code but not for encryption technology.

Also, it would be helpful to insert at the end of the last sentence of 740.17(a)(1) "unless specifically authorized by other provisions of the EAR (e.g., key upgrades, subsequent bundling interpretation)". Some U.S. subsidiaries believe they are at a disadvantage in having to obtain classifications that other companies do not. The provision does not make such a distinction, because it only applies to items "exported under this paragraph", but as written that subtlety has been lost even on BXA experts discussing the matter at special seminars.

Finally, the defined term "U.S. Subsidiary" should replace the undefined "subsidiary of U.S. firm" in initial paragraph and paragraph (1) of Part 740.17(a).

2.5 If the Retail Distinction is Retained, Clarify Application of Retail. As described in Part 1 above, we strongly prefer that all encryption products be treated the same as retail. Alternatively, the definition of "retail" should be revised to be the same as the general cryptography note (with the exception of key length limitations). If the first major change is not made, Section 740.17(a)(3) needs clarification. Insert in subsection (iv) after "Encryption products" the phrase "not meeting provisions of (i) and (ii) above but" to clarify the application of this helpful provision to allow companies with functionally equivalent products to meet competition. Delete the term "low end" from "servers in subsection (iii) and "routers and switches" in that same section, and otherwise clarify that nothing in this illustrative list restricts products that meet criteria of (i) and (ii) from being classified as retail. Further, replace the term "sold" in subsection (i) in all cases with "transferred or anticipated to be transferred" for consistency and to allow for classifications of products being brought to market. The Administration has clearly applied "anticipated to be transferred" in some of its applications approving new products, but certain exporters have

been advised that this is not possible, giving the appearance of different treatment.

Insert the terms "distributors, or resellers" after "retail outlets" in subsection (i)(A) to level the playing field for different distribution methods and nomenclature. Subsection (ii)(D) of the definition would be clearer if it deleted the word "specifically" before "designed".

We were advised by the BXA that the intent of Section 740.17(e)(3)(i) on key length increases was that, once a product is classified as retail, changes to the key length made by a letter as specified in this section do not change the status of the product, i.e. it still remains retail. This intent needs to be made explicit as this section otherwise appears to require another product review in order for the product to keep its retail status.

Delete Restrictions on Network Infrastructure Products. Section 740.17(a)(3)(i)(D) should be eliminated. Certain high end products have been classified as retail, but agencies have said for others that there is a school of thought that any product that runs on a LAN is network infrastructure, giving the appearance that the application of this provision may be subjective from one product to another. Because most low end retail products have the same encryption that scales to high end infrastructure products, the distinction only serves to keep U.S. exporters from competing in the high end market with non-U.S. companies. Likewise, the provision in (C) serves no useful purpose.

Treat Compiled Code from Community Source Code the Same Way as the Source Code. As discussed above, BXA has advised that freely available object code compiled from publicly available source code receives the same treatment (TSU or, as we propose makes more sense, TSPA). The same principles should apply to so-called "community" source eligible for export License Exception ENC pursuant to Section 740.17(a)(5)(i) of the EAR. If the community source is eligible for License Exception ENC, then the executable code should be, too, regardless of whether it includes an open cryptographic interface.

Scalable Software Firewall-VPN Products Should Be Afforded "Retail" Status. Products that combine firewall and virtual private network ("VPN") capabilities are important components of critical infrastructure protection. Indeed, the U.S. government should promote, rather than restrict, the widespread deployment of firewall-VPN products because of their crucial role in Internet security. Companies have received conflicting guidance from representatives of BXA and other agencies on two important questions. First, may scalable software firewall-VPN products qualify as "retail"? Second, if scalable software firewall-VPN products do not qualify as "retail", are they properly classified as "network infrastructure products" for purposes of the reporting requirements? We submit that scalable software firewall-VPN products should be considered eligible for retail status and thus are not network infrastructure products. Such products typically are licensed for a number of concurrent users that would qualify for "small-office [or] home-office", as that term is understood in the context of Section 740.17(a)(3)(iii). The mere fact that software-only products may scale better than competing hardware products should not provide a basis for exclusion of such products from retail treatment. Failure to afford retail status to scalable software firewall-VPN products will distort the market by forcing developers to integrate firewall-VPN capabilities with other products, like operating systems, in order to compete effectively.

Network Management Encryption Products Should Be Afforded ENC Retail Treatment or Be Decontrolled. Products that merely allow a system administrator to configure devices on a network and obtain status reports on network devices, securely and remotely, should be decontrolled provided that they do not allow encryption or decryption of user data. The ability to manage devices on a network securely and remotely is fundamental to sound and cost-effective deployment of networking products and protection of the nation's critical infrastructure. Furthermore, provided that such products do not encrypt user data, such network management products should not frustrate known intelligence gathering operations or law enforcement activities. Finally, it is worth noting that the leading product in this market segment is Open SSH, which is an open source product eligible for export under License Exception TSU. For these reasons, among others, we believe that network management products should be exempt from control under ECCN 5A/D002, and classified without a one-time review under ECCN 5A/D992, regardless of cryptographic strength, or at least be made eligible for ENC Retail status.

The Provisions Applicable to Internet and Telecommunications Service Providers Should Apply to Any Civil End-User. Provisions in Section 740.17(a)(4) allow specified civil end-users to provide non-retail products as services to governments, but do not allow other companies to do so on the same basis. This

provision should apply to any civil user.

2.6 Reduce and Streamline Reporting Provisions 740.17(g). The following comments supplement those in Part 1 above.

No Reports Should Be Required for Exports of Any Retail Products. Delete "exported to individual consumers" from 740.17(g)(1)(iv) and (2)(ii). Reporting of retail exports is a phenomenal waste of resources, private and government. These products are eligible for export everywhere except to embargoed countries and are now exported in the millions, making reporting information meaningless. For direct distribution, distinguishing between individual consumers and others is usually impossible. We appreciate the accommodations for anonymous downloads, but the volume of data and the burden of reporting other types of exports overwhelm the value. Exporters of retail products will have to choose between two bad alternatives. One would be over reporting by sending in all relevant information, but that might violate the EU Privacy Directive. The other would be to make a reasonable determination whether sales via certain channels were predominantly to individuals or enterprises and report only those predominantly to enterprises, resulting in some over reporting and some under reporting. It is not clear that the regulations authorize such an approach. A less preferable amendment to relieve the burden here would be to add in Section 740.17(g)(1)(iv) and (2)(ii) "in single units with no license for multiple use copies (other than for backup), or when loaded onto or accompanying personal computers and workstations" so that only multiple product shipments would be reported and so that PCs which have numerous types of software, more and more often with encryption, do not need to be reported. Many if not most of the voluntary disclosures made to BXA have been of PCs exported without clear knowledge that they contained retail programs with encryption functions. It is an impossible task for exporters of such products to keep track of such minor software programs, often provided free of charge. If no relief is granted in this area, the burden is such that some distributors are likely to shift distribution and thus employment overseas to avoid reporting obligations, an unfortunate result of the policy indeed.

Reduce Burden of Reporting for Indirect Sales. Likewise, the requirement of subsection (2)(i) to report "if collected, the end user name and address" even when selling via distributors seems potentially to call for reporting of registration cards, again, voluminous and largely inaccurate. We appreciate that this provision requires only reports of information "collected", but "systematically collected" would be a better term as the term "collected" by itself could reasonably be construed to cover anyone in the company actually obtaining the information, which is a broader net than we understand you intend to cast.

Reduce Reporting for Components, Commercial Source Code, and General Purpose Toolkits. The requirement to provide technical descriptions under 740.17(g)(3) is very problematic for exports of components, commercial source code, and general purpose toolkits that are sold directly to hundreds or thousands of OEMs. If exporters of such items must provide a technical description of a final product for each OEM, the burden would be enormous for both exporters and the government. We appreciate that Part 4.h of the Preamble provides that such reporting requirements can be adjusted on a case by case basis to waive such reporting requirements when enough information is provided during the initial technical review to enable the U.S. Government to understand the types of products that will result. This provision should be included in Section 740.17(g)(3) of the regulation itself and should apply to commercial source code and general purpose tool kits as well (provided of course that the sufficient showing can be made).

"The requirement to provide non-proprietary descriptions of final products will be waived for components constrained by function for use in a particular class of end products. Reporting is not required for products covered by the subsequent bundling interpretation in Section 770.2(n)."

Eliminate Special Reporting for Network Infrastructure Products. The special reporting requirements for sales of network infrastructure products to telecommunications and Internet service providers should be eliminated, consistent with the objectives of simplicity and transparency. Let us take as an example a typical "turnkey" export by a systems integrator setting up a new ISP in a Tier 3 country. If that systems integrator were to export one high performance computer, one network infrastructure product, and one "retail" encryption product, then that systems integrator would have to file four different reports at three different times under Sections 740.17(a)(5), 742.12(b)(3)(iv) and 743.1 of the EAR.

Remove Rollback for Reporting to Banks and Financial Institutions and Their Customers.

We also appreciate the changes made for exports from U.S. banks and financial institutions, and the interpretation that the term "for banking and financial operations" as covering communications by banks and financial institutions with their customers. However, no justification has been demonstrated for rolling back a provision of the 1998 policy that eliminated reporting for exports of the same encryption items to non-U.S. banks and financial institutions. Reports that did not need to be provided during the past year are no more necessary for the proper functioning of the law and have no more practical utility now than when they were not required. We recommend that the word "operations" be changed to "matters", that the qualifier "U.S." be deleted. Exporters who sell largely to the financial industry have to report for some of their exports and not others, a burdensome and wasteful requirement.

Allow for an Extra 30 Day Grace Period to Prepare Reports. The reporting burden is grossly underestimated in the preamble and will take immense time and effort given the increasing proliferation of encryption products. One month after the close of a period is not sufficient time to gather all of the data required to report multitude of exports of products through many different channels and compile it and report it.

