Billing Code: 3510-33-P

DEPARTMENT OF COMMERCE

Bureau of Export Administration

15 CFR Parts 730, 732, 734, 736, 738, 740, 742, 744, 748, 750, 768, 772, and 774

[Docket No. 960918265-6366-03]

RIN 0694-AB09

Encryption Items Transferred from the U.S. Munitions List to the Commerce Control List

AGENCY: Bureau of Export Administration, Commerce

ACTION: Interim rule.

SUMMARY: This interim rule amends the Export Administration Regulations (EAR) by exercising jurisdiction over, and imposing new combined national security and foreign policy controls on, certain encryption items that were on the United States Munitions

List, consistent with Executive Order 13026 and pursuant to the Presidential Memorandum of that date, both issued by President Clinton on November 15, 1996.

On October 1, 1996, the Administration announced a plan to make it easier for Americans to use stronger encryption products to protect their privacy, intellectual property and other valuable information. The plan envisions a worldwide key management infrastructure with the use of key escrow and key recovery encryption items to promote electronic commerce and secure communications while protecting national security and public safety. To provide for a transition period for the development of this key management infrastructure, this rule permits the export and reexport of 56-bit key length DES or equivalent strength encryption items under the authority of a License Exception, if an exporter makes satisfactory commitments to build and/or market recoverable encryption items and to help build the supporting international infrastructure. This policy will apply to hardware and software.

DATES: Effective Date : This rule is effective (DATE OF PUBLICATION).

Comment Date : (45 DAYS AFTER DATE OF PUBLICATION).

ADDRESSES: Written comments (six copies) should be sent to: Nancy Crowe, Regulatory Policy Division, Bureau of Export Administration, Department of Commerce, 14th Street and Pennsylvania Ave., N.W., Room 2705, Washington, D.C. 20230.

FOR FURTHER INFORMATION CONTACT: James A. Lewis, Office of Strategic Trade and Foreign Policy Controls, Telephone: (202) 482-0092.

SUPPLEMENTARY INFORMATION:

Background

Following upon the Administration's October 1 announcement, on November 15, 1996, the President issued the Memorandum directing that all encryption items controlled on the U.S. Munitions List, except those specifically designed, developed, configured, adapted, or modified for military applications, be transferred to the Commerce Control List. The Memorandum and Executive Order 13026 (November 15, 1996, 61 FR 58767) also set forth certain additional provisions with respect to controls on such encryption items to be imposed by the Department of Commerce. The Executive Order also provides for appropriate controls on the export and foreign dissemination of encryption items controlled on the U.S.

Munitions List that are placed on the Commerce Control List. In issuing the Memorandum the President stated:

> Encryption products, when used outside the United States, can jeopardize our foreign policy and national security interests. Moreover, such products, when used by international criminal organizations, can threaten the safety of U.S. citizens here and abroad, as well as the safety of the citizens of other countries. The exportation of encryption products must be controlled to further U.S. foreign policy objectives, and promote our national security, including the protection of the safety of U.S. citizens abroad.

This initiative will support the growth of electronic commerce; increase the security of the global information infrastructure; protect privacy, intellectual property and other valuable information; and sustain the economic competitiveness of U.S. encryption product manufacturers during the transition to a key management infrastructure. Under this initiative, non-recoverable encryption items up to 56-bit key length DES or equivalent strength will be permitted for export and reexport after a one-time review of the strength of the item and if the exporter makes satisfactory commitments to build and/or market

recoverable encryption items, to support an international key management infrastructure. This policy will apply to hardware and software and will last through December 31, 1998.

The initiative addresses important foreign policy and national security concerns identified by the President. Export controls on cryptographic items are essential to controlling the spread abroad of powerful encryption products which could be harmful to critical U.S. national security, foreign policy and law enforcement interests. This initiative will preserve such controls and foster the development of a key management infrastructure necessary to protect important national security, foreign policy and law enforcement concerns.

Encryption software 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. As the President indicated in E.O. 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 other software regulated under the EAR.

The government recognizes that several factors, including the development of common international encryption policies, the need for an international key recovery infrastructure, and technological change, will influence market development in key recovery products. At the same time, the government is committed to a two-year transition period. The government will continually evaluate progress towards key recovery throughout and beyond the two-year period and will tailor the implementation of its policies in consultation with the public.

This interim rule implements the Administration's policy on encryption exports and reexports. This rule amends the Export Administration Regulations (EAR) by imposing national security and foreign policy controls ("EI" for Encryption Items) on certain information security systems and equipment, cryptographic devices, software and components specifically designed or modified therefor, and related technology ("encryption items"). "Encryption items" subject to the EAR do not include encryption items specifically designed, developed, configured, adapted or modified for military applications (including command, control and intelligence applications). Such items remain on the U.S.

Munitions List, and continue to be controlled by the Department of State, Office of Defense Trade Controls. EI controls apply to encryption software 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 the same date.

This interim rule also amends the Export Administration Regulations by requiring a license for exports and reexports to all destinations, except Canada, of certain encryption items controlled for EI reasons. 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. Exporters should allow 40 days for the processing of licenses, consistent with E.O. 12981. The licensing policy is as follows:

(1) Certain mass-market encryption software. Certain encryption software that was 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 may be released from “EI” controls and thereby made eligible for mass market treatment after a one-time BXA review. To determine eligibility for mass market treatment,

exporters must submit a classification request to BXA. 40-bit mass market encryption software may be eligible for a 7-day review process, and company proprietary software may be eligible for 15-day processing. See new Supplement No. 6 to part 742 and §748.3(b)(3) for additional information. Note that the one-time review is for a determination to release encryption software in object code only. Exporters requesting release of the source code should refer to paragraph (b)(3)(v)(E) of Supplement No. 6 to part 742. If, after a one-time review, BXA determines that the software is released from EI controls, such software is eligible for all provisions of the EAR applicable to other software, such as License Exception TSU for mass-market software. If BXA determines that the software is not released from EI controls, a license is required for export and reexport to all destinations, except Canada, and license applications will be considered on a case-by-case basis.

(2) Key Escrow, Key Recovery and Recoverable encryption software and commodities . Recovery encryption software and equipment controlled for EI reasons under ECCN 5D002 or under ECCN 5A002, including encryption equipment designed or modified to use recovery encryption software, may be made eligible for License Exception KMI after a one-time BXA review. License Exception KMI is available for all destinations except Cuba, Iran, Iraq, Libya, North Korea, Syria and Sudan. To determine

eligibility, exporters must submit a classification request to BXA. Requests for one-time review of key escrow and key recovery encryption products will receive favorable consideration provided that, prior to the export or reexport, a key recovery agent satisfactory to BXA has been identified (refer to new Supplement No. 5 to part 742) and security policies for safeguarding the key(s) or other material/information required to decrypt ciphertext as described in Supplement No. 5 to part 742 are established to the satisfaction of BXA and are maintained after export or reexport as required by the EAR. If the exporter or reexporter intends to be the key recovery agent, then the exporter or reexporter must meet all of the requirements of a key recovery agent identified in Supplement No. 5 to part 742. In addition, the key escrow or key recovery system must meet the criteria identified in Supplement No. 4 to part 742. Note that eligibility is dependent on continued fulfilment of the requirements of a key recovery agent identified in Supplement No. 5 to part 742. Since the establishment of a key management infrastructure and key recovery agents may take some time, BXA will, while the infrastructure is being built, consider exports of key recovery encryption products which facilitate establishment of the key management infrastructure before a key recovery agent is named, consistent with national security and foreign policy. When BXA approves such cases, exporters of products described in Supplement No. 4 to part 742 are required

to furnish the name of an agent by December 31, 1998. Requests for one-time review of recoverable products which allow government officials to obtain, under proper legal authority and without the cooperation or knowledge of the user, the plaintext of the encrypted data and communications will also receive favorable consideration.

(3) Non-recovery encryption items up to 56-bit key length DES or equivalent strength supported by a satisfactory business and marketing plan for exporting recoverable items and services. Manufacturers of non-recovery encryption items up to 56-bit key length DES or equivalent strength will be permitted to export and reexport under the authority of License Exception KMI, provided that the requirements and conditions of the License Exception are met. Exporters must submit a classification request for an initial BXA review of the item and a satisfactory business and marketing plan that explains in detail the steps the applicant will take during the two-year transition period beginning January 1, 1997 to develop, produce, and/or market encryption items and services with recoverable features. Producers would commit to produce key recovery products. Others would commit to incorporate such products into their own products or services. Plans will be evaluated in consideration of good faith efforts by the exporter to promote key recovery products and infrastructure. Such efforts can include: the scale of key recovery research and

development, product development, and marketing plans; significant steps to reflect potential customer demand for key recovery products in the firm's encryption-related business; and how soon a key recovery agent will be identified. Note that BXA will accept requests for classification of non-recoverable encryption items up to 56-bit key length DES or equivalent strength under this paragraph from distributors, re-sellers, integrators, and other entities that are not manufacturers of the encryption items. The use of License Exception KMI is not automatic; eligibility must be renewed every six months. Renewal after each six-month period will depend on the applicant's adherence to explicit benchmarks and milestones as set forth in the plan approved with the initial classification request and amendments as approved by BXA. This relaxation of controls and use of License Exception KMI will last through December 31, 1998. The plan submitted with classification requests for the export of non-recoverable encryption items up to 56-bit key length DES or equivalent strength must include the elements in new Supplement No. 7 to part 742. Note that distributors, re-sellers, integrators, and other entities that are not manufacturers of the encryption items are permitted to use License Exception KMI for exports and reexports of such items only in instances where a classification has been granted to the manufacturer of the encryption items. The authority to so export or reexport will be

for a time period ending on the same day the producer's authority to export or reexport ends.

