Billing Code: 3510-33-P

DEPARTMENT OF COMMERCE

Bureau of Export Administration

15 CFR Parts 734, 740, 742, 762 and 774

[Docket No. 960918265-6296-02]

RIN: 0694-AB09

Licensing of key escrow encryption equipment and software.

AGENCY: Bureau of Export Administration, Commerce

ACTION: Interim final rule.

This interim final rule amends the Export Administration Regulations (EAR) by imposing national security controls on key escrow information security (encryption) equipment and software transferred from the U.S. Munitions List to the Commerce Control List following a commodity jurisdiction determination by the Department of State.

This interim final rule also amends the EAR to exclude key escrow items from the de minimis provisions for items exported from abroad and to exclude key escrow encryption software from mass market eligibility. Further, key escrow encryption software is subject to the EAR even when made publicly available.

EFFECTIVE DATE: (THIS RULE IS EFFECTIVE: DATE OF PUBLICATION).

ADDRESSES: Written comments should be sent to Nancy Crowe, Regulatory Policy Division, Office of Exporter Services, Bureau of Export Administration, Room 2705, 14th Street and Pennsylvania Avenue, N.W., 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

In August 1995 the United States decided to ease export licensing requirements for key escrow encryption software products. As part of this decision to allow the export of these products, draft criteria were developed for key escrow products and for key holders. Products that conform to these criteria will be considered for transfer from the U.S. Munitions List to the Commerce Control List following a case-by-case determination by the Department of State through the commodity jurisdiction procedures.

Once transferred, key escrow encryption items will be controlled for national security reasons. A license will be required from the Department of Commerce to all destinations, except Canada. This is an initial step in liberalizing the treatment of encryption exports.

The Bureau of Export Administration is preparing regulations to further implement the Administration's encryption policies, which will be published in the Federal Register in the near future. These further measures are based upon the Administration's October 1, 1996 announcement of plans to make it easier for Americans to use stronger encryption products to protect their privacy, intellectual property and other valuable information, and the November 15,

1996, Presidential Memorandum and Executive Order 13026 (15 November 1996, 61 FR 58767) 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 plan to make it easier for Americans to use stronger encryption products to protect their privacy, intellectual property and other valuable information envisions a worldwide key management infrastructure with the use of key recovery and key escrow encryption items to promote electronic commerce and secure communications while protecting national security and public safety. The Memorandum sets 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.

This interim final rule amends that EAR to reflect the new licensing policy for key escrow encryption items. The Bureau of Export Administration will accept license applications for the export and reexport of key escrow encryption items in unlimited quantities for all destinations except to embargoed destinations and destinations the Secretary of State has determined to support international terrorism. Such applications will receive favorable consideration provided that, prior to the export or reexport, a key holder satisfactory to the Department of Commerce has been identified (see new Supplement No. 5 part 742) and procedures for safeguarding the key as described in a Supplement No. 5 to part 742 are established to the satisfaction of the Department of Commerce and are maintained after export or reexport as required by the EAR and any license conditions. In addition, the key escrow system must meet the criteria identified in a new Supplement No. 4 to part 742.

This interim final rule also amends part 734 of the EAR to reflect that key escrow encryption software will be subject to the EAR even when made publicly available, and to exclude key escrow encryption software and items from the de minimis provision for items. Further, this interim final rule amends part 740 of the EAR to exclude key escrow encryption software

from the mass market provisions of License Exception TSU, and amends part 762 of the EAR to clarify the additional records that must be kept for compliance with the recordkeeping provisions of the EAR.

Finally, this interim final rule also amends Supplement No. 1 to part 774 (the Commerce Control List) by clarifying that once transferred from the U.S. Munitions List (USML) to the Commerce
Control List (CCL) following a case-by-case determination by the Department of State through the commodity jurisdiction procedures, key escrow encryption items and software are controlled on the CCL under Export Control Classification Numbers 5A002.a and 5D002.c.1 respectively.

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.

Consistent with the provisions of section 6 of the Export Administration Act, a foreign policy report was submitted to Congress on (DATE OF REPORT), notifying the Congress of the Department's intention to impose foreign policy controls on key escrow encryption products.

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).

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

2. Notwithstanding any other provision of the 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, 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 1980 (44 U.S.C. 3501 et seq.). These collections have been approved by the Office of Management and Budget under control numbers 0694-0088.