Change the Requirement for Electronic Reporting in Certain Formats to an Option. This provision imposed a new burden on exporters, though it is obviously beneficial for government. To date, BXA has refrained from requiring that reporting be done in any specific format. Exporters should be able to submit reports in whatever format is most convenient, as they do now for other types of exports pursuant to Section 743. Moreover, the draft rule seems to require companies to compile a complete and detailed report of their business activity (including customer names/addresses and volumes) in a single electronic file with no security provisions. BXA should not even encourage submission of electronic reports unless it has a secure methods of transmission such as encrypted files or separate hand deliveries to a trusted official of each of the two agencies.

2.7 Clean Up Technical Review Provisions. Technical review criteria remain a cumbersome delay for companies for whom time to market is critical to maintain a competitive edge. We recommend the following improvements.

Comply with the 30 Calendar Day Limit. The addition of the right to export to non-government entities 30 days after submission at first blush seems to be a remarkable improvement, but the fact that there are no controls on exports of any encryption products to non-government entities indicates that no review should be required or that this time period be amended to ten days. If BXA can do normal classifications and NDAA reviews in ten days, surely the agency can tell if enough information to understand the product was submitted in that time period. For non-retail products, the ability to export to non-governments should commence on submission of the classification application. For retail products, BXA and NSA must honor the normal 14-day time period for classifications, at minimum the 30 day time period that the Administration extended to itself in this Rule. As a practical matter, exporters of retail products cannot discriminate between governments and other end-users so will have to wait for the classification to export. Moreover, Supplement 6 to EAR Part 742 extends from the current statutory and regulatory requirement of 14 calendar days to process a classification to 30 calendar days, which is over twice the prior time limit. It is thus unacceptable that the Administration does not find itself bound by these regulations and routinely exceeds even this extended time limit. Most classifications are taking around 60 days.

Eliminate Mandatory Classification Request for ECCNs 5X992 Items. We continue to object to a requirement that exporters obtain a classification for items under ECCNs 5X992. Exporters are not required to seek classifications for any other ECCNs, but they may do so if they have questions. (See EAR Part 748.) The provisions of Category 5, Part 2 of the CCL set out objective criteria that exporters can apply themselves. We know of no classification of 64-bit items that has been denied. It is time to eliminate the requirement for this review.

Clarify Provisions for Exports to Syria for ECCNs 5A992, 5D992, or 5E992. Section 742.15(b)(1) provides that items classified under ECCNs 5A992, 5D992, or 5E992 may not be exported to certain countries, including Syria. But, those ECCNs allow export of encryption items (not telecommunications items) to Syria. Insert the following sentence after the word Syria: "(Exports of items controlled under these ECCNs require a license for Syria only if subject to AT Column 1 controls.)" Given the ongoing Middle East Peace Talks, this is not the time to tighten controls on exports to Syria inadvertently.

Ensure that Supplement 6 to Part 742 Correctly Specifies Information that Needs to Be

Provided. (A) Exporters need to provide information on distribution methods to obtain the coveted "retail" classification, but Supplement 6 does not say so. Supplement 6 should be revised to add that exporters seeking a retail classification should provide information as to why the product meets the provisions of 740.17(a)(3)(i) and (ii) or (iii), (vi), or (vii). (B) Supplement 6 should also clarify whether or when any source code will be required to be submitted. Companies obviously control proprietary source code very tightly, and will typically not release it to any party without a Non-Disclosure Agreement. It is currently hard to predict when source code will be required.

Allow for Specification Based Reviews Instead of Product by Product Reviews. We appreciate that the Administration has not published results of classifications, though we believe it would be helpful to publish or link to exporter publications when the exporter waives confidentiality provisions. Otherwise, the Administration is engaging in redundant reviews. It would help to reduce the number of reviews if the Administration would allow for classifications based on a model cryptographic specification describing the encryption design parameters, the relevant encryption algorithm for encryption and key exchange, the applicable interfaces, likely types of product applications, and likely sales channels and customer types. Reporting could also be streamlined in like fashion by allowing exporters to describe the types of end-users and parts of the world for products meeting the specifications rather than reporting on each and every export.

2.7 Simplify Confusing Inconsistencies Regarding Key Length Limits and Product Classification.

The Rule is unclear and confusing regarding the classification of products with various symmetric / asymmetric key length combinations, especially with respect to 64-bit products. We understand that the Wassenaar Arrangement creates many of these problems by setting decontrol levels at 56-bit and 512 bit, but allowing mass market decontrol at 64-bit with no asymmetric limit. A chart to supplement the regulations certainly helps. Nevertheless, there should be a way to simplify the classifications and, ultimately, the Wassenaar rules. Because virtually all of these products are effectively decontrolled, and the real problem is one of "labeling", it would be much simpler and cleaner to remove EI controls and allow exports under, preferably, NLR, but at minimum under License Exception ENC as retail authority of all encryption products with a symmetric key length of 64-bit regardless of the key exchange mechanism (or at least to 1024). That way, exporters would have a simple option to apply rather having to decide which of several complex classifications and shipping options applies to substantially similar products.

The simple option (using ENC if the Administration feels constrained by Wassenaar obligations) can be established via the following changes. Revise Section 740.17(a)(3)(vii) to state: "Any encryption products with a symmetric key of 64-bit or below and a key exchange mechanism of 1024-bit or below is released from EI controls and may be exported under License Exception ENC. See Section 742.15(b)(1) and Category 5, Part 2 of the CCL for options to classify some such products under ECCNs 5A992, 5D992, or 5E992." Also, add the following sentence at the end of Section 740.15(b)(1): "Note that exporters have the option of exporting any encryption products with a symmetric key of 64-bit or below and a key exchange mechanism of 1024-bit or below under License Exception ENC (see Section 740.17(a)(3)(vii))."

In any case, in Section 740.17(e)(3)(i), insert "or non-mass market software" to the parenthetical "(or for hardware [INSERT], ENC)" to cover upgrades to non-mass market software as well. It would be preferable simply to say in this section "Any 56-bit product previously classified as eligible for export under License Exceptions TSU or ENC may increase key lengths . . . to 64 . . . 1024 . . . and still be eligible for export under NLR or ENC as retail without an additional review." Also, make clear in Section 740.17(e)(2) and 742.15(b)(1) that 56-bit products previously approved as eligible for export under TSU or ENC qualify for ECCN 5A992 or 5D992 or ENC without further review.

2.8 Put Finance Specific Restrictions under the Money and Banking Decontrols to Conform with Long-Standing Interpretations. The provisions for finance specific encryption products now set out in Section 740.17(a)(3)(vi) have long been an empty box as they apply to products that the State Department and the NSA long ago advised exporters of financial products were decontrolled under provisions now set out in the "Related Controls" paragraph under ECCN 5A002 "cryptographic equipment [and software] specially designed and limited for banking use or money transactions". The overlapping provisions are confusing and unnecessary. The provision in Section 740.17(a)(3)(vi) should be moved to the Interpretation provision of EAR 770.2(n), which should make clear that such products are classified under ECCNs 5A992 and 5D992 per the decontrol note. We have consistently pointed out this issue ever since the regulations moved to the jurisdiction of the EAR in 1996.

2.9 Section 742.15 Still Needs to Be Cleaned Up to Clarify Certain Issues. First, Section 742.15(b)(1) should be moved to subsection (a) because it reflects decontrol rather than licensing policy for controlled items. Subsection (b) starts by describing licensing policies for ECCN 5A/D/E002 items identified under paragraph (a), but subsection (b)(1) addresses items that can be classified under ECCNs 5A/D/E992. This section should also make clear that classification requests are optional (even if recommended) for anything that can be classified under ECCNs 5A/D/E992.

Second, as noted previously, this section should explicitly describe the differences between 56-bit and 64-bit products and the key exchange limits affecting each (1024 for 56-bit and 512 for 64), and why those distinctions exist to answer the obvious questions raised. Again, we recommend simple NLR or ENC classification for all such products.

Third, subsection (b)(2) needs a cross reference to License Exception ENC provisions under Section 740.17(a).

Fourth, the Administration could ameliorate a lot of concerns if Section 742.15(b)(3) would specify additional licensing policy for exports to government end-users, such as whether ELAs would likely be approved for export to government end-users in countries listed in Country Group A:1 (or Computer Tier 1, for that matter). The International Traffic in Arms Regulations allow for reexport of most Munitions List components to Governments of NATO, Australia, and Japan without a license. (22 C.F.R. § 123.9(e).) The EAR should do so as well. The provisions added are helpful, but do not even go as far as the ITAR.

Fifth, the licensing provisions should make clear that distributors and resellers can make exports under ELAs if they comply with the restrictions thereunder. This provision was in the prior regulation and should not be relegated to a preamble since it contradicts other provisions that state that only license holders may export under a license. Also, this section should provide that ELA licensees are only liable for violations by others that they "knew" would occur.

2.10 Eliminate Technical Assistance Provisions in Section 744.9. As discussed in Section 1, the provisions of Section 744.9 are now anachronistic and no longer useful. They should be eliminated entirely as no longer serving a useful purpose. At a minimum, they should be revised to reflect that technical assistance regarding use of lawfully exported U.S. items is not prohibited. Most companies must provide technical assistance for their exportable products. U.S. exporters will also need to compete to provide assistance in developing products overseas. And, users must provide technical assistance to non-U.S. suppliers to ensure that products meet quality control standards, just as NIST has done with potential non-U.S. suppliers for AES. Without revision, the prohibitions in Section 744.9 would prohibit normal activities related to authorized exports and even imports. This is particularly true for exports of encryption source code, toolkits, and encryption components. These services, like encryption products, should be exportable under license exception to commercial users. Otherwise the U.S. Government will continue to provide foreign competitors with significant market advantages, as they can supply identical technical services to the same customers without first obtaining a U.S. license. This is too important to leave to a one line provision in the preamble.