Exporters authorized to export 56-bit DES or equivalent strength non-key recovery products in exchange for commitments to key recovery will be allowed to service and support the customers of those products during and after the two-year period. Support and service includes maintenance or replacement of products to correct defects or maintain existing functionality. It also includes upgrades that do not increase the strength of the encryption in the product.

Exporters authorized to export 56-bit DES or equivalent strength non-key recovery products during the interim period may also export under a license additional quantities of those 56-bit DES or equivalent strength non-key recovery products after the two-year period to existing customers. Such sales may be made to the customers of any exporter that was authorized to export such products in exchange for key recovery commitments during the two-year period. The additional quantities sold may not be disproportionate to the customer's embedded base.

(4) All other encryption items .

(i) Encryption licensing arrangement . This is intended to continue without change the regulatory treatment of the distribution and warehouse arrangements currently permitted under the International Traffic in Arms Regulations. Applicants may submit license applications for exports and reexports of certain encryption commodities and software in unlimited quantities for all destinations except Cuba, Iran, Iraq, Libya, North Korea, Syria, and Sudan. Applications will be reviewed on a case-by-case basis. Encryption licensing arrangements may be approved with extended validity periods specified by the applicant in block #24 on Form BXA-748P. In addition, the applicant must specify the sales territory and classes of end-users. Such licenses may require the license holder to report to BXA certain information such as item description, quantity, value, and end-user name and address.

(ii) Applications for encryption items not authorized under an encryption licensing arrangement . Applications for the export and reexport of all other encryption items will be considered on a case-by-case basis.

(5) Applications for encryption technology . Applications for the export and reexport of encryption technology will be considered on a case-by-case basis.

Note that all “EI” encryption items are not subject to any mandatory foreign availability procedures of the EAA or the EAR. In section 1(a) of Executive Order 13026, the President states:

> I have determined that the export of encryption products described in this section may 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 subject to public disclosure or judicial review without revealing or implicating classified information that could harm United States national security and foreign policy interests. Accordingly, section 4(c) and 6(h)(2) - (4) of the Export Administration Act of 1979 ("the EAA") ..., all other analogous provisions of the EAA relating to foreign availability, and the regulations in the EAR relating to such EAA provisions, shall not be applicable with respect to export controls on such encryption products.

This interim rule amends part 768, Foreign Availability, to make clear that the provisions of that part do not apply to encryption items transferred to the Commerce Control List.

This interim rule also amends part 734 to exclude encryption items transferred from the U.S. Munitions List to the Commerce Control List consistent with E.O. 13026 (61 FR 58767, November 15, 1996) and pursuant to the Presidential Memorandum of that date from the de minimis provisions for items exported from abroad. This rule also amends part 734 of the EAR to reflect that encryption software controlled for EI reasons under ECCN 5D002 that has been transferred to the Department of Commerce from the Department of State by Presidential Memorandum will be subject to the EAR even when publicly available. A printed book or other printed material setting forth encryption source code is not itself subject to the EAR (see §734.3(b)(2)). However, notwithstanding §734.3(b)(2), encryption source code in electronic form or media (e.g., computer diskette or CD ROM) remains subject to the EAR (see §734.3(b)(3)). The administration continues to review whether and to what extent scannable encryption source or object code in printed form should be subject to the EAR and reserves the option to impose export controls on such software for national security and foreign policy reasons. Note that there is a new definition of “export of encryption source code and object code software” (see §734.2(b)(9)).

This rule creates a new License Exception KMI for exports of certain encryption software and equipment. This rule also amends

part 740 and Supplement No. 2 to part 774 to reflect that encryption software will not be eligible for “mass market” treatment under the General Software Note or for export as beta-test software under License Exception BETA unless released from EI controls through a one-time BXA review (refer to new Supplement No. 6 to part 742). Encryption items transferred from the USML to the CCL prior to November 15, 1996 are not controlled for EI reasons. Note that License Exception TMP is available for temporary exports and reexports of encryption items except under the provisions for beta-test software. License Exceptions TMP and BAG effectively replace the Department of State’s personal use exemption. Software and technology that was controlled by the Department of Commerce prior to (DATE OF PUBLICATION) are not affected by this rule and will continue to be eligible for the publicly available treatment. Software controlled by the Department of Commerce prior to (DATE OF PUBLICATION) will continue to be eligible for mass market treatment under the General Software Note, and License Exception TSU for mass-market software.

For purposes of this rule, “recovery encryption products” refers to encryption products (including software) that allow government officials to obtain under proper legal authority and without the cooperation or knowledge of the user, the plaintext of encrypted data and communications. Such products fulfill the objectives of

the Administration’s encryption policy. Other approaches to access and recovery may be defined in the future.

This interim rule also amends part 742 to reflect the new combined national security and foreign policy controls imposed by this rule, and adds a new Supplement No. 4 titled “Key Escrow or Key Recovery Products Criteria” that includes product criteria, a new Supplement No. 5 titled “Key Escrow or Key Recovery Agent Criteria, Security Policies, and Key Escrow or Key Recovery Procedures” that includes interim requirements for key recovery agents, a new Supplement No. 6 titled “Guidelines for Submitting a Classification Request for a Mass Market Software Product that contains Encryption” that includes the criteria for the one-time review of classification requests for release of certain encryption software from EI controls, and a new Supplement No. 7 titled “Review Criteria for Exporter Key Escrow or Key Recovery Development Plans.”

This interim rule also amends part 744 to add a general prohibition in §744.9 with respect to technical assistance in the development or manufacture abroad of encryption commodities and software controlled for EI reasons and makes conforming changes throughout the EAR.

This interim rule makes conforming changes in part 748 for classification requests, amends part 750 of the EAR to reflect the Department of Justice role in the review of encryption license applications, adds new definitions to part 772, and amends the Commerce Control List (Supplement No. 1 to part 774) by adding new EI controls under ECCNs 5A002, 5D002, and 5E002 for commodities, software and technology that are placed under Commerce Department jurisdiction, consistent with E.O. 13026, by Presidential Memorandum.

In certain cases, semiannual reporting requirements on quantities shipped and country of destination will be imposed on exporters, in order to allow the United States to fulfill the reporting requirements of its international obligations, such as the Wassenaar Arrangement.

The scope of controls on the release to foreign nationals of technology and software subject to the EAR may be amended in a separate Federal Register Notice.

This rule involves no new curtailment of exports, because the transfer or removal of items from the United States Munitions List to the CCL maintains a continuity of controls. Therefore, the provisions regarding the impact of new controls do not apply,

and contract sanctity also does not apply to this imposition of controls.

U.S. persons holding valid USML licenses and other approvals issued by the Department of State prior to (DATE OF PUBLICATION) may ship remaining balances authorized by such licenses or approvals under the authority of the EAR by filing Shippers Export Declarations (SEDs) with District Directors of Customs, citing this Federal Register Notice and the State Department license number. Such shipments shall be in accordance with the terms and conditions, including the expiration date, existing at the time of issuance of the State license. Any reports required for distribution and other types of agreements previously authorized by the Department of State, valid at the time of this publication, should be henceforth submitted to the Department of Commerce. Actions pending at the Department of State on (DATE OF PUBLICATION), including pending license applications, must be refiled with the Department of Commerce. Export violations, including the terms and conditions of export, shall hereafter constitute a violation of the EAR.

Consistent with the provisions of section 6 of the Export Administration Act, a foreign policy report was submitted to Congress on December 24, 1996, notifying the Congress of the Department's intention to impose controls on certain information

security systems and equipment, cryptographic devices, software and components specifically designed or modified therefor, and related technology that will be controlled on the CCL and that will be subject to new control procedures.

Although the Export Administration Act (EAA) expired on August 20, 1994, the President invoked the International Emergency Economic Powers Act and continued in effect, to the extent permitted by law, the provisions of the EAA and the EAR in Executive Order 12924 of August 19, 1994, notice of August 15, 1995 (60 FR 42767), and notice of August 14, 1996 (60 FR 42527).

Rulemaking Requirements

1. This interim rule has been determined to be significant for purposes of E.O. 12866. A cost benefit analysis has been prepared and is available upon request by contacting James A. Lewis at (202) 482-0092.

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 0694-0048 and 0694-0088. This rule also contains a new collection-of-information requirement subject to the PRA that has received emergency approval under OMB control number 0694-0104. The new information requirement and estimated public burden hours include: marketing plans (40 hours each); semiannual progress reports (8 hours each); safeguard procedures (4 hours); recordkeeping (2 hours); and annual reports (4 hours). These estimates include the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collections of information. Send comments regarding these burden estimates or any other aspect of these collections of information, including suggestions for reducing the burden, to OMB Desk Officer, New Executive Office Building, Washington, DC 20503.

3. This rule does not contain policies with Federalism implications sufficient to warrant preparation of a Federalism assessment under Executive Order 12612.

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 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 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 these regulations, this rule is issued in interim form and comments will be considered in the development of final regulations. Accordingly, the Department 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 (45 DAYS AFTER DATE OF PUBLICATION). 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 person 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.

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. Communications from agencies of the United States Government or foreign governments will not be made available for public inspection.