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 final rule. Because a notice of proposed rulemaking and an opportunity for public comment are not required to be given for this rule under 5 U.S.C. or by any other law, the 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 final 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 (INSERT DATE 30 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, DC 20230. Records in this facility, including written public comments and memoranda summarizing the substance of oral communications, may be inspected and copied in accordance with regulations published in Part 4 of Title 15 of the Code of Federal Regulations. Information about the inspection and copying of records at the facility may be obtained from Margaret Cornejo, Bureau of Export Administration Freedom of Information Officer, at the above address or by calling (202) 482-5653.

List of Subjects

15 CFR part 734

Administrative practice and procedure, Exports, Foreign trade.

15 CFR parts 740

Administrative practice and procedure, Exports, Foreign trade, Reporting and Recordkeeping requirements.

15 CFR part 762

Administrative practice and procedures, Business and industry, Confidential business information, Export, Foreign trade, Reporting and recordkeeping requirements.

15 CFR parts 742 and 774

Exports, Foreign trade.

Accordingly, parts 734, 740, 742, 762 and 774 of the Export Administration Regulations (15 CFR Parts 730-799) are amended as follows:

1. The authority citation for 15 CFR part 734 continues to read as follows:

Authority: 50 U.S.C. app. 2401 et seq.; 50 U.S.C. 1701 et seq.; E.O. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; E.O. 12938, 59 FR 59099, 3 CFR, 1994 Comp., p. 950; 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).

2. The authority citation for 15 CFR part 740 continues to read as follows:

Authority: 50 U.S.C. app. 2401 et seq.; 50 U.S.C. 1701 et seq.; E.O. 12924, 59 FR

43437, 3 CFR, 1994 Comp., p. 917; 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 742 continues to read as follows:

Authority: 50 U.S.C. app. 2401 et seq.; 50 U.S.C. 1701 et seq.; 18 U.S.C. 2510 et seq.; 22 U.S.C. 3201 et seq.; 42 U.S.C. 2139a; E.O. 12058, 43 FR 20947, 3 CFR, 1978 Comp., p. 179; E.O. 12851, 58 FR 33181, 3 CFR, 1993 Comp., p. 608; E.O. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; E.O. 12938, 59 FR 59099, 3 CFR, 1994 Comp., p. 950; 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 part 762 continues to read as follows:

Authority**:** 50 U.S.C. app. 2401 et seq.; 50 U.S.C. 1701 et seq.; E.O. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; 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 774 continues to read as follows:

Authority: 50 U.S.C. app. 2401 et seq.; 50 U.S.C. 1701 et seq.; 10 U.S.C. 7420; 10 U.S.C. 7430(e); 18 U.S.C. 2510 et seq.; 22 U.S.C. 287c; 22 U.S.C. 3201 et seq.; 22 U.S.C. 6004; 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).

PART 734 - [AMENDED]

6. Section 734.3 is amended by redesignating paragraphs (b)(3)(i) through (b)(3)(iv) as (b)(3)(i)(A) through (b)(3)(i)(D), and adding a new paragraph (b)(3)(ii) to read as follows:

(b) * * *

(3)(i) * * *

(ii) Key escrow encryption software controlled under ECCN 5D002.c.1 remains subject to the EAR even when made publicly available (see Supplement No. 1 to part 774 of the EAR).

7. 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) Key escrow encryption software controlled under ECCN 5D002.c.1 or equipment designed or modified to use key escrow encryption items controlled under ECCN 5A002.a.

transferred from the U.S. Munitions List following a case-by-case determination by the Department of State through the commodity jurisdiction procedure.

* * * * *

(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 key escrow encryption software controlled under ECCN 5D002.c.1 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.

8. Section 734.7 is amended by revising paragraph (b) 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). Note that key escrow encryption software controlled under ECCN 5D002.c.1 remains subject to the EAR even when made publicly available (see Supplement No. 1 to part 774 of the EAR).

PART 740 - LICENSE EXCEPTIONS

9. Section 740.8 is amended by redesignating paragraph (d)(2) as (d)(3) and adding a new paragraph (d)(2) to read as follows:

§740.8 Technology and software - unrestricted.

* * * * *

(d) * * *

(2) Software not eligible for this License Exception. This License Exception is not available for key escrow encryption software controlled