2.11 Expand Interpretation Section 770.2(n) to:

Insert the following descriptor after the phrase "functional encryption capacity": "(i.e., confidentiality algorithm or key exchange mechanism)". This provision should also cross reference the ability to increase key lengths in Section 740.17(e)(3).

Include a Statement re Crypto Aware Products. Add: "Products that do not include encryption functions but that make encryption calls to products already classified may be classified under the same category as the product which they call for encryption functions." Few exporters realize that NSA interprets the regulations as requiring such "crypto aware" products to be reviewed, even though they classify them according to the product that they call. Principal among these are products making calls to the Microsoft CAPI, which allegedly must be reviewed and are routinely classified as eligible for TSU export. The vast majority of exporters of such products have no idea that they need to be reviewed. This duplication of effort and trap for the unwary should be eliminated.

Clarify the Restriction Regarding Other CCL Entries. Revise the last sentence to read “This does not relieve exporters from more restrictive controls that may apply if the item is also covered by another ECCN.

Clarify MAC Decontrol in the Interpretations or a Note to Category 5, Part 2. We appreciate the clarification in the Preamble that it was not the intent of the new Wassenaar language to be more restrictive regarding “data authentication equipment that calculates a Message Authentication Code (MAC) or similar result to ensure that no alteration of text has taken place . . .” and that such items (including software) continue to be excluded from control under ECCN 5A002. This important provision needs to be included as a Note to Category 5, Part 2, or in the Interpretations Section 770.2(n) rather than left to the preamble.

Clarify that the “related control” decontrol provision d. under ECCN 5A002 applies to DVD and MPEG type functions by stating: The decontrol provisions in Category 5, Part 2 also remove from ECCNs 5A002 or 5D002 the execution of algorithms for audio/video data restricted to performing decrypt and encrypt functions for tamper resistance purposes associated with the execution of copy protected data (e.g., DVD and MPEG).

2.12 The Definition of “Government End-User” Has Been Improved, but can be Improved Further. We recommend that the civil end-uses described as likely to be favorably considered for license applications in Section 742.15(b)(3) be moved to paragraph (b) of the definition of Government (which lists what is not considered “government” for these purposes) so that licenses do not even need to be filed for such end-uses. Delete from Section 742.15(b)(3) the phrase “social or financial services to the public, civil justice, social insurance, pensions and retirement, taxes and communications between governments and their citizens”. Insert in part (b) of the definition of “Government End-user (as applied to encryption items)” the phrase “and other entities engaged in civil uses, e.g., the provision of social or financial service to the public, civil justice, social insurance, pensions and retirement, taxes and communications between governments and their citizens.”

2.13 BXA Should Consolidate Decontrol Provisions in Category 5, Part 2, Section 774, Supplement 1. Presumably, drafting is somewhat constrained by the structure of the Wassenaar Arrangement, but the format is confusing even for experts in export control. The **decontrol provisions now appear in three places**, the Cryptography Note 3, the Related Controls paragraph to ECCN 5D002, and technical notes under ECCN 5A002.a.1. The “related controls” paragraph is not a logical place for decontrol provisions. It would be helpful to move the decontrol provisions from the “Related Controls” paragraph into a new Note 4 up front, and add there a cross reference to the exclusions from controls in the technical notes to ECCN 5A002.a.1. This section should also cross reference Section 742.15, particularly any requirement (if retained against our advice) that products be reviewed before they can be decontrolled. Most experienced exporters who classify their products look to the CCL and will not be aware from those provisions that in this rare case some products decontrolled by the CCL must be formally classified for the decontrol to apply.

2.14 References to the “T-7” Countries Should Also include “and (if applicable) embargoed destinations (See Part 746)” in all cases to avoid confusion. This is lost in the preamble.

2.15 Eliminate ECCN 5E002. The Administration should negotiate with Wassenaar Arrangement allies to eliminate ECCN 5E002 as no longer serving any useful purpose. ECCN 5E002 on the Commerce Control List (“CCL”) of the EAR should be removed, for two reasons. First, we note that almost all encryption technology is publicly available within the definition set forth in Section 734.7 of the EAR. Second, we note that, to the extent the technology may be proprietary, it is common to encryption classified under ECCN 5E992 on the CCL of the EAR.

The only kind of technology we can think of that is neither publicly available nor common to ECCN 5E992 is masks and similar technology that may be specially designed for products controlled under ECCN 5A002. We submit that, because the end-item that is the products of U.S.-origin technology, remains subject to the EAR, there is no benefit to retaining ECCN 5E002 merely to create a licensing requirement for the offshore manufacture of items controlled under 5A002.

The RPTAC appreciates the opportunity to submit these comments. We welcome the opportunity answer questions you may have or to discuss them with you.

Respectfully submitted,

RPTAC Encryption Working Group on behalf of the RPTAC
(Patricia J. Steiner, Lucent Technologies Inc., Co-Chair; Roszel C. Thomsen II, Thomsen & Burke, L.L.P., Co Chair; Walter E. Spiegel, NCR Corporation; Vera A. Murray, IBM Corp.; Ben H. Flowe, Jr., Berliner, Corcoran & Rowe, L.L.P.; Sandra L. Vincent, Intel Corp; Kathleen Gebeau, QUALCOMM, Inc.; David B. Calabrese, Electronic Industries Alliance; and David H. Robb, GTE Corp.)

cc: Under Secretary William Reinsch
Ms. Charlotte Knepper
Mr. Bruce McConnell
RPTAC Members
PECSENC

cc: Under Secretary William Reinsch
Ms. Charlotte Knepper
Mr. Bruce McConnell

ICOTT INDUSTRY COALITION ON TECHNOLOGY TRANSFER

1400 L Street, N.W., Washington, D.C. 20005 Suite 800 (202) 371-5994

May 15, 2000

Mr. Frank J. Ruggiero
Regulatory Policy Division
Bureau of Export Administration
U.S. Department of Commerce, Room 2705
14th Street and Pennsylvania Avenue, N.W.
Washington DC 20230

Re: Revisions to Encryption Items, 65 Fed. Reg. 2492 (2000)

Dear Mr. Ruggiero:

On behalf of the Industry Coalition on Technology Transfer ("ICOTT"), we submit these comments on the interim final rule entitled Revisions to Encryption Items that appeared in the Federal Register for January 14, 2000 (the "Rule"). We commend the Bureau of Export Administration ("BXA") for the significant steps taken in the Rule, which represents a substantial improvement over the regime it replaces. Even with the Rule, however, the regulations still are complex and burdensome for the encryption exporter. Moreover, there is great—and growing—foreign availability of encryption products, such that United States controls are largely ineffective. We urge BXA to refine and improve the control, review, classification and reporting procedures further so that they do not become licensing requirements by another name.

ICOTT's detailed comments on the Rule are attached as a separate document. ICOTT's general comments on the Rule are as follows:

1. The Rule establishes a new category of "retail encryption commodities and software." The definition of "retail" is unduly restrictive and does not reflect the dynamic marketplace for encryption commodities and software. We urge BXA to change the "retail" definition to a "mass market" definition that follows the logic of the mass market criteria set forth in section 211(d)(2) of the Gramm-Enzi bill (S. 1712). Specifically, the determination whether an encryption item has mass market status should take account of the following elements:

- (a) availability for sale in a large volume to multiple potential purchasers;
- (b) wide distribution through normal commercial channels, such as retail stores, direct marketing catalogues, electronic commerce, and other means;

(c) shipment and delivery by generally accepted commercial means of transport; and

(d) usable for normal intended purposes without substantial/specialized support for installation or use.

The revised definition should include within the "mass market" category fifty-six bit products with key exchange mechanisms between 512 and 1024 bits and products that are functionally equivalent to products that have been classified as mass market (per 15 C.F.R. § 740.17(a)(3)(iv) and (vii)).

We recognize that our proposed definition is inconsistent with the current Wassenaar Arrangement definition and accordingly we urge the Administration to seek to make that definition consistent with the one set out above.

2. The structure of the regulations is overly complex and in many ways unrealistic. The regulations apply to twelve distinct product groups, each governed by separate rules with which exporters must comply. This is unnecessarily confusing for even expert compliance personnel of major multinational companies, much less for small businesses or for foreign reexporters. For example, there should be only one set of rules for all products with encryption key lengths of sixty-four bits or less, and rules for publicly available source code and object code should apply to encryption items in the same way as for non-encryption products (putting them outside the scope of the EAR instead of under License Exception TSU or ENC). The estimated times in the Rulemaking Requirements section of this Rule grossly underestimate exporters' burdens to learn these rules and complying with them in their current form. For example, while it may take only five minutes to complete a notification of source code being made available on the Internet for export under License Exception TSU, that short time only comes after hours of education and application of the rules to particular products. Rather than four hours to complete semi-annual reporting requirements, we estimate that it will take each exporter hundreds, if not thousands, of hours to educate the necessary personnel, determine which products will require which type of reports, set up systems where possible, and gather and consolidate the information for the submission to the BXA. This time could be spent far more productively by our companies.

3. The structure for non-"retail" encryption items allows exports to commercial end users in all but nine countries but prohibits transfers to governments in any country except Canada. This may be the broadest and most difficult to administer end-user and end-use export control ever created. Exporters are doing their best to make sure that they do not export or facilitate exports of such products to governments, but it is unrealistic to expect that governments

will never obtain these products or equivalent products, particularly since the encryption components are often exactly the same as those for retail products. All commercial encryption products should be exportable under the same rules as for ENC retail products. Section 740.17(a)(2) should be revised by [1] removing the phrase "to any individual, commercial firm, or non-government end-user" and [2] striking the remainder of (a)(2) and all of (a)(3), so that it allows exports of reviewed items to any end-user other than those in the nine embargoed and terrorist-supporting countries. That would substantially streamline the Rule and eliminate considerable confusion and wasted resources.