The public record concerning these regulations will be maintained in the Bureau of Export Administration Freedom of Information Records Inspection Facility, Room 4525, Department of Commerce, 14th Street and Pennsylvania Avenue, N.W., Washington, D.C. 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 Margaret

Cornejo, Bureau of Export Administration Freedom of Information Officer, at the above address or by calling (202) 482-5653.

This rule has been determined to be a major rule as defined in 5 U.S.C. § 804(2) for purposes of Congressional review under 5 U.S.C. ch. 8. Notwithstanding 5 U.S.C. § 801(a)(3), this rule is effective (DATE OF PUBLICATION) pursuant to authority at 5 U.S.C. § 808(2) as there is good cause to waive the requirement to provide notice and public procedure thereon. This action implements an Administration initiative that is intended to protect the national security and foreign policy interests of the United States and streamlines export controls for encryption items. Therefore, notice and public procedure that would delay implementation of this rule is contrary to the public interest.

List of Subjects

15 CFR Part 730

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

15 CFR Parts 732, 740, 748, 750, and 768

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

15 CFR Part 734

Administrative practice and procedure, Exports, Foreign trade.

15 CFR Parts 736, 738, 742, 772, and 774

Exports, Foreign trade.

15 CFR Part 744

Exports, Foreign trade, Reporting and Record keeping requirements.

Accordingly, parts 730, 732, 734, 736, 738, 740, 742, 744, 748, 750, 768, 772, and 774 of the Export Administration Regulations (15 CFR Parts 730-799) are amended as follows:

1. The authority citation for 15 CFR part 730 is revised 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; Sec. 201, Pub. L. 104-58, 109 Stat. 557 (30 U.S.C. 185(s)); 30 U.S.C. 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. 11912, 41 FR 15825, 3 CFR, 1976 Comp., p. 114; E.O. 12002, 42 FR 35623, 3 CFR, 1977 Comp., p.133; E.O. 12058, 43 FR 20947, 3 CFR, 1978 Comp., p. 179; E.O. 12214, 45 FR 29783, 3 CFR, 1980 Comp., p. 256; E.O. 12851, 58 FR 33181, 3 CFR, 1993 Comp., p. 608; E.O. 12867, 58 FR 51747, 3 CFR, 1993 Comp., p. 649; E.O. 12918, 59 FR 28205, 3 CFR, 1994 Comp., p. 899; E.O. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; E.O. 12938, 59 FR 59099, 3 CFR, 1994 Comp., p. 950; Executive Order 13026 (November 15, 1996, 61 FR 58767); Notice of August 15, 1995 (60 FR 42767, August 17, 1995); and Notice of August 14, 1996 (61 FR 42527); E.O. 12981 (60 FR 62981).

2. The authority citation for 15 CFR parts 732, 736, 740, 748, 768, and 772 is revised 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; Executive Order 13026 (November 15, 1996, 61 FR 58767) Notice of August 15, 1995 (60 FR 42767, August 17, 1995); and Notice of August 14, 1996 (61 FR 42527).

3. The authority citation for 15 CFR part 734 is revised 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; Executive Order 13026 (November 15, 1996, 61 FR 58767); Notice of August 15, 1995 (60 FR 42767, August 17, 1995); and Notice of August 14, 1996 (61 FR 42527).

4. The authority citation for 15 CFR parts 738 and 774 is revised 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; Sec. 201, Pub. L. 104-58, 109 Stat. 557 (30 U.S.C. 185(s)); 30 U.S.C. 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; Executive Order 13026 (November 15, 1996, 61 FR 58767); Notice of August 15, 1995 (60 FR 42767, August 17, 1995); and Notice of August 14, 1996 (61 FR 42527).

5. The authority citation for 15 CFR part 742 is revised 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; Executive Order 13026 (November 15, 1996, 61 FR 58767); Notice of August 15, 1995 (60 FR 42767, August 17, 1995); and Notice of August 14, 1996 (61 FR 42527).

6. The authority citation for 15 CFR part 744 is revised to read as follows:

Authority: 50 U.S.C. app. 2401 et seq.; 50 U.S.C. 1701 et seq.; 22 U.S.C. 3201 et seq.; 42 U.S.C. 2139a; 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; Notice of August 15, 1995 (60 FR 42767, August 17, 1995); and Notice of August 14, 1996 (61 FR 42527).

7. The authority citation for 15 CFR part 750 is revised 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; Executive Order 13026 (November 15, 1996, 61 FR 58767); Notice of August 15, 1995 (60 FR 42767, August 17, 1995); E.O. 12981, 60 FR 62981; and Notice of August 14, 1996 (61 FR 42527).

PART 730 - [AMENDED]

8. Section 730.5 is amended by adding a new sentence to the end of paragraph (d) to read as follows:

§730.5 Coverage of more than exports.

* * * * *

(d) * * * The EAR also restrict technical assistance by U.S. persons with respect to encryption commodities or software.

PART 732 - [AMENDED]

9. Section 732.2 is amended by adding two new sentences at the end of the introductory text to paragraph (b) and by adding two new sentences at the end of the introductory text to paragraph (d) to read as follows:

§732.2 Steps regarding scope of the EAR.

* * * * *

(b) * * * Note that encryption software controlled for EI reasons under ECCN 5D002 on the Commerce Control List (refer to Supplement No.1 to Part 774 of the EAR) shall be subject to the EAR even if publicly available. Accordingly, the provisions of the EAR concerning the public availability of items are not applicable to encryption items controlled for “EI” reasons under ECCN 5D002.

* * * * *

(d) * * * Note that encryption items controlled for EI reasons under ECCN 5A002 or ECCN 5D002 on the Commerce Control List (refer to Supplement No.1 to Part 774 of the EAR) shall be subject to the EAR even if they incorporate less than the de minimis level of U.S. content. Accordingly, the provisions of the EAR concerning de minimis levels are not applicable to encryption items controlled for "EI" reasons under ECCN 5A002, ECCN 5D002, or ECCN 5E002.

* * * * *

10. Section 732.3 is amended by adding two new sentences to the end of paragraph (e)(2) to read as follows:

§732.2 Steps regarding the ten general prohibitions.

* * * * *

(e) Step 10: Foreign-made items incorporating U.S.-origin items and the de minimis rule .* * *

(2) * * *Note that encryption items controlled for EI reasons under ECCN 5A002 or ECCN 5D002 on the Commerce Control List

(refer to Supplement No.1 to Part 774 of the EAR) shall be subject to the EAR even if they incorporate less than the de minimis level of U.S. content. Accordingly, the provisions of the EAR concerning de minimis levels are not applicable to encryption items controlled for "EI" reasons under ECCN 5A002, ECCN 5D002, or ECCN 5E002.

PART 734 - [AMENDED]

11. Section 734.2 is amended by revising paragraphs (b)(1) and (b)(2) introductory text and by adding a new paragraph (b)(9) to read as follows:

§734.2 Important EAR terms and principles.

* * * * *

(b) Export and reexport . (1) Definition of export . "Export" means an actual shipment or transmission of items subject to the EAR out of the United States, or release of technology or software subject to the EAR to a foreign national in the United States, as described in paragraph (b)(2)(ii) of this section. See part 772 of the EAR for the definition that applies to exports of satellites subject to the EAR. See paragraph (b)(9) of this section for the definition that applies to exports of

encryption source code and object code software subject to the EAR.

(2) Export of technology or software . (See paragraph (b)(9) for provisions that apply to encryption source code and object code software.) "Export" of technology or software, excluding encryption software subject to "EI" controls, includes:

* * * * *

(9) Export of encryption source code and object code software .

(i) For purposes of the EAR, the export of encryption source code and object code software means:

(A) An actual shipment, transfer, or transmission out of the United States (see also paragraph (b)(9)(ii) of this section); or

(B) A transfer of such software in the United States to an embassy or affiliate of a foreign country.

(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) 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, photooptical, 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 outside the United States. Such precautions shall include:

(A) Ensuring that the facility from which the software is available controls the access to and transfers of such software through such measures as:

(1) The access control system, either through automated means or human intervention, checks the address of every system requesting or receiving a transfer and verifies that such systems are located within the United States;

(2) 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 Act, and that anyone receiving such a transfer cannot export the software without a license; and

(3) Every party requesting or receiving a transfer of such software must acknowledge affirmatively that he or she understands that the cryptographic software is subject to export controls under the Export Administration Act and that anyone receiving the transfer cannot export the software without a license; or

(B) Taking other precautions, approved in writing by the Bureau of Export Administration, to prevent transfer of such software outside the U.S. without a license.

12. Section 734.3 is amended by revising paragraph (b)(3) and by adding a note to paragraphs (b)(2) and (b)(3) to read as follows:

§734.3 Items subject to the EAR.

* * * * *

(b) * * *

(3) Publicly available technology and software, except software controlled for EI reasons under ECCN 5D002 on the Commerce Control List, that:

(i) Are already published or will be published as described in §734.7 of this part;

(ii) Arise during, or result from, fundamental research, as described in §734.8 of this part;

(iii) Are educational, as described in §734.9 of this part;

(iv) Are included in certain patent applications, as described in §734.10 of this part.

Note to paragraphs (b)(2) and (b)(3) of this section: A printed book or other printed material setting forth encryption source

code is not itself subject to the EAR (see §734.3(b)(2)). However, notwithstanding §734.3(b)(2), encryption source code in electronic form or media (e.g., computer diskette or CD ROM) remains subject to the EAR (see §734.3(b)(3)).

* * * * *

13. Section 734.4 is amended by revising paragraph (b) and revising paragraph (h) to read as follows:

§734.4 De minimis U.S. content.

