DEPARTMENT OF COMMERCE

Bureau of Export Administration

15 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 for 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 56-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, 725 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.*; 50 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.*; 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).

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

Authority: 50 U.S.C. app. 2401 *et seq.*; 50 U.S.C. 1701 *et seq.*; 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 Commercial 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 for 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-uses 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

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

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

Document No. 164