At a minimum the U.S. should match the recent action of the European Union permitting encryption items to be freely exported within a "license free zone" of EU countries (plus ten other countries). U.S. companies will be at a severe disadvantage with their European competitors if such action is not taken promptly. In the Preamble to the Rule, the BXA stated that if the EU took such an action, "the Administration [would] take the necessary steps to ensure U.S. exporters are not disadvantaged." The Administration should take those steps now.

4. EI restrictions should be removed from retail and publicly available items (Sections 734.7, 740.17(a)(3), and others). Such restrictions are unrealistic and are damaging to U.S. competitiveness. Retail items may be exported anywhere in the world except the "terrorist-supporting" countries (currently seven in number), yet these items remain subject to EI controls. Retail items should be removed from EI controls for the following reasons:

- currently, the *de minimis*, "publicly available," and foreign availability rules do not apply to EI-controlled items. These rules have been carefully developed in recognition of the practical and legal (including constitutional) limitations of U.S. export enforcement, and they should be applied to retail encryption items. To do otherwise undermines the Rule and will harm United States competitiveness.
- existing controls on reexports, U.S.-origin content, and direct products will adequately protect the Administration's concerns without creating distrust and raising competitive barriers.
- if there is no *de minimis* exception available for greater-than-64-bit items, foreign manufacturers are likely to eliminate consideration of these U.S.-origin products. Foreign manufacturers will simply design out these components because compliance costs or United States-imposed sales restrictions exceed the value of the item.

Revisions to Encryption Items

May 15, 2000

Page 4

- maintaining EI controls will result in substantial lost sales or will force the continued, unprofitable designing, manufacturing, and marketing of products in domestic and exportable strengths.

5. It is also time to eliminate the ITAR-type controls on technical assistance that apply even when there is no controlled export or reexport. Those provisions—under Section 744.9 of the EAR—no longer serve a useful purpose and are not appropriate for the EAR. They simply inhibit U.S. programmers and other U.S. persons who are aware of them from operating on a level playing field with their counterparts around the world. It is helpful that the Preamble provides that exporters of unrestricted source code are not prohibited from providing technical assistance to foreign customers, but exporters of commercial products should not be inhibited from helping their customers either. Likewise, U.S. users of encryption products should freely be able to tell non-U.S. suppliers of such products how to design their encryption products to meet the U.S. users' needs just as the Commerce Department's National Institute of Standards and Technology (NIST) has been doing with the non-U.S. bidders to supply the U.S. with its Advanced Encryption Standard that will replace DES for U.S. Government use. Now, as NIST found out the hard way, the EAR requires the U.S. user to obtain a license to provide "technical assistance" to non-U.S. persons. The Administration should clearly identify what, if any, purpose the rules prohibiting technical assistance continue to serve (beyond the export control rules) and justify the continuation of these unusual restrictions or, if as we submit they do more harm than good, eliminate them.

6. Open cryptographic interfaces are not permitted for exports under License Exception ENC, but public source code products to build products with open cryptographic interfaces are freely exportable under License Exception TSU, as are publicly available products compiled from such source code. Likewise, non-U.S. source and object code products with open C APIs are freely available around the world. It serves no useful purpose to restrict U.S. exporters from providing such products and thus to require U.S. software developers to undertake more cumbersome and expensive programming than non-U.S. competitors. BXA should eliminate this restriction by deleting Section 740.17(f).

7. The Administration agreed in December 1998 to eliminate all reporting requirements for exports of encryption items under the multilateral export control rules of the Wassenaar Arrangement. Thus, the cumbersome and confusing reporting requirements in this Rule are unilateral controls that burden and add costs to U.S. encryption exporters that are not borne by our non-U.S. competitors. The Administration has not even attempted to explain why there is some benefit to the United States that justifies this burden, opting instead to require U.S. industry to justify why it should not be required to report such encryption exports.

Indeed, the reporting requirements have in some respects become more burdensome and complicated under the Rule. For example, financial encryption software previously was not subject to a reporting requirement. Under the Rule, though, such software may be subject to a reporting requirement if the end user is a non-United States financial institution. In another example, some exports to telecommunications providers and Internet Service Providers ("ISPs") must be reported at the time of export. Similarly, exports of certain types of encryption source code must be reported to the BXA "by the time of export." We doubt that the benefit to the government of receiving such reporting outweighs the burden to exporters of preparing and submitting it. We therefore recommend that reporting of exports made under license exceptions be eliminated. The Rule continues disparities between encryption items that have been "decontrolled" by our allies in the Wassenaar Arrangement, on the one hand, and items that remain controlled by the United States under ECCNs 5A002, 5D002 and 5E002 but are eligible for "streamlined treatment" under License Exception TSU or ENC, on the other. Given the wide—and ever widening—availability of encryption, the United States should not control encryption items (even if they are eligible for license exceptions) that are not controlled by our allies.

8. We commend the BXA for the significant step in the Preamble indicating that foreign-based companies with subsidiaries in the U.S. may apply for ELAs to obtain treatment equivalent to that extended to foreign subsidiaries of U.S. parent companies under Section 740.17(a)(1). We look forward to further steps to ensure "national treatment" for foreign-based enterprises with significant U.S. interests, including large employment, capital investments, technology development and exports.

9. Encryption exporters should be able to self-classify their products just like all other exporters subject to the EAR. The BXA should eliminate the requirement that BXA, rather than the would-be exporter, classify ECCN 5x992 items. This requirement does not exist for other ECCNs.

10. BXA should make clear that redundant classifications are not required for encryption items that have been "decontrolled." For example, the Rule is unclear as to whether a new classification would be required for encryption technology—previously classified under ECCN 5E002—for an item that uses 56-bit encryption that has been "decontrolled." We recommend that the following paragraph be added to Section 742.15(b):

Encryption commodities, software and technology up to and including 56-bits with an asymmetric key exchange algorithm not exceeding 512 bits that were reviewed and classified by BXA prior to January 14, 2000 under ECCNs 5A002, 5D002 or 5E002 and that no longer are controlled by those ECCNs may be classified by exporters under ECCNs 5A992, 5D992 or 5E992 without further review by BXA.

11. The Rule establishes a thirty-day default period for BXA to approve properly submitted classification requests for certain encryption items. If the thirty-day limit is exceeded, the exporter may go ahead and ship the item to non-government end users before the BXA issues the formal classification approval. However, this default rule by its terms applies only to requests for classification under License Exception ENC. We understand that BXA intended to have the thirty-day default rule also apply to classification requests for "NLR" (e.g., classifications for ECCNs 5A992, 5D992, and 5E992) and that BXA is responding to requests from exporters by confirming orally the application of the thirty-day default rule to NLR classifications. This policy should be made clear to all exporters, and the Rule should be amended as soon as possible to reflect this policy.

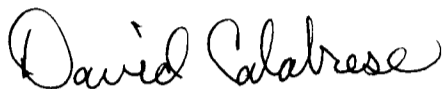
12. As explained in more detail in the attachment, BXA should clarify and/or modify the use of the term "encryption items" to eliminate inconsistencies in the use of the term. In addition, it is not realistic or consistent to maintain EI controls on retail encryption items that may now be exported to most destinations.

As mentioned previously, additional detailed comments on specific provisions of the Rule are attached.

Revisions to Encryption Items
May 15, 2000
Page 7

The Industry Coalition on Technology Transfer (ICOTT) is a group of major trade associations (names listed below) whose thousands of individual member firms export controlled goods and technology from the United States. ICOTT's principal purposes are to advise U.S. Government officials of industry concerns about export controls, and to inform ICOTT's member trade associations (and in turn their member firms) about the U.S. Government's export control activities.

Sincerely,



David Calabrese
Acting Chair, Coordinating Committee



Eric L. Hirschhorn
Executive Secretary

ICOTT Members

- American Electronics Association (AEA)
- American Association of Exporters and Importers (AAEI)
- Electronic Industries Alliance (EIA)
- Semiconductor Equipment and Materials International (SEMI)
- Semiconductor Industry Association (SIA)

DETAILED COMMENTS ON THE REVISED ENCRYPTION REGULATIONS

1. We suggest that, for clarity and completeness, the substantive and interpretive text that appears in the Preamble (e.g., no change in the 5x992 status of message authentication code, password, and authentication items; provision of encryption services by end users of encryption items) also be included in the regulation itself.

2. The designator "EI" serves no apparent purpose, is confusing, and should be dropped. If the designation is retained, the Rule should be amended to clarify that EI applies only to 5x002 items and not to 5x992 items.

EI applies only to encryption items transferred from the U.S. Munitions List ("USML") to the Commerce Control List ("CCL") pursuant to Executive Order 13026 of November 15, 1996, according to 5A002, 5D002, and 5E002 License Requirement Notes. Thus "EI" does not apply to encryption items that were on the CCL before the 1996 transfer. However, nowhere in the EAR is there an identification of which encryption items are EI and which are not. Even an exporter who researches pre-1996 and post-1996 State and Commerce control lists cannot determine which items are EI because unpublished commodity jurisdiction determinations affect what was, or was not, transferred.