* * * * *

(b) There is no de minimis level for the reexport of foreign-origin items that incorporate the following:

(1) Items controlled by ECCN 9A004.a; or

(2) "Information security" systems and equipment, cryptographic devices, software and components specifically designed or modified therefor, and related technology controlled for "EI" reasons under ECCN, 5A002 ECCN 5D002, and 5E002. Certain mass market encryption software may become eligible for

de minimis only after a one-time BXA review (refer to §742.15(b)(1)).

* * * * *

(h) Notwithstanding the provisions of paragraphs (c) and (d) of this section, U.S.-origin technology controlled by ECCN 9E003a.1 through a.12, and .f, and related controls, and encryption software controlled for "EI" reasons under ECCN 5D002 or encryption technology controlled for "EI" reasons under ECCN 5E002 do not lose their U.S.-origin when redrawn, used, consulted, or otherwise commingled abroad in any respect with other software or technology of any other origin. Therefore, any subsequent or similar software or technology prepared or engineered abroad for the design, construction, operation, or maintenance of any plant or equipment, or part thereof, which is based on or uses any such U.S.-origin software or technology is subject to the EAR.

14. Section 734.5 is amended by adding paragraph (c) to read as follows:

§734.5 Activities of U.S. and foreign persons subject to the EAR.

* * * * *

(c) Technical assistance by U.S. persons with respect to encryption commodities or software as described in §744.9 of the EAR.

15. Section 734.7 is amended by revising paragraph (b) and by adding paragraph (c) to read as follows:

§734.7 Published information and software.

* * * * *

(b) Software and information is published when it is available for general distribution either for free or at a price that does not exceed the cost of reproduction and distribution. See Supplement No. 1 to this part, Questions G(1) through G(3).

(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 even when publicly available.

16. Section 734.8 is amended by adding a sentence to the end of paragraph (a) to read as follows:

§734.8 Information resulting from fundamental research.

(a) * * * 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 Supplement No. 1 to part 774 of the EAR).

* * * * *

17. Section 734.9 is revised to read as follows:

§734.9 Educational information.

"Educational information" referred to in §734.3(b)(3)(iii) of this part is not subject to the EAR if it is released by instruction in catalog courses and associated teaching laboratories of academic institutions. Dissertation research is discussed in §734.8(b) of this part. (Refer to Supplement No. 1 to this part, Question C(1) through C(6)). 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 Supplement No. 1 to part 774 of the EAR).

18. Supplement No.1 to Part 734 is amended by revising the introductory paragraph to read as follows:

SUPPLEMENT NO. 1 TO PART 734 - QUESTIONS AND ANSWERS - TECHNOLOGY AND SOFTWARE SUBJECT TO THE EAR

This Supplement No. 1 contains explanatory questions and answers relating to technology and software that is subject to the EAR. It is intended to give the public guidance in understanding how BXA interprets this part, but is only illustrative, not comprehensive. In addition, facts or circumstances that differ in any material way from those set forth in the questions or answers will be considered under the applicable provisions of the EAR. Exporters should note that the provisions of this supplement do not apply to encryption software (including source code) 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. See §742.15 of the EAR. This Supplement is divided into nine sections according to topic as follows:

* * * * *

PART 736 - [AMENDED]

19. Section 736.2 is amended by revising paragraph (b)(7) to read as follows:

§736.2 General prohibitions and determination of applicability.

* * * * *

(7) General Prohibition Seven -- Support of Certain Activities by U.S. persons .

(i) Support of Proliferation Activities (U.S. Person Proliferation Activity) . If you are a U.S. Person as that term is defined in §744.6(c) of the EAR, you may not engage in any activities prohibited by §744.6(a) or (b) of the EAR which prohibits the performance, without a license from BXA, of certain financing, contracting, service, support, transportation, freight forwarding, or employment that you know will assist in certain proliferation activities described further in part 744 of the EAR. There are no License Exceptions to this General Prohibition

Seven in part 740 of the EAR unless specifically authorized in that part.

(ii) You may not, without a license from BXA, provide certain technical assistance to foreign persons with respect to encryption items, as described in §744.9 of the EAR.

* * * * *

PART 738 - [AMENDED]

20. Section 738.2 is amended by adding "EI Encryption Items" in alphabetical order to the list of Reasons for Control in paragraph (d)(2)(i)(A).

PART 740 - [AMENDED]

21. Part 740 is amended by redesignating §§740.8 through 740.15 as §§740.9 through 740.16 and by adding a new §740.8 to read as follows:

§740.8 Key Management Infrastructure.

(a) Scope. License Exception KMI authorizes the export and reexport of certain encryption software and equipment.

(b) Eligible software and equipment.

(1) Recovery encryption items. Eligible items are recovery encryption software and equipment controlled under ECCNs 5D002 or 5A002 made eligible as a result of a one-time BXA review. You may initiate this review by submitting a classification request for your product in accordance with paragraph (d)(1) of this section.

(2) Non-recoverable encryption items. Eligible items are 56-bit DES or equivalent strength non-key recovery software and equipment controlled under ECCNs 5D002 or 5A002 made eligible as a result of a one-time BXA review. You may initiate this review by submitting a classification request for your product in accordance with paragraph (d)(2) of this section.

(c) Eligible destinations. License Exception KMI is available for all destinations, except Cuba, Libya, North Korea, Iraq, Iran, Syria, and Sudan.

(d) Additional eligibility requirements.

(1) Recovery encryption items . Classification requests for recovery encryption software and equipment must meet the following criteria:

(i) Key escrow and key recovery products .

(A) Key escrow and key recovery products must meet the criteria identified in Supplement No. 4 to part 742 of the EAR;

(B) Key recovery agents must meet the criteria identified in Supplement No. 5 to part 742 of the EAR;

(C) Key recovery agents must implement the security policies and key escrow /key recovery procedures identified in Supplement No. 5 to part 742 of the EAR;

(D) Key recovery agents must comply with all applicable EAR Record keeping requirements, including record retention requirements; and

(E) Key recovery agents must carry out the key holding obligations as approved by BXA, and any violation of any of the key holding obligations shall also constitute a violation of the EAR. Note that the key recovery agent’s continuing

compliance with key recovery agent requirements and key safeguard procedures is a condition for use of License Exception KMI. The exporter or reexporter, whether that person is the key recovery agent or not, must submit a new classification request to BXA if there are any changes (e.g., termination, replacement, additions) to the previously approved key recovery agent.

(ii) Other recoverable encryption items. Requests for one-time review of recoverable products which allow government officials to obtain, under proper legal authority and without the cooperation or knowledge of the user, the plaintext of the encrypted data and communications will receive favorable consideration.

(2) Non-recoverable encryption items. Upon approval of your classification request submitted in accordance with this paragraph (d)(2), you will become eligible to use License Exception KMI for six months. In order to continue using this License Exception, you must renew your eligibility by submitting the progress report described in paragraph (d)(2)(ii) of this section. Classification requests for 56-bit DES or equivalent strength non-key recovery software and equipment must meet the following criteria:

(i) Initial request must be submitted with a business plan that explains in detail the steps the applicant will take during the two-year transition period according to the criteria identified in Supplement No. 7 to part 742 of the EAR;

(ii) Renewal for use of this License Exception is contingent upon progress reports sent to BXA every six months and the applicant’s adherence to benchmarks and milestones as set forth in the plan submitted for the initial classification request.

(iii) Applicants may inform their authorized distributors that an approved classification and plan has been granted to them and the distributors’ authority to so export or reexport will be for a time period ending on the same day the applicant’s authority to export or reexport ends.

(e) Reporting requirements . (1) You must provide semiannual reports to BXA identifying:

(i) Ultimate consignee; specific end-user name and address, if available; and country of ultimate destination; and

(ii) Quantities of each encryption item shipped.

(2) You must submit reports no later than March 1 and no later than September 1 of any given year.

22. Newly designated §740.9 is amended by revising paragraph (c)(3) to read as follows:

§740.9 Temporary imports, exports, and reexports (TMP).

* * * * *

(c) * * *

(3) Exports of beta test software . All software that is controlled by the Commerce Control List (Supplement No. 1 to part 774 of the EAR), and under Commerce licensing jurisdiction, is eligible for export and reexport, subject to the restrictions of this paragraph, except encryption software controlled for EI reasons under ECCN 5D002. Certain encryption software may become eligible after a one-time BXA review (refer to §742.15(b)(1) of the EAR).

* * * * *

23. Newly designated §740.11 is amended by revising paragraphs (b)(2)(iii) and (b)(2)(iv) to read as follows:

§740.11 Governments and international organizations (GOV).

* * * * *

(b) * * *

(2) * * *

(iii) Items for official use within national territory by agencies of cooperating governments. This License Exception is available for all items consigned to and for the official use of any agency of a cooperating government within the territory of any cooperating government, except:

(A) Computers with a CTP greater than 10,000 MTOPS when destined for Argentina, Hong Kong, South Korea, Singapore or Taiwan;

(B) Items identified on the Commerce Control List as controlled for missile technology (MT), chemical and biological warfare (CB), or nuclear nonproliferation (NP) reasons;

(C) Regional stability items controlled under Export Control Classification Numbers (ECCNs) 6A002, 6A003, 6D102, 6E001, 6E002, 7D001, 7E001, 7E002, and 7E101 as described in §742.6(a)(1) of the EAR; or

(D) Encryption items controlled for EI reasons as described in the Commerce Control List.

(iv) Diplomatic and consular missions of a cooperating government . This License Exception is available for all items consigned to and for the official use of a diplomatic or consular mission of a cooperating government located in any country in Country Group B (see Supplement No. 1 to part 740), except:

(A) Computers with a CTP greater than 10,000 MTOPS when destined for Argentina, Hong Kong, South Korea, Singapore or Taiwan;

(B) Items identified on the Commerce Control List as controlled for missile technology (MT), chemical and biological warfare (CB), or nuclear nonproliferation (NP) reasons;

(C) Regional stability items controlled under Export Control Classification Numbers (ECCNs) 6A002, 6A003,

6D102, 6E001, 6E002, 7D001, 7E001, 7E002, and 7E101 as described in §742.6(a)(1) of the EAR; or

(D) Encryption items controlled for EI reasons as described in the Commerce Control List.

* * * * *

24. Newly designated §740.13 is amended by revising paragraph (d)(2) to read as follows:

§740.13 Technology and software - unrestricted (TSU).

* * * * *

(2) Software not eligible for this License Exception. This License Exception is not available for encryption software controlled for "EI" reasons under ECCN 5D002. (Refer to §§742.15(b)(1) and 748.3(b) of the EAR for information on item classifications regarding a one-time BXA review for release from EI controls.)

* * * * *

PART 742 - [AMENDED]

25. Part 742 is amended by revising §742.15 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. As the President indicated in E.O. 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 all destinations, except Canada, for 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"). For encryption items previously on the U.S. Munitions List and currently authorized for export or reexport under a State Department license, distribution arrangement or any other authority of the State Department, U.S. persons holding valid USML licenses and other approvals issued by the Department of State prior to (DATE OF PUBLICATION) may ship remaining balances authorized by such licenses or approvals under the authority of the EAR by filing Shippers Export Declarations (SEDs) with District Directors of Customs, citing the provisions of this section effective on (DATE OF PUBLICATION) and the State Department license number. Such shipments shall be in accordance with the terms and conditions, including the expiration date, existing at the time of issuance of the State license. Violations of such authorizations, terms and conditions constitute violations of the EAR. Any reports required for distribution and other types of agreements previously authorized by the Department of State, prior to (DATE OF PUBLICATION)should be henceforth submitted to BXA at the following address:

Office of Strategic Trade and Foreign Policy Controls
Bureau of Export Administration
Department of Commerce

14th Street and Pennsylvania Ave., N.W.

Room 2705

Washington, D.C. 20230

(b) Licensing policy . The following licensing policies apply to items identified in paragraph (a) of this section. This section refers you to Supplements No. 4, No. 5, and No. 7 to this part 742. For purposes of these supplements, “products” refers to commodities and software. 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.

(1) Certain mass-market encryption software . Consistent with E.O. 13026 of November 15, 1996 (61 FR 58767), certain encryption software that was transferred from the U.S. Munitions List to the Commerce Control List pursuant to the Presidential Memorandum of November 15, 1996 may be released from “EI” controls and thereby made eligible for mass market treatment after a one-time review. To determine eligibility for mass market treatment, exporters must submit a classification request to BXA. 40-bit mass market encryption software may be eligible for a 7-day review process, and company proprietary software may be eligible for 15-day processing. Refer to Supplement No. 6 to

part 742 and §748.3(b)(3) of the EAR for additional information. Note that the one-time review is for a determination to release encryption software in object code only unless otherwise specifically requested. Exporters requesting release of the source code should refer to paragraph (b)(3)(v)(E) of Supplement No. 6 to part 742. If, after a one-time review, BXA determines that the software is released from EI controls, such software is eligible for all provisions of the EAR applicable to other software, such as License Exception TSU for mass-market software. If BXA determines that the software is not released from EI controls, a license is required for export and reexport to all destinations, except Canada, and license applications will be considered on a case-by-case basis.

(2) Key Escrow, Key Recovery and Recoverable encryption software and commodities . Recovery encryption software and equipment controlled for EI reasons under ECCN 5D002 or under ECCN 5A002, including encryption equipment designed or modified to use recovery encryption software, may be made eligible for license exception KMI after a one-time BXA review. License Exception KMI is available for all destinations except Cuba, Iran, Iraq, Libya, North Korea, Syria and Sudan. To determine eligibility, exporters must submit a classification request to BXA. Requests for one-time review of key escrow and key recovery encryption items will receive favorable consideration

provided that, prior to the export or reexport, a key recovery agent satisfactory to BXA has been identified (refer to Supplement No. 5 to part 742) and security policies for safeguarding the key(s) or other material/information required to decrypt ciphertext as described in Supplement No. 5 to part 742 are established to the satisfaction of BXA and are maintained after export or reexport as required by the EAR. If the exporter or reexporter intends to be the key recovery agent, then the exporter or reexporter must meet all of the requirements of a key recovery agent identified in Supplement No. 5 to part 742. In addition, the key escrow or key recovery system must meet the criteria identified in Supplement No. 4 to part 742. Note that eligibility is dependent on continued fulfilment of the requirements of a key recovery agent identified in Supplement No. 5 to part 742. Since the establishment of a key management infrastructure and key recovery agents may take some time, BXA will, while the infrastructure is being built, consider requests for eligibility to export key recovery encryption products which facilitate establishment of the key management infrastructure before a key recovery agent is named, consistent with national security and foreign policy. When BXA approves such cases, exporters of products described in Supplement No. 4 to part 742 are required to furnish the name of an agent by December 31, 1998. Requests for one-time review of recoverable products which allow government officials to obtain, under proper legal

authority and without the cooperation or knowledge of the user, the plaintext of the encrypted data and communications will receive favorable consideration.

(3) Non-recovery encryption items up to 56-bit key length DES or equivalent strength supported by a satisfactory business and marketing plan for exporting recoverable items and services .

(i) Manufacturers of non-recovery encryption items up to 56-bit key length DES or equivalent strength will be permitted to export and reexport under the authority of License Exception KMI provided that the requirements and conditions of the License Exception are met. Exporters must submit a classification request for an initial BXA review of the item and a satisfactory business and marketing plan that explains in detail the steps the applicant will take during the two-year transition period beginning January 1, 1997 to develop, produce, and/or market encryption items and services with recoverable features. Manufacturers would commit to produce key recovery products. Others would commit to incorporate such products into their own products or services. Such efforts can include: the scale of key recovery research and development, product development, and marketing plans; significant steps to reflect potential customer demand for key recovery products in the firm’s encryption-related business; and how soon a key recovery agent will be identified.

Note that BXA will accept requests for classification of non-recoverable encryption items up to 56-bit key length DES or equivalent strength under this paragraph from distributors, re-sellers, integrators, and other entities that are not manufacturers of the encryption items. The use of License Exception KMI is not automatic; eligibility must be renewed every six months. Renewal after each six-month period will depend on the applicant's adherence to explicit benchmarks and milestones as set forth in the plan approved with the initial license classification and amendments as approved by BXA. This relaxation of controls and use of License Exception KMI will last through December 31, 1998. The plan submitted with classifications for the export of non-recoverable encryption items up to 56-bit key length DES or equivalent strength must include the elements in Supplement No. 7 to part 742.

(ii) BXA will make a determination on such classification requests within 15 days of receipt. Exports and reexports of non-recoverable encryption items up to 56-bit key length DES or equivalent strength will be authorized under the provisions of License Exception KMI, contingent upon BXA's review and approval of a satisfactory progress report related to the ongoing plan submitted by the applicant. The applicant must submit a letter to BXA every six months requesting approval of the progress report. Note that distributors, re-sellers,

integrators, or other entities that are not manufacturers of the encryption items are permitted to use License Exception KMI for exports and reexports of such items only in instances where a classification has been granted to the manufacturer of the encryption items or a classification has been granted to the distributors, re-sellers, integrators, or other entities. The authority to so export or reexport will be for a time period ending on the same day the producer's authority to export or reexport ends.

(4) All other encryption items .

(i) Encryption licensing arrangement . Applicants may submit license applications for exports and reexports of certain encryption commodities and software in unlimited quantities for all destinations except, Cuba, Iran, Iraq, Libya, North Korea, Syria, and Sudan. Applications will be reviewed on a case-by-case basis. Encryption licensing arrangements may be approved with extended validity periods specified by the applicant in block #24 on Form BXA-748P. In addition, the applicant must specify the sales territory and classes of end-users. Such licenses may require the license holder to report to BXA certain information such as item description, quantity, value, and end-user name and address.

(ii) Applications for encryption items not authorized under an encryption licensing arrangement. Applications for the export and reexport of all other encryption items will be considered on a case-by-case basis.

(5) Applications for encryption technology. Applications for the export and reexport of encryption technology will be considered on a case-by-case basis.

(c) Contract sanctity. Contract sanctity provisions are not available for license applications reviewed under this section.

(d) [Reserved]

26. Part 742 is amended by revising Supplement No. 4 and Supplement No. 5, and by adding a new Supplement No. 6 and a new Supplement No. 7 to read as follows:

SUPPLEMENT NO. 4 TO PART 742 - KEY ESCROW OR KEY RECOVERY PRODUCTS CRITERIA

Key Recovery Feature

(1) The key(s) or other material/information required to decrypt ciphertext shall be accessible through a key recovery feature.

(2) The product’s cryptographic functions shall be inoperable until the key(s) or other material/information required to decrypt ciphertext is recoverable by government officials under proper legal authority and without the cooperation or knowledge of the user.