It is our understanding that prior to the issuance of the Rule (January 14, 2000), all items transferred in 1996 were controlled by ECCNs 5A002, 5D002, or 5E002 and that the encryption items that were on the CCL before the 1996 transfer were classified to ECCNs 5A992, 5D992, or 5E992. If that is correct, after January 14, 2000, some items that originally were EI items are now properly classified under 5A992, 5D992, or 5E992, because 5A002 coverage was reduced and 5D002 and 5E002 coverage largely is derivative of coverage under 5A002. The statement in 15 C.F.R. § 742.15(a) that EI items "include" those controlled under 5A002, 5D002, and 5E002 seemingly implies that there are also EI items controlled elsewhere. We know of nothing in the EAR, however, to indicate that EI controls apply to items in ECCNs 5A992, 5D992, and 5E992. Moreover, we know of no other categories that include encryption hardware, software, or technology.

Other provisions of the EAR, however, could be read to suggest that EI applies to *all* encryption items, not just those transferred in 1996 or those in the 5x002 categories. Section 742.15(a) states that "EI" stands for "encryption items" and refers the reader to part 772 for the definition of "encryption items." Part 772 in turn defines "encryption items" as including "*all* encryption commodities, software, and technology that contain encryption features and are subject to the EAR" (emphasis added), yet the existence of non-EI encryption categories (namely the 5x992 categories) means that the definition either is overinclusive or inaccurate.

Still other provisions of the EAR are inconsistent as to whether EI covers all, or only some, encryption items. Section 734.3(b)(3) provides that only software controlled for EI reasons under ECCN 5D002 is excepted from the publicly available software exclusion from "subject to the EAR." However, the statement in the note to section 734.3(b)(2) and (b)(3) that encryption source code in electronic form remains subject to the EAR is not limited to EI items or to ECCN 5D002, leaving in doubt whether publicly available non-EI or 5D992 source code in electronic form is subject to the EAR.

Additional provisions of the EAR are confusing as to the consequences of the use of the term "EI." Section 770.2(m) states that software controlled for EI reasons under ECCN 5D002 is eligible for License Exception BAG and, for laptops loaded with encryption software, the tools-of-trade portion of License Exception TMP. Section 770.2(m) is silent as to whether non-EI items under ECCN 5D002, or EI or non-EI items under ECCN 5D992, are eligible for these license exceptions. ECCN 5D992 is not an issue for TMP tools of trade to embargoed countries (§ 740.9(a)(3)(i)(A)) but it is an issue for Syria. Syria and the embargoed countries are generally eligible for License Exception BAG. The section 740.14(f)(3) provision that EI items may not be exported to those countries implies that non-EI items are eligible. Section 740.14(f)(3) does not mention ECCN 5D002; but reading it together with section 770.2(m), which does mention 5D002, leads to the conclusion that the EI portion of 5D992 is also eligible.

Section 740.14(f)(1) provides that only a U.S. citizen or permanent resident may permanently export EI items under License Exception BAG. This leaves open the possibilities that anyone (whether or not a U.S. citizen/permanent resident) may (1) *temporarily* export EI items under License Exception BAG (most baggage exports are temporary); (2) either permanently or temporarily export *non-EI* items under BAG; and (3) (if read together with 770.2(m)) either permanently or temporarily export 5D992 EI items (assuming that any items classified to 5D992 are EI items) under BAG.

3. *Publicly Available.* It seems irrational that printed material setting forth encryption source code qualifies for the "publicly available" exclusion from "subject to the EAR," whereas the same information in electronic form does not (section 734.3(b)(2) and (b)(3) note). See *Junger v. U.S. Department of State*, ___ F.3d ___, 2000 U.S. App. LEXIS 6161, 2000 FED App. 0117p (6th Cir. 2000). Electronic and printed source code both should qualify if they meet the standard criteria for the "publicly available" category.

We appreciate that the proposed regulation permits publicly available source code to be exported freely after notification. 15 C.F.R. § 740.13(e) (License Exception TSU). However, the benefits of this permission are lost by maintaining control over the products of such software. This only ensures that most open source software encryption development will be done outside the United States.

We recommend that BXA either (1) drop all EI controls by deleting the last sentence of Section 734.8(a), with corresponding changes to other sections or (2) remove EI controls from retail items.

4. *Section 740.13.* The first sentence of Section 740.13(d)(2) should be revised to clarify that the other portions of Section 740.13, such as the provisions for bug fixes and sales technical data, continue to be available for encryption software and technology: "This subparagraph (d) is not available"

5. *Section 740.13(e).* We appreciate that published source code may now be exported after notification. However, the provision permitting this should be included in section 734.7 as well as section 740.13(e)(1). Further, there is no rational reason that the section should not also apply to published *object* code. (We note here parenthetically that object code should also be included in the last sentence of Section 740.17(f) and that the cross reference in that sentence should be to Section 734.7.) Further, it is not apparent to us why the T7 countries should be excluded from the "publicly available" rule, as that concept is premised on the assumption that as a practical matter, publicly available information and software cannot be controlled to any destination.

6. *Section 740.17—U.S. Subsidiaries.* "U.S. firm" and "subsidiary of U.S. firm" are not defined. Section 740.17(a)(1) also refers to "foreign subsidiaries of U.S. companies (as defined in Part 772)." However, the term defined in Part 772 is "U.S. subsidiary."

The phrase "their foreign national employees" should be changed to "foreign nationals" to make clear that the deemed export rule does not apply to, for example, consultants, employees of U.S.-based foreign companies, and foreign students.

So as not to disadvantage U.S. subsidiaries, the following phrase should be added at the end of the last sentence of Section 740.17(a)(1): "unless specifically authorized by other provisions of the EAR (e.g., key upgrades, subsequent bundling interpretation)."

7. *Section 740.17—Retail Items.* In subsection (a)(3)(i), the word “sold” should be replaced in all cases with “transferred or to be transferred.” Also, add the words “distributors or resellers” after “retail outlets” to account for different distribution methods and nomenclature.

To allow companies with functionally equivalent products to meet competition, revise subsection (a)(3)(iii) to read: “Note that encryption products not meeting the provisions of (i) and (ii) above but that provide equivalent functionality”

In subsection (a)(3)(iii), delete the modifier “low end” from “servers” and clarify that nothing in this illustrative list restricts products that meet the criteria of (a)(3)(i) and (ii) from being classified as “retail.” Alternatively, subsection (a)(3)(iii) might be moved to the Supplementary Information section to avoid any inference that it presents an additional set of technical criteria.

8. *Section 740.17—Classifications and Key Lengths.* Classification of items with various key lengths is confusing, especially for 64-bit products. We understand that the Wassenaar language creates much of this confusion by setting general decontrol levels at 56 bits for symmetric keys and 512 bits for asymmetric keys, but allowing mass market decontrol of symmetric keys at 64 bits and of asymmetric keys at any length. Nevertheless, this issue could be more simply addressed. Ideally, since most of these products are decontrolled, they should be removed from EI controls and permitted to be exported under NLR.

A less ideal, but acceptable, option would be to permit 64-bit symmetric (and at least 1024-bit asymmetric) items to be exported under License Exception ENC. This could be accomplished by revising Section 740.17(a)(3)(vii) to state: “Any encryption product with symmetric key of 64 bits or less and a key exchange mechanism up to and including 1024 bits is released from EI controls and may be exported under License Exception ENC. See Section 742.15(b)(1) and Category 5, Part 2 of the CCL for options to classify some such products under ECCNs 5A992, 5D992, or 5E992.” In addition, add the following at the end of Section 742.15(b)(1): “Note that exporters may export any encryption product with a symmetric key of 64 bits or less and a key exchange mechanism up to and including 1024 bits under License Exception ENC (see Section 740.17(a)(3)(vii)).”

To cover upgrades to non-mass market software, the first sentence of section 740.17(e)(3)(i), should be revised as follows: “Mass market commodities and software . . . previously eligible to use License Exception TSU (or for hardware or non-mass market software, ENC)” Preferably, however, this first sentence should be simplified as follows: “Any 56-bit product previously classified as eligible for export under License Exception TSU or ENC may increase key lengths to 64 bits . . . and . . . 1024 bits and remain eligible for export under NLR or ENC as retail products without an additional review.”

It should also be made clear in Section 740.17(e)(2) (and in 742.15(b)(1)) that 56-bit products previously approved for export under TSU or ENC qualify for ECCN 5A992/5D992 or ENC without further review.

9. *Internet or Telecommunications Service Providers.* It is not necessary to single out internet and telecommunications service providers for disparate treatment as is currently done in Section 740.17(a)(4) and it has not been justified as to why exports or reexports to such entities of "network infrastructure products" require reports "by the time of export."

10. *Section 740.17—Reporting.* Exports of retail products should not have to be reported. Section 740.17(g)(1)(iv) should be modified to delete the phrase "exported to individual consumers" and 740.17(g)(2)(ii) should be modified to delete the phrase "if the end user is an individual consumer." Reporting retail product exports requires a tremendous expenditure of private and government resources that is not justified by the meager benefit it may provide to the government.

BXA should clarify reporting of components, source code, and toolkits. Again, these reports do not reflect business models and will impose a substantial burden, particularly for those items sold to, perhaps, thousands of OEMs. We appreciate that the Supplementary Information notes that reporting can be waived on a case-by-case basis. However, we recommend adding the following language to Section 740.17(g)(3): "The requirement to provide non-proprietary descriptions of final products will be waived for components, software, and toolkits constrained by function for use in a particular class of end products. Reporting is not required for products covered by the subsequent bundling interpretation in Section 770.2(n)."

No justification has been shown for imposing a reporting requirement for non-U.S. banks and financial institutions. We therefore strongly urge that reporting requirements for banks, financial institutions, and their customers and contractors be removed.

We continue to be uncertain whether "banking and financial operations" includes communications with customers. We also suggest that "operations" be changed to "matters."

Increase the time for filing reports. The reporting burden is significantly underestimated in the Supplementary Information and the time required to collect information from myriad locations and channels and to prepare the reports will exceed the 30 days permitted in Section 740.17(g)(5). We recommend that the time for reporting be extended to 60 days.

11. *Availability of License Exceptions.* The EAR are silent as to encryption items' eligibility for many license exceptions. Encryption items are explicitly eligible for License

Exceptions KMI, ENC, BAG, the tools-of-trade portion of TMP, and the unrestricted encryption source code portion of TSU. Encryption items are explicitly ineligible for License Exceptions LVS, GBS, CIV, TSR, GFT, the international safeguards and cooperating government portions of License Exception GOV, and the mass market software portion of License Exception TSU. The EAR are silent as to whether encryption items are eligible for any other license exceptions.

The additional exceptions that are appropriate for encryption item eligibility include: RPL; APR; the remainder of TMP (i.e., in addition to tools of trade and to a U.S. subsidiary); the U.S. Government and Chemical Weapons Convention portions of GOV; operation, sales, and software update portions of TSU; and equipment and spare parts for a vessel or aircraft portion of AVS.

One might conclude that License Exceptions do apply when they are silent. Section 736.1 states: "A person may undertake transactions subject to the EAR without a license or other authorization, unless the regulations affirmatively state such a requirement." On the other hand, it might be argued that this general rule is overridden, at least for software, by the ECCN 5D002 first Note statement that encryption software is not accorded the same treatment under the EAR as other software.

12. *Section 742.15—Other Issues.* Section 742.15(b)(1)(i) should be revised to be consistent with ECCN 5A002.a.1. The latter (which is identical to Wassenaar entry 5.A.2.a.1) reclassifies from 5A002 to 5A992 equipment having a symmetric algorithm employing a key length in excess of 56 bits or an asymmetric algorithm where the security of the algorithm is based on one of three parameters. Section 742.15(b)(1)(i), on the other hand, transfers only items that include an asymmetric algorithm based on a single, different parameter.

Section 742.15(b)(1) should also explicitly describe the differences between 56-bit and 64-bit products and the key limits affecting each, and why those distinctions exist.

We reiterate a previously made point that Section 742.15(b)(1) should provide that classification requests are optional. Finally, we suggest that Section 742.15(b)(1) be moved to Section 742.15(a) because it reflects decontrol rather than licensing policy for controlled items.

Section 742.15(b)(2) should include a cross reference to License Exception ENC (Section 740.17(a)).

13. *Interpretation: Section 770.2(n).* In the second sentence, following the words "functional encryption capacity," we suggest the insertion of the following parenthetical phrase: "(i.e., confidentiality algorithm or key exchange mechanism)." Also, to clarify what we believe to be a widespread misunderstanding about "crypto aware" products, we suggest the addition of

the following sentence: "Products that do not themselves include encryption functions but that make encryption calls to products already classified may be classified under the same category as the product to which they make encryption calls."

We appreciate the clarification in the Supplementary Information regarding the continued exclusion of message authentication code (MAC) and authentication items from 5A002 control. 65 Fed. Reg. at 2494. We suggest that this information should be included in Section 770.2(n) or as a Note to Category 5, Part 2.

It would also be helpful to clarify the status of DVD and MPEG function by including the following sentence in this Section 770.2(n): "The decontrol provisions in Category 5, Part 2 also include items incorporating algorithms for audio/video data which are restricted to performing encrypt and decrypt functions to prevent unauthorized tampering with copy protected data."

14. *Section 772—Definitions.* We recommend that the list of civil end-uses likely to receive favorable consideration (Section 742.15(b)(3)) be removed from that section and added at the end of the definition of "Government End-User" as follows: "... and other entities engaged in civil uses, e.g., the provision of social or financial service to the public, civil justice, social insurance, pensions and retirement, taxes and communications between governments and their citizens."

We also suggest that because the Wassenaar Munitions List is identified in the definition of "Government End-User," it would be useful to include a reference to the Wassenaar web site where that list may be found.

15. *Section 774, Supplement 1.* The decontrol provisions for encryption items now appear in three places: Cryptography Note 3, the Related Controls paragraph under ECCN 5A002, and the technical notes under ECCN 5A002.a.1. Placing excluded items in the Related Controls section in 5A002 is confusing. These items should be moved to a new Note 4, following the Cryptography Note. A cross reference to the technical notes to 5A002.a.1 should also be included there as well.

We have substantial concerns about the removal of subparagraphs (f) and (h) of the current Related Controls under ECCN 5A002, relating to access control devices such as ATMs and point of sale terminals (subparagraph (f)) and equipment for banking and money transactions (subparagraph (h)). We would urge the BXA to confirm that the exceptions for these specific devices mentioned in these previous subparagraphs have been carried forward in the new Rule.

16. *Additional Concerns.* Similar terms appear in section 740.17(a)(3) and the Cryptography Note in part 774. Several of the terms used in these two section are similar, but not identical, and therefore may create needless confusion. Examples include the following:

- "retail selling points" (Part 774) vs. "retail outlets independent of the manufacturer" and "sales directly by the manufacturer for consumer use" (Section 740.17)
- "from stock" (Part 774) vs. "not customized" (Section 740.17)
- "designed for installation by the user without further substantial support by the supplier" (Part 774) vs. "[d]o not require substantial support for installation and use" (Section 740.17)

If these terms are intended to be identical, we suggest that the same term be used in both sections. If not, the reasons for the differences should be explained.

* * *

ENC 18
1 of 6

HOGAN & HARTSON
L.L.P.

DANIEL B. PONEMAN
PARTNER
(202) 637-6904
DBPONEMAN@HHLAW.COM

COLUMBIA SQUARE
555 THIRTEENTH STREET, NW
WASHINGTON, DC 20004-1109
TEL: (202) 637-5600
FAX: (202) 637-5910
www.hhlaw.com

May 15, 2000

Mr. Frank J. Ruggiero
Regulatory Policy Division
Bureau of Export Administration
Department of Commerce
14th Street and Pennsylvania Ave., NW
Room 2705
Washington, D.C. 20230

Dear Mr. Ruggiero:

RE: CSPP Comments on January 14 Encryption Regulation

I am writing on behalf of the Computer Systems Policy Project (CSPP), a coalition of chief executive officers from America's leading information technology companies. CSPP has welcomed the January 14 encryption regulation, which has produced substantial improvement in encryption-related export licensing issues. That said, a number of issues addressed in that January 14 regulation still require further reform, as reflected in the following comments.

1. European Union. In light of the EU decision to provide for license-free treatment for cryptographic products on an EU+10 basis, any revised or subsequent U.S. regulation must fulfill the Administration's January 14 commitment to take the necessary steps to ensure U.S. exporters are not disadvantaged by the EU action. At a minimum we would propose "Canada-like" treatment for all EU countries and any other countries covered by the EU decision. Reliance upon the Canada model for dual-use export licensing has the dual advantages of administrative simplicity and the familiarity of a well-established precedent in the Export Administration Regulations. Prompt U.S. action will be critical to achieving a level playing field to avoid a built-in 30-day headstart for European over American companies due to

BRUSSELS BUDAPEST* LONDON MOSCOW PARIS* PRAGUE* WARSAW

BALTIMORE MD BOULDER, CO COLORADO SPRINGS, CO DENVER, CO LOS ANGELES, CA MCGLEAN, VA NEW YORK, NY

*Affiliated Office

HOGAN & HARTSON L.L.P.
Mr. Frank J. Ruggiero
May 15, 2000
Page 2

different technical review requirements. Such a headstart could be significant in determining success or failure for new product launches or in export bid situations. Moreover, since the EU tends to avoid reporting requirements, viewing them as too cumbersome to be compatible with efficient export controls, the United States should also refrain from imposing any reporting requirements for exports to these countries.

As timing considerations are critical to American competitiveness, CSPP believes that U.S. exporters will be disadvantaged by the EU decision unless the Administration acts decisively and quickly in promulgating a new regulation on this matter. Once a Commission decision is made – even if implementing regulations are not issued at the national level for several months – in practice member state governments will start licensing under the new policy immediately, as U.S. agencies often do. It is therefore important that the Administration publish regulations without delay in order to ensure that there is no further erosion of US competitiveness. ***At a minimum, if new regulations cannot be issued immediately upon announcement of an EU decision, CSPP strongly urges that at that time the Administration announce as a matter of policy that it will accord U.S. exporters the same treatment and that, pending issuance of an implementing regulation, U.S. licensing policy will reflect that decision.***

2. Complexity. The rules are still too complex. Cryptographic products fall into 12 categories – each entailing different treatment under the regulations – depending on whether key lengths are 56 bits, 64 bits, 512 bits, 1024 bits, or whether the product is mass market, retail, etc. At a minimum, all products up to and including 64 bits without regard to key management should be classified under ECCN 5A992 or 5D992. The U.S. should also advocate conforming changes under the Wassenaar Arrangement to assure a level playing field for U.S. companies vis-à-vis foreign competitors. In addition, products that use encryption for network management, where the encryption is not user-accessible, should be removed from EI controls and classified as 5A992 or 5D992. These products (e.g., intrusion-detection systems) use encryption to protect network information to and from a network administrator, and are critical for infrastructure protection.

3. Definitions: Government and Retail. The government should provide greater clarity and guidance with regard to the definitions of "government" and "retail" in the regulation. We note that any regulatory benefit from the stricter treatment for governments under the U.S. regulations will likely be offset by driving government

HOGAN & HARTSON L.L.P.

Mr. Frank J. Ruggiero

May 15, 2000

Page 3

end-users to the broad array of foreign cryptographic products that now compete effectively against U.S. products and solutions.

- Hardware and software appear to be treated differently for purposes of qualifying as "retail" products, contrary to the Administration approach not to discriminate between hardware and software. If a company puts a chip on a motherboard but that chip is unlinked to a particular application, that product should be treated as retail.
- Similarly, if a small server links to ten or 10,000 users, the cryptography is the same, so it seems unfair to preclude large servers from retail treatment. The fact that a particular product is highly scalable (e.g., a large web server), should not disqualify that product from retail classification.
- Scalable products that combine firewall and VPN capabilities in software should be considered "retail". Otherwise, the government will be artificially forcing the market to move toward a model where these capabilities must be bundled into other products, such as operating systems, in order to qualify for retail treatment.
- The "retail" definition should allow for "anticipated sales and transfers", in addition to products sold or transferred. Absence of such a provision will hobble U.S. manufacturers' ability to make large sales in the face of foreign competition.
- The regulation should clarify that increasing a key length of a retail product via a letter does not change the status of the product, i.e. it remains retail.
- The regulation should also avoid product discrimination arising from an exporter choosing to adopt electronic distribution of non-retail software products. The requirement to screen products posted on the web functions as an impediment to the growth of e-commerce. Non-retail products can be posted on the web, but only if the exporter screens for government end-users. EAR Section 734.2(b)(9)(iii)(A) provides for the precautionary measures of screening for foreign government end-users by checking for foreign government domain names (e.g., .gov, .gouv, .mil or similar addresses). In practice, companies lack effective methodology to screen for these names efficiently or effectively. Thus, in order to avoid any risk of noncompliance, exporters will often choose not to post *any* non-retail products on the web for electronic download. Since electronic

HOGAN & HARTSON L.L.P.
Mr. Frank J. Ruggiero
May 15, 2000
Page 4

distribution is a dynamic and emerging trend, this constraint in the regulation will unfairly burden the many companies that are currently trying to shift to a business model that makes use of that form of distribution.

4. *Interfaces, source code, toolkits.* Certain ambiguities in implementation have been identified, and should be clarified in the regulation.

- Once encryption source code is made open source or community source, the CAPIs contained therein can no longer be effectively controlled. Given that fact, it no longer makes sense to subject CAPIs to discriminatory treatment in the regulations. CAPIs should be allowed to be exported under license exception ENC, as would any other cryptographic product.
- More broadly, if the government allows open or community cryptographic source code to be exported with no prior technical review, it should not require technical review of the executables of the same source code. Once an open or community encryption source code is allowed to be exported without prior technical review, the binary form of that same code should receive the same regulatory treatment.
- The regulation should clarify that, in the case of a foreign product developed with or incorporating US-origin encryption source code, components, or toolkits, the product should be exportable and reexportable as a retail product under Sec. 740.17(a)(3) without further review and classification by BXA.
- Exporters should be allowed to export source code without further notice to government if the only change in the product is an increase in key length.
- Continued Administration efforts to constrain OCI exports from the United States, despite allowing source code exports under license exception, will inevitably be to lead independent software vendors to write code to the non-U.S.-origin OCIs, which will be readily available and accessible from foreign manufacturers. The net effect will be to damage the US technology sector, with no apparent gain for national security or law enforcement.

5. *Reporting requirements.* These requirements are still complex and burdensome; they should be reduced. The rulemaking requirement section grossly underestimates the time it takes a large multinational company to compile the reports. One CSPP member company estimates that providing the encryption reports will require over 1000 hours of effort every six months. If the government

HOGAN & HARTSON L.L.P.

Mr. Frank J. Ruggiero

May 15, 2000

Page 5

does not read and analyze all this information, these Administration resources could and should be more effectively deployed elsewhere.

- Since different reporting rules apply depending on the product and/or customer, it is often unclear how to comply with the reporting requirements. For example, the special reporting requirement for the sale of network infrastructure products to telecommunications and Internet service providers is burdensome and should be eliminated.
- Since *bundling of individual products* into retail products has become so extensive, the reporting requirements on such products have the effect of requiring companies to report on virtually all products. There should be no reporting requirements for *any* retail product. Since it is more difficult for companies to differentiate between sales to distributors and individual customers, many exporters are opting for reporting of all sales. For retail products, this is a significant administrative burden.
- Similarly, *commingling of product inventory* makes it very difficult for companies to distinguish between retail products sold directly to a consumer vs. a distributor, reseller, or OEM. Retail sales to consumers, of course, are exempt from reporting; sales to distributors, resellers, and OEMs are not. If for reporting purposes companies commonly commingle these products for either inventory or sales reporting purposes under existing business models, then the logical compliance-based choice is to report on everything retail. Here again, the better approach would be to eliminate reporting on *any* retail product.
- In practice it is difficult to provide a nonproprietary technical description of toolkits. If an exporter does provide such information to BXA, pursuant to Sec. 740.17(g)(3), the regulation should clarify that it is only necessary to provide that information one time, i.e. if different toolkits contain the same cryptographic functionality the exporter does not need to provide the nonproprietary information each time.
- It is also very difficult and, at times, impossible to provide nonproprietary technical descriptions for end products using mass-market encryption components (e.g., chips, open or community source code), given the many customers to whom these components are sold. The regulation should clarify that such reporting is not necessary where (a) nonproprietary technical information is not readily available or collected in the ordinary course of

HOGAN & HARTSON L.L.P.

Mr. Frank J. Ruggiero

May 15, 2000

Page 6

business; or (b) the classification review process already takes account of generic descriptions of the kind of class or end products in which the components are used.

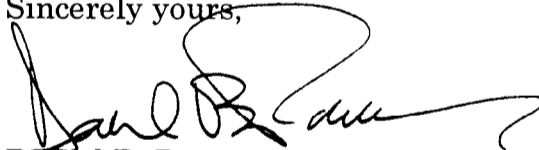
6. *Technical reviews.* These reviews should be accelerated.

- One way to facilitate faster technical reviews would be to reduce their burden on the Administration by requiring only a one-time technical review for products built to a particular encryption specification. This "spec-based" review would require company submission of such data as the product design parameters included in the specification, the standard to be implemented, a description of the related electrical and programmatic interfaces, a list of the types of product applications likely to implement this specification, and the sales channels through which the products would likely be sold (including the extent to which such products would meet the retail definition). Products built to the specification would not be subject to case-by-case technical reviews, provided they conformed to the technical and sales channel parameters detailed in the spec review. Reporting for spec-compliant products would also not be required.
- The regulation should clarify when it is necessary to submit a product developed using publicly-available encryption source code to BXA for a technical review.

7. *Deemed export rule.* While the issue of technology transfers to foreign nationals in the United States was supposed to be resolved favorably by the regulation (i.e. by not treating such transfers as deemed exports), problems have been encountered in implementation (e.g., vis-à-vis contractor employees in the U.S.). The regulation should clarify that outside contractors or consultants (whether natural or juridical persons), co-ops, interns, and temporary employees are eligible for License Exception ENC under the January 14 regulation.

Thank you for your consideration of these comments.

Sincerely yours,



Daniel B. Poneman
Counsel to CSPP

American Electronics Association

Representing the U.S. electronics, software and information technology industries

WWW Address: <http://www.aeanet.org>

5201 Great America Parkway, Suite 520, Santa Clara, CA 95054 Telephone: 408-987-4200 Fax: 408-970-8565

Mailing Address: P.O. Box 54990, Santa Clara, CA 95056-0990

601 Pennsylvania Ave., NW, North Building, Suite 600, Washington, DC 20004 Telephone: 202-682-9110 Fax: 202-682-9111

ENC 19
AEA 10f7

May 15, 2000

Frank J. Ruggiero
Regulatory Policy Division
Bureau of Export Administration
Department of Commerce
14th Street and Pennsylvania Ave., N.W.
Room 2705
Washington, DC 20230

Re: Comments on the Interim Final Rule on Revisions to Encryption Items (65 Fed. Reg. 2492; Jan. 14, 2000)

Dear Mr. Ruggiero:

The American Electronics Association (AEA) is pleased to provide the following comments on the Commerce Department's January interim final regulation affecting exports of encryption items. AEA is a 3,000-member company organization representing the U.S. electronics, software and information technology industries.

AEA and its member companies have worked closely with the government to bring about new and improved rules on the treatment of encryption exports. We believe that the interim rule represents a major step in achieving the type of change that is both necessary and overdue. The new regulation's approach of enabling U.S. companies to export certain widely available encryption products without crippling license requirements and other regulatory restrictions will help to restore the ability of U.S. companies to compete in a global market for encryption.

Despite the constructive thrust of these new rules, further changes and improvements are needed. In many respects, exports of U.S. commercial encryption items remain significantly regulated and restricted under the new rule. Many U.S. exporters continue to face significant and unjustified requirements both before and after exporting. The new rules can be extremely confusing and complex, particularly for small and medium exporters.

The following comments regarding the interim rule address significant issues and shortcomings of the January regulation that, if left unchanged, will present continued and unjustified barriers for U.S. exporters of encryption products and unnecessarily jeopardize U.S. leadership in this important technology.

I. EU Encryption Reforms

Before addressing specific provisions of the rule, AEA would like to emphasize the critical importance of ensuring U.S. competitiveness in the face of major encryption policy reforms that are expected to be adopted by the EU very soon. These reforms will likely create a significant imbalance between U.S. and EU encryption policies. The EU policy changes will apparently permit license-free, review-free exports of unlimited strength encryption to certain nations collectively comprising the vast majority of the global encryption market. These countries are expected to include EU member states as well as ten other countries, including the United States, Canada, Japan, Hungary, the Czech Republic, Poland, Australia, New Zealand, Norway, and Switzerland.

The interim rule anticipated this development, stating that the Administration will take necessary steps to ensure that U.S. exporters are not disadvantaged by this new authorization for EU exporters. These "necessary steps" will have to be devised and implemented rapidly in order to limit adverse competitive effects on U.S. suppliers of encryption. Allowing this policy imbalance to languish will permit EU suppliers to more reliably service foreign customers. In response to the EU's latest policy change, AEA urges the Administration to quickly implement "Canada-like treatment" of U.S. encryption exports to the EU plus eight other non-EU countries (excluding Canada and the United States). The United States should also follow the same approach with respect to any future liberalization of this magnitude that takes place on a bilateral or other multilateral basis.

II. "Retail" Label

Despite substantial improvements in how the new rules define "retail" encryption items, including an illustrative list, AEA objects to maintaining "retail" as the standard for accessing the broadest form of encryption decontrol. The interim rule correctly includes in the retail category ostensibly non-retail encryption items, such as chips, that are nevertheless sold in high volume through mass market means. This leads to confusion and uncertainty on the part of exporters and marks a major disconnect in the regulation.

When determining which encryption items merit the broadest form of decontrol, the new rules should principally consider the extent to which an item is unsusceptible and unworthy of export licensing and other controls. As AEA has advocated in the past, this ought to be a mass market, rather than a retail, test. The basic elements of the test should include high-volumes, sales through retail and/or other commercial channels, and the ability to use the product without substantial support.

The interim rule has indeed moved towards, though not in name, a mass market test. AEA suggests that the next logical step is to replace the "retail" label with "mass market" and thereby bring consistency, clarification, and greater integrity to this important aspect of the new rule.

III. Specification-Based Reviews

A shortcoming of the current classification review process is the need to individually subject those products that are based on the same overall encryption specification to one-time reviews. As an alternative, AEA proposes that there be a single classification review for a particular encryption specification (e.g., Bluetooth) that would take into consideration the types of products and applications that would be built to that specification. This approach would preclude the need for individual assessments on many products that all operate on the same basic standard.

Knowledge of an underlying encryption specification and its technical aspects is a sufficient indicator of an associated product's cryptographic capabilities and features. While finished products may vary by use, application, customer and the like, a review of the underlying specification can show the inherent technical constraints associated with those products. For example, the specification can require electrical and programmatic interfaces that by their nature can limit the encryption functionality of products rendered therefrom.

Under this specification-based approach, the government should rely on the following information:

- (1) technical descriptions of encryption hardware design parameters that uniquely identify the design and describe its functionality;
- (2) the relevant encryption standard;
- (3) a description of the electrical and programmatic interfaces;
- (4) likely types of product applications; and
- (5) likely sales channels and customer types.

With this information, the government requirement for having technical data on U.S. encryption products on the world market would be satisfied. It should also provide a basis for determining whether the products rendered from the specification will have retail status. Individual reviews of such products would therefore not be necessary. A review would only become necessary to the extent a product exceeded the design/marketing parameters laid out in the "spec review." Additionally, by providing representative sales and marketing data during the spec review, an exporter would not need to engage in post-export reporting for products utilizing approved specifications.

IV. Export Reporting Requirements

Retail items. The interim rule's maintenance of reporting requirements on certain retail encryption items -- notably those sold through distributors and resellers -- is extremely burdensome and unjustified and should be ended. By regulatory definition, retail encryption items are sold in large volume without restriction, cannot be easily altered, do not require meaningful outside support, and are designed for individual consumers. By

all accounts, it is highly unreasonable and unnecessary to attempt to track such products through periodic reporting.

Not only do retail reporting requirements offer little if any value to export control authorities, they also present a variety of operational and competitive issues for exporters. For example, products for sale to individual consumers can be commingled along with items destined for resellers or OEMs, thereby compelling exporters to shoulder the burden of reporting on all retail items to ensure compliance.

AEA strongly recommends that all retail encryption items be exempt from any export reporting. Potentially relevant product or customer information (e.g., types of retail channels/customers and approximate quantities) could be provided up-front during the classification review.

Components, Source Code and Toolkits. Under the interim rule, special reporting requirements apply to encryption components, source code and toolkits sold directly to manufacturers. These requirements, including the need to provide technical descriptions of the end products, present major difficulties for exporters due to the often very high number of OEM customers who are spread around the world and the unorthodox requests this rule would entail. The requirement should be clarified to allow for an exemption from reporting whenever non-proprietary technical descriptions of end items are not readily available or collected in the ordinary course of business. A reporting exemption should also be allowed when an exporter can provide up-front in the classification review process a generic description of the kind of class of end products in which the components are used.

The interim rule in part recognizes the problematic issues presented by this requirement and provides that reporting on components can be adjusted on a case-by-case basis to deal with this issue. AEA suggests that this provision, currently residing in the interim rule's preamble, be made part of the actual regulatory language and be expanded to include encryption source code and toolkits.

Foreign Banks and Financial Institutions. The current exemption from reporting for sales to U.S. banks and financial institutions should be fully extended to equivalent foreign institutions. The existing distinction presents an unjustified rollback of prior reforms and should be eliminated.

Network Infrastructure Products. The interim rule's requirement that exports of network infrastructure products be reported at the time of shipment is excessive and unnecessary. Such products merit treatment similar to other encryption items.

V. Removal of EI Controls

EI controls should no longer apply to retail encryption items now that these items are freely exportable to nearly all customers and destinations. When subject to EI controls,

items face additional restrictions and are excluded from several important provisions, including de minimis, foreign availability, and public availability treatment. Retail encryption items appropriately have been freed of nearly all licensing restrictions. It would be unnecessary and costly to nevertheless maintain special EI restrictions on such items.

VI. De Minimis Treatment for EI Controlled Commodities

To the extent that certain encryption items remain under EI controls, it is equally important that these items receive de minimis treatment. Such treatment, which recognizes that an item falling under a certain level of overall product content is not worthy of control, should not be based upon the reason for control. Rather, it should strictly be based on the underlying rationale of the de minimis provision. Therefore, whether or not EI-controlled, all encryption items should be eligible for de minimis treatment.

Maintaining U.S. controls on foreign-produced end-items that incorporate U.S. encryption items, regardless of the level of the content, is a mistake that has and will continue to harm U.S. producers. Foreign manufacturers will have a strong incentive to look beyond U.S. suppliers for encryption components and parts. The interim rule states that, while foreign-produced items incorporating U.S. encryption are subject to the EAR, they will not need to receive prior U.S. authorization for export from the foreign country. This is a helpful yet inadequate solution to the de minimis issue. A de minimis rule must be made eligible for all encryption items.

VII. Open Cryptographic Interfaces

Open cryptographic interfaces should be eligible under new license exception ENC. The interim rule's exclusion of these products is impractical and likely to be very costly to U.S. exporters. While the U.S. appropriately allows license-free and review-free exports of open cryptographic source code, code executables remain subject to strict controls. This is an unjustified and unnecessary policy that will cost U.S. exporters considerable export opportunities. Special restrictive treatment for open cryptographic interfaces should be deleted from throughout the interim rule.

VIII. Technical Assistance

Controls on technical assistance for encryption items should be removed. Currently, exporters face the prospect that technical assistance may be licensable even when the encryption item or technology at issue is freely exportable. Exporters should be permitted to offer technical assistance relative to their products and technology without having to secure prior authorization.

IX. Electronic Distribution of Non-Retail Software Products

The requirement to screen against government end-users for electronic distribution of non-retail software products should be eliminated. While these products can be posted on the web, companies must comply with the requirement under Section 734.2(b)(9)(iii)(A) to conduct reverse dns against .gov, .gouv, .mil or similar addresses. The problem with this requirement is the lack of an effective screening methodology, which is due in part to the complexity of making the "government" determination for any given end-user. In fact, most companies find that this is just not practicable. An inability to screen efficiently or effectively means that companies have to play it safe and simply not post non-retail products on the web for electronic download.

Many companies are currently trying to shift to a business model that uses an electronic means of distribution. The regulations should not impede this growing trend.

X. Additional Issues

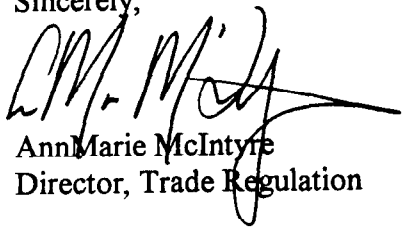
- Retail encryption software should be included as one of the items exempt from download restrictions and requirements under section 734.2.
- The regulations should clarify that the authorization under ENC to transfer encryption technology to foreign national employees in the United States for internal company use should also include contractors, interns, and certain other workers. The current formulation is too narrow.
- In addition to removing the special reporting requirements for network infrastructure products, across-the-board exclusion of such products from the retail category should be eliminated. These types of items are readily available outside the United States and can be easily scaled-up from other widely available products. As with most other encryption items, network infrastructure products should be reviewed on a case-by-case basis for retail status.
- The regulations should re-visit the pressing issue of extending not just parity but equal licensing treatment to responsible foreign headquartered enterprises with significant U.S. presence.
- A new paragraph should be added to Section 742.15(b) of the Bureau of Export Administration (BXA) regulations, as follows:

Encryption commodities, software and technology up to and including 56-bits with an asymmetric key exchange algorithm not exceeding 512 bits that were reviewed and classified by BXA prior to January 14, 2000 under ECCNs 5A002, 5D002 or 5E002 may be classified and exported under ECCNs 5A992, 5D992 or 5E992, without further review by BXA.

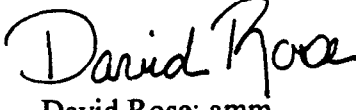
This change makes clear that a duplicative BXA review is not necessary for items that have previously been classified as 'EI' items, but now clearly fall outside of 'EI' controls under the new BXA regulations. The interim final regulations are ambiguous on this point.

Thank you for your time and consideration of these comments.

Sincerely,



AnnMarie McIntyre
Director, Trade Regulation



David Rose: amm
AEA Encryption Work Group Chairman