(3) The output of the product shall automatically include, in an accessible format and with a reasonable frequency, the identity of the key recovery agent(s) and information sufficient for the key recovery agent(s) to identify the key(s) or other material/information required to decrypt the ciphertext.

(4) The product’s key recovery functions shall allow access to the key(s) or other material/information needed to decrypt the ciphertext regardless of whether the product generated or received the ciphertext.

(5) The product’s key recovery functions shall allow for the recovery of all required decryption key(s) or other material/information required to decrypt ciphertext during a period of authorized access without requiring repeated

presentations of access authorization to the key recovery agent(s).

Interoperability Feature

(6) The product’s cryptographic functions may interoperate with:

(i) Other key recovery products that meet these criteria, and shall not interoperate with products whose key recovery feature has been altered, bypassed, disabled, or otherwise rendered inoperative; and

(ii) Non-key recovery products only when the key recovery product permits access to the key(s) or other material/information needed to decrypt ciphertext generated or received (i.e., one direction at a minimum) by the key recovery product.

Design, Implementation and Operational Assurance

(7) The product shall be resistant to efforts to disable or circumvent the attributes described in criteria one through six.

(8) The product’s cryptographic function’s key(s) or other material/information required to decrypt ciphertext shall be

escrowed with a key recovery agent(s) (who may be a key recovery agent(s) internal to the user's organization) acceptable to BXA, pursuant to the criteria in Supplement No. 5 to Part 742. Since the establishment of a key management infrastructure and key recovery agents may take some time, BXA will, while the infrastructure is being built, consider exports of key recovery encryption products which facilitate establishment of the key management infrastructure before a key recovery agent is named. Exporters of products described in this Supplement No. 4 to part 742 are required to furnish the name of an agent by December 31, 1998.

SUPPLEMENT NO. 5 TO PART 742 - KEY ESCROW OR KEY RECOVERY AGENT CRITERIA, SECURITY POLICIES, AND KEY ESCROW OR KEY RECOVERY PROCEDURES

KEY ESCROW OR KEY RECOVERY AGENT REQUIREMENTS; SECURITY POLICIES; KEY ESCROW OR KEY RECOVERY PROCEDURES

This Supplement sets forth criteria that the Department of Commerce will use to approve key recovery agents to support approval of the export or reexport of key recovery encryption items controlled for EI reasons under ECCNs 5A002 and 5D002.

Any arrangements between the exporter or reexporter and the key recovery agent must reflect the provisions contained in this Supplement in a manner satisfactory to BXA, in conjunction with other agencies. This Supplement outlines the criteria for employing key recovery agent personnel for key recovery procedures. An applicant for eligibility to export or reexport key recovery items shall provide, or cause the proposed key recovery agent to provide, to BXA sufficient information concerning any proposed key recovery agent arrangements to permit BXA's evaluation of the key recovery agent's security policies, key recovery procedures, and suitability and trustworthiness to maintain the confidentiality of the key(s) or other material/information required to decrypt ciphertext. The key recovery agent, who must be approved by BXA, may be the applicant for the classification request. When there is no key recovery agent involved, or the customer will self-escrow abroad, with or without a legal obligation to the exporter, the customer must be approved by BXA. BXA retains the right, in addition to any other remedies, to revoke eligibility for License Exception KMI if BXA determines that a key recovery agent no longer meets these criteria. The requirements related to the suitability and trustworthiness, security policies, and key recovery procedures of the key recovery agent shall be made terms and conditions of the License Exception for key recovery items. BXA shall require

the key recovery agent to provide a representation that it will comply with such terms and conditions.

Note: Use of key recovery agents located outside the U.S. is permitted if acceptable to BXA in consultation with the host government, as appropriate.

I. Key Recovery Agent Requirements

(1)(a) A key recovery agent must identify by name, date and place of birth, and social security number, individual(s) who:

(i) Is/are directly involved in the escrowing of key(s) or other material/information required to decrypt ciphertext; or

(ii) Have access to key(s) or other material/information required to decrypt ciphertext, or

(iii) Have access to information concerning requests for key(s) or other material/information required to decrypt ciphertext; or

(iv) Respond to requests for key(s) or other material/information required to decrypt ciphertext; or

(v) Is/are in control of the key recovery agent and have access or authority to obtain key(s) or other material/information required to decrypt ciphertext, and

(b) Must certify that such individual(s) meet the requirements of the following paragraphs (b)(i) or (b)(ii). BXA reserves the right to determine at any time the suitability and trustworthiness of such individual(s). Evidence of an individual's suitability and trustworthiness shall include:

(i) Information indicating that the individual(s):

(A) Has no criminal convictions of any kind or pending criminal charges of any kind;

(B) Has not breached fiduciary responsibilities (e.g., has not violated any surety or performance bonds); and

(C) Has favorable results of a credit check; or,

(ii) Information that the individual(s) has an active U.S. government security clearance of Secret or higher issued or updated within the last five years.

(2) The key recovery agent shall timely disclose to BXA when an individual no longer meets the requirements of paragraphs I.(1)(b)(i) or (ii).

(3) A key recovery agent must, to remain eligible for License Exception KMI, identify to BXA by name, date and place of birth, and social security number any new individual(s) who will assume the responsibilities set forth in paragraph I.(1)(a) of this Supplement. Before that individual(s) assumes such responsibilities, the key recovery agent must certify to BXA that the individual(s) meets the criteria set forth in subparagraphs I.(1)(b)(i) or (b)(ii) of this Supplement. BXA reserves the right to determine at any time the suitability and trustworthiness of such personnel.

(4) If ownership or control of a key recovery agent is transferred, no export may take place under previously issued approvals until the successor key recovery agent complies with the criteria of this Supplement.

(5) Key recovery agents shall submit suitable evidence of the key recovery agent’s corporate viability and financial responsibility (e.g., a certificate of good standing from the state of incorporation, credit reports, and errors/omissions insurance).

(6) Key recovery agents shall disclose to BXA any of the following which have occurred within the ten years prior to the application:

(a) Federal or state felony convictions of the business;

(b) Material adverse civil fraud judgments or settlements; and

(c) Debarments from federal, state, or local government contracting.

The applicant shall also timely disclose to BXA the occurrence of any of the foregoing during the use of License Exception KMI.

(7) Key recovery agent(s) shall designate an individual(s) to be the security and operations officer(s).

(8) A key recovery agent may be internal to a user’s organization and may consist of one or more individuals. BXA may approve such key recovery agents if sufficient information is provided to demonstrate that appropriate safeguards will be employed in handling key recovery requests from government entities. These safeguards should ensure: the key recovery agent’s structural

independence from the rest of the organization; security; and confidentiality.

II. Security Policies

(1) Key recovery agents must implement security policies that assure the confidentiality, integrity, and availability of the key(s) or other material/information required for decryption of the ciphertext.

(a) Procedures to assure confidentiality shall include:

(i) Encrypting all key(s) or other material/information required to decrypt ciphertext while in storage, transmission, or transfer; or

(ii) Applying reasonable measures to limit access to the database (e.g. using keyed or combination locks on the entrances to escrow facilities and limiting the personnel with knowledge of or access to the keys/combinations).

(b) Procedures to assure the integrity of the database (i.e. assuring the key(s) and other material/information required to decrypt ciphertext are protected against unauthorized changes) shall include the use of access controls such as database password

controls, digital signatures, system auditing, and physical access restrictions.

(c) Procedures to assure the availability of the database (i.e. assuring that key(s) and other material/information required to decrypt ciphertext are retrievable at any time) shall include system redundance, physical security, and the use of cryptography to control access.

(2) Policies and procedures shall be designed and operated so that a failure by a single person, procedure, or mechanism does not compromise the confidentiality, integrity and availability of key(s)or other material/information required to decrypt ciphertext. Security policies and procedures may include, but are not limited to , multi-person control of access to recoverable keys, split keys, and back-up capabilities.

(3) Key recovery agents shall implement policies that protect against unauthorized disclosure of information regarding whose encryption material is stored, the fact that key(s) or other material/information required to decrypt ciphertext was requested or provided, and the identity of a requester. Procedures to assure the confidentiality of this information shall include those described in paragraph II.(1)(a) of this supplement.

(4) Key recovery agents shall provide to BXA prompt notice of a compromise of a security policy or of the confidentiality of key(s) or other material/information required to decrypt ciphertext.

III. Key Recovery Procedures

(1) Key recovery agents shall maintain the ability to make the key(s) or other material/information required to decrypt ciphertext available until notified otherwise by BXA. Key recovery agents shall make requested key(s) or other material/information required to decrypt ciphertext available, to the extent required by the request, within two hours from the time they receive a request from a government agency acting under appropriate legal authority.

(2) Key recovery agents shall maintain data regarding key recovery requests received, release of key(s) or other material/information required to decrypt ciphertext, database changes, system administration access, and dates of such events for purposes of audits by BXA.

(3) The key recovery agent must transfer all key recovery equipment, key(s) and/or other material/information required to

decrypt ciphertext, key recovery database, and all administrative information necessary to its key recovery operations to another key recovery agent approved by BXA in the event that:

(a) The key recovery agent dissolves or otherwise terminates escrowing
operations, or

(b) BXA determines that there is a risk of such dissolution or termination, or

(c) BXA determines that the key recovery agent is no longer suitable or trustworthy.

SUPPLEMENT NO. 6 TO PART 742 - GUIDELINES FOR SUBMITTING A CLASSIFICATION REQUEST FOR A MASS MARKET SOFTWARE PRODUCT THAT CONTAINS ENCRYPTION

Classification requests for release of certain mass market encryption software from EI controls must be submitted on Form BXA-748P, in accordance with §748.3 of the EAR. To expedite review of the request, clearly mark the envelope “Attn.: Mass

Market Encryption Software Classification Request". In Block 9: Special Purpose of the Form BXA-748P, you must insert the phrase "Mass Market Encryption Software. 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., N.W.
Washington, D.C. 20230

(a) Requests for mass market encryption software that meet the criteria in paragraph (a)(2) of this Supplement will be processed in seven (7) working days from receipt of a properly completed request. Those requests for mass market encryption software that meet the criteria of paragraph (a)(1) of this Supplement only will be processed in fifteen (15) working days from receipt of a properly completed request. When additional information is requested, the request will be processed within 15 working days of the receipt of the requested information.

(1) A mass market software product that meets all the criteria established in this paragraph will be processed in fifteen (15) working days from receipt of the properly completed request:

(i) The commodity must be mass market software. Mass market software is computer software that is available to the public via sales from stock at retail selling points by means of over-the-counter transactions, mail order transactions, or telephone call transactions;

(ii) The software must be designed for installation by the user without further substantial support by the supplier. Substantial support does not include telephone (voice only) help line services for installation or basic operation, or basic operation training provided by the supplier; and

(iii) The software includes encryption for data confidentiality.

(2) A mass market software product that meets all the criteria established in this paragraph will be processed in seven working days from receipt of the properly completed request:

(i) The software meets all the criteria established in paragraph (a)(1)(i) through (iii) of this supplement;

(ii) The data encryption algorithm must be RC4 and/or RC2 with a key space no longer than 40 bits. The RC4 and RC2 algorithms are proprietary to RSA Data Security, Inc. To ensure that the subject software is properly licensed and correctly implemented, contact RSA Data Security, (415)595-8782;

(iii) If both RC4 and RC2 are used in the same software, their functionality must be separate. That is, no data can be operated sequentially on by both routines or multiply by either routine;

(iv) The software must not allow the alteration of the data encryption mechanism and its associated key spaces by the user or any other program;

(v) The key exchange used in data encryption must be:

(A) A public key algorithm with a key space less than or equal to a 512 bit modulus and/or;

(B) A symmetrical algorithm with a key space less than or equal to 64 bits; and

(vi) The software must not allow the alteration of the key management mechanism and its associated key space by the user or any other program.

(b) Instructions for the preparation and submission of a classification request that is eligible for seven day handling are as follows:

(1) If the software product meets the criteria in paragraph (a)(2) of this Supplement, you must call the Department of Commerce on (202) 482-0092 to obtain a test vector. This test vector must be used in the classification process to confirm that the software has properly implemented the approved encryption algorithms.

(2) Upon receipt of the test vector, the applicant must encrypt the test plain text input provided using the commodity's encryption routine (RC2 and/or RC4) with the given key value. The applicant should not pre-process the test vector by any compression or any other routine that changes its format. Place the resultant test cipher text output in hexadecimal format on an attachment to form BXA-748P.

(3) You must provide the following information in a cover letter to the classification request:

(i) Clearly state at the top of the page “Mass Market Encryption Software - 7 Day Expedited Review Requested”;

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

(iii) State the name of the single software product being submitted for review. A separate classification request is required for each product;

(iv) State how the software has been written to preclude user modification of the encryption algorithm, key management mechanism, and key space;

(v) Provide the following information for the software product:

(A) Whether the software uses the RC2 and/or the RC4 algorithm and how the algorithm(s) is used. If both of these algorithms are used in the same product, also state how the functionality of each is separated to assure that no data is operated on by both algorithms;

(B) Pre-processing information of plain text data before encryption (e.g. the addition of clear text header information or compression of the data);

(C) Post-processing information of cipher text data after encryption (e.g. the addition of clear text header information or packetization of the encrypted data);

(D) Whether a public key algorithm or a symmetric key algorithm is used to encrypt keys and the applicable key space;

(E) For classification requests regarding source code:

(1) Reference the applicable executable product that has already received a one-time review;

(2) Include whether the source code has been modified by deleting the encryption algorithm, its associated key management routine(s), and all calls to the algorithm from the source code, or by providing the encryption algorithm and associated key management routine(s) in object code with all calls to the algorithm hidden. You must provide the technical details on how you have modified the source code;

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

(F) Provide any additional information which you believe would assist in the review process.

(c) Instructions for the preparation and submission of a classification request that is eligible for 15 day handling are as follows:

(1) If the software product meets only the criteria in paragraph (a)(1) of this supplement, you must prepare a classification request. Send the original to the Bureau of Export Administration. Send a copy by Express Mail to:

Attn.: 15 day Encryption Request Coordinator
P.O. Box 246
Annapolis Junction, MD 20701-0246

(2) You must provide the following information in a cover letter to the classification request:

(i) Clearly state at the top of the page “Mass Market Software and Encryption - 15 Day Expedited Review Requested”;

(ii) State that you have reviewed and determined that the software subject of the classification request, meets the criteria of paragraph (a)(1) of this Supplement;

(iii) State the name of the single software product being submitted for review. A separate classification request is required for each product;

(iv) State that a duplicate copy, in accordance with paragraph (c)(1) of this Supplement, has been sent to the 15 day Encryption Request Coordinator; and

(v) Ensure that the information provided includes brochures or other documentation or specifications relating to the software, as well as any additional information which you believe would assist in the review process.

(3) Contact the Bureau of Export Administration on (202) 482-0092 prior to submission of the classification to facilitate the submission of proper documentation.

SUPPLEMENT NO. 7 TO PART 742 - REVIEW CRITERIA FOR EXPORTER KEY ESCROW OR KEY RECOVERY DEVELOPMENT PLANS

Exporter Key Recovery Plan

(1) Export of 56-bit digital encryption standard (DES) or equivalent strength encryption products, without key recovery, will be permitted, in exchange for specific commitments to key recovery products and services and a key management infrastructure. After a one-time review of the strength of the product, the 56-bit DES or equivalent strength products will be eligible for export License Exception KMI, provided that the exporter submits an acceptable plan.

(2) Acceptable plans include: export licenses issued for, and demonstrations of, key recovery products to appropriate U.S. agencies; plans describing products under development with key recovery features (see paragraph (3) of this supplement), and for distributors, a plan describing intentions to offer for distribution key recovery products.

(3) Following are topical areas to include in the plan, which should be submitted to the Department of Commerce, Bureau of Export Administration, in the form of a letter from senior corporate management:

(i) Steps the applicant has taken or will take (depending on its line of business) to develop, produce, distribute, market, and/or transition to encryption products with key recovery features. The plan should include benchmarks and milestones for incorporating key recovery features into products and services, and for the supporting key management infrastructure, including key recovery agent(s); and

(ii) Provision, at the applicant's discretion, of other information to indicate commitment to the development of a key management infrastructure, such as participation in US Government pilot programs, current key recovery products or services provided, role in NIST's Technical Advisory Committee on a Key Management Infrastructure, participation in other encryption policy committees or groups, or other support for the key management infrastructure.

(4) Renewal of License Exception KMI must be sought by sending a letter to BXA every six months reporting progress in meeting milestones set forth in the exporter's plan for key recovery products and services.

PART 744 - [AMENDED]

27. Part 744 is amended by adding a new §744.9 to read as follows:

§744.9. Restrictions on technical assistance by U.S. persons with respect to encryption items.

(a) General prohibition . No U.S. person may, without a license from BXA, provide technical assistance (including training) to foreign persons with the intent to aid a foreign person in the development or manufacture outside the United States of encryption commodities and software that, if of United States origin, would be controlled for "EI" reasons under ECCN 5A002 or 5D002. Note that this prohibition does not apply if the U.S. person providing the assistance has a license or is otherwise entitled to export the encryption commodities and software in question to the foreign person(s) receiving the assistance. Note in addition that the mere teaching or discussion of information about cryptography, including, for example, in an academic setting, by itself would not establish the intent described in this section, even where foreign persons are present.

(b) Definition of U.S. person . For purposes of this section, the term U.S. person includes:

(1) Any individual who is a citizen or permanent resident alien of the United States;

(2) Any juridical person organized under the laws of the United States or any jurisdiction within the United States, including foreign branches; and

(3) Any person in the United States.

(c) License review standards . Applications involving activities described in this section will be reviewed on a case-by-case basis to determine whether the activity is consistent with U.S. national security and foreign policy interests.

PART 748 - [AMENDED]

28. Section 748.3 is amended by adding a new paragraph (b)(3) to read as follows:

§748.3 Classification and Advisory Opinions.

* * * * *

(b) * * *

(3) Classification requests for a one-time Department of Commerce review of encryption software transferred from the U.S. Munitions List consistent with E.O. 13026 of November 15, 1996 (61 FR 58767) and pursuant to the Presidential Memorandum of that date are required prior to export to determine eligibility for release from EI controls. Refer to Supplement No. 6 to part 742 for instructions on submitting such requests for mass market encryption software. For requests for Key Escrow, Key Recovery, or Recovery encryption products, include the word “Encryption” in Block 24: Additional Information.

* * * * *

PART 750 - [AMENDED]

29. Section 750.3 is amended by adding a new paragraph (b)(2)(v) to read as follows:

§750.3 Review of license applications by BXA and other government agencies and departments.

* * * * *

(b) * * *

(2) * * *

(v) The Department of Justice is concerned with controls relating to encryption items.

PART 768 - [AMENDED]

30. Section 768.1(b) is amended to read as follows:

§768.1 Introduction.

* * * * *

(b) Scope. This part applies only to the extent that items are controlled for national security purposes. This part does not apply to encryption items that were formerly controlled on the U.S. Munitions List and that were transferred 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, which shall not be subject to any mandatory foreign availability review procedures.

* * * * *

31. Section 768.3 is amended by adding a new sentence at the end of paragraph (a) to read as follows:

§768.3 Foreign availability assessment.

(a) * * * The effect of any such determination on the effectiveness of foreign policy controls may be considered independent of this part.

* * * * *

PART 772 - [AMENDED]

32. Part 772 is amended by adding new definitions of “Encryption items,” “Encryption object code,” "Encryption software," and "Encryption source code," in alphabetical order and by amending the definitions of "Advisory Committee on Export Policy (ACEP)," "Commodity," "Export Administration Review Board (EARB)," and "Operating Committee (OC)," to read as follows:

Part 772 - Definitions of Terms

* * * * *

Advisory Committee on Export Policy (ACEP) . The ACEP voting members include the Assistant Secretary of Commerce for Export Administration, and Assistant Secretary-level representatives from the Departments of State, Defense, Justice (for encryption exports), Energy, and the Arms Control and Disarmament Agency. The appropriate representatives of the Joint Chiefs of Staff and the Director of the Nonproliferation Center of the Central Intelligence Agency are non-voting members. The Assistant Secretary of Commerce for Export Administration is the Chair. Appropriate acting Assistant Secretary, Deputy Assistant Secretary or equivalent strength of any agency or department may serve in lieu of the Assistant Secretary of the concerned agency or department. Such representatives, regardless of rank, will speak and vote on behalf of their agencies or departments. The ACEP may invite Assistant Secretary-level representatives of other Government agencies or departments (other than those identified above) to participate in the activities of the ACEP when matters of interest to such agencies or departments are under consideration. Decisions are made by majority vote.

* * * * *

Commodity . Any article, material, or supply except technology and software. Note that the provisions of the EAR applicable to the control of software (e.g. publicly available provisions) are

not applicable to encryption software. Encryption software is controlled because, like the items controlled under ECCN 5A002, it has a 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.

* * * * *

Encryption items . The phrase encryption items includes all encryption commodities, software, and technology that contain encryption features and are subject to the EAR. This does not include encryption items specifically designed, developed, configured, adapted or modified for military applications (including command, control and intelligence applications) which are controlled by the Department of State on the U.S. Munitions List.

Encryption object code . Computer programs containing an encryption source code that has been compiled into a form of code that can be directly executed by a computer to perform an encryption function.

Encryption software . Computer programs that provide capability of encryption functions or confidentiality of

information or information systems. Such software includes source code, object code, applications software, or system software.

Encryption source code . A precise set of operating instructions to a computer that, when compiled, allows for the execution of an encryption function on a computer.

* * * * *

Export Administration Review Board (EARB) . EARB voting members are the Secretary of Commerce, the Secretary of State, the Secretary of Defense, the Secretary of Energy, the Attorney General (for encryption exports), and the Director of the Arms Control and Disarmament Agency. The Chairman of the Joint Chiefs of Staff and the Director of Central Intelligence are non-voting members. The Secretary of Commerce is the Chair of the EARB. No alternate EARB members may be designated, but the acting head or deputy head of any agency or department may serve in lieu of the head of the concerned agency or department. The EARB may invite the heads of other Government agencies or departments (other than those identified in this definition) to participate in the activities of the EARB when matters of interest to such agencies or departments are under consideration. Decisions are made by majority vote.

* * * * *

Operating Committee (OC) . The OC voting members include representatives of appropriate agencies in the Departments of Commerce, State, Defense, Justice (for encryption exports), and Energy and the Arms Control and Disarmament Agency. The appropriate representatives of the Joint Chiefs of Staff and the Director of the Nonproliferation Center of the Central Intelligence Agency are non-voting members. The Department of Commerce representative, appointed by the Secretary, is the Chair of the OC and serves as the Executive Secretary of the Advisory Committee on Export Policy. The OC may invite representatives of other Government agencies or departments (other than those identified in this definition) to participate in the activities of the OC when matters of interest to such agencies or departments are under consideration.

* * * * *

PART 774 - [AMENDED]

33. In Supplement No. 1 to part 774 (the Commerce Control List), Category 5 - Telecommunications and Information Security

is amended by revising ECCNs 5A002, 5D002 and 5E002, to read as follows:

Category 5 - Telecommunications and Information Security

* * * * *

II. Information Security

* * * * *

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

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 only 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.

License Exceptions

LVS: N/A

GBS: N/A

CIV: N/A

List of Items Controlled

Unit: $ value

Related Controls: N/A

Related Definitions: N/A

Items:

a. Designed or modified to use "cryptography" employing digital techniques to ensure "information security";

b. Designed or modified to perform cryptanalytic functions;

c. Designed or modified to use "cryptography" employing analog techniques to ensure "information security";

Note: 5A002.c does not control the following:

1. Equipment using "fixed" band scrambling not exceeding 8 bands and in which the transpositions change not more frequently than once every second;

2. Equipment using "fixed" band scrambling exceeding 8 bands and in which the transpositions change not more frequently than once every ten seconds;

3. Equipment using "fixed" frequency inversion and in which the transpositions change not more frequently than once every second;

4. Facsimile equipment;

5. Restricted audience broadcast equipment; and

6. Civil television equipment;

d. Designed or modified to suppress the compromising emanations of information-bearing signals;

Note: 5A002.d does not control equipment specially designed to suppress emanations for reasons of health and safety.

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

f. 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;

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

Note: 5A002 does not control:

a. "Personalized smart cards" or specially designed components therefor, with any of the following characteristics:

1. Not capable of message traffic encryption or encryption of user-supplied data or related key management functions therefor; or

2. When restricted for use in equipment or systems excluded from control under the note to 5A002.c, or under paragraphs b through h of this note.

b. Equipment containing "fixed" data compression or coding techniques;

c. Receiving equipment for radio broadcast, pay television or similar restricted audience television of the consumer type, without digital encryption and where digital decryption is limited to the video, audio or management functions;

d. Portable or mobile radiotelephones for civil use (e.g., for use with commercial civil cellular radiocommunications systems) that are not capable of end-to-end encryption;

e. Decryption functions specially designed to allow the execution of copy-protected "software", provided the decryption functions are not user-accessible;

f. Access control equipment, such as automatic teller machines, self-service statement printers or point of sale terminals, that protects password or personal identification numbers (PIN) or similar data to prevent unauthorized access to facilities but does not allow for encryption of files or text, except as directly related to the password or PIN protection;

g. 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;

h. Cryptographic equipment specially designed and limited for use in machines for banking or money transactions, such as automatic teller machines, self-service statement printers or point of sale terminals.

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 controls apply to encryption software 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. License Exceptions for commodities are not applicable.

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,

and it is not eligible for the General Software Note (“mass market” treatment under License Exception TSU for mass market software). After a one-time BXA review, certain encryption software may be released from EI controls and made eligible for the General Software Note treatment as well as other provisions of the EAR applicable to software. Refer to §742.15(b)(1) of the EAR, and Supplement No. 6 to part 742.

License Exceptions

CIV: N/A

TSR: N/A

List of Items Controlled

Unit: $ value

Related Controls: N/A

Related Definitions: 5D002.a controls “software” designed or modified to use “cryptography” employing digital or analog techniques to ensure “information security”.

Items:

a. "Software" specially designed or modified for the "development", "production" or "use" of equipment or "software" controlled by 5A002, 5B002 or 5D002.

b. "Software" specially designed or modified to support "technology" controlled by 5E002.

c. Specific "software" as follows:

c.1. "Software" having the characteristics, or performing or simulating the functions of the equipment controlled by 5A002 or 5B002;

c.2. "Software" to certify "software" controlled by 5D002.c.1;

c.3. "Software" designed or modified to protect against malicious computer damage, e.g., viruses;

NOTE: 5D002 does not control:

a. "Software" "required" for the "use" of equipment excluded from control under the Note to 5A002;

b. "Software" providing any of the functions of equipment excluded from control under the Note to 5A002.

5E002 "Technology" according to the General Technology Note for the "development", "production" or use of equipment controlled by 5A002 or 5B002 or "software" controlled by 5D002.

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 controls applies only to encryption technology transferred from the U.S. Munitions 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.	

License Exceptions

CIV: N/A

TSR: N/A

List of Items Controlled

Unit: N/A

Related Controls: N/A

Related Definitions: N/A

Items:

The list of items controlled is contained in the ECCN heading.

34. In Supplement No. 2 to Part 774 the "General Software Note" is revised to read as follows:

SUPPLEMENT NO. 2 TO PART 774 - GENERAL TECHNOLOGY AND SOFTWARE NOTES

I. General Technology Note. * * *

* * * * *

II. General Software Note . License Exception TSU (“mass market” software) is available to all destinations, except Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria, for release of software that is generally available to the public by being:

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

1. Over the counter transactions;

2. Mail order transactions; or

3. Telephone call transactions; and

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

Note: License Exception TSU for mass market software does not apply to encryption software controlled for EI reasons under ECCN 5D002. Encryption software may become eligible after a one-time BXA review according to the provision of §742.15(b)(1) of the EAR.

DATED:

Sue E. Eckert

Assistant Secretary for

Export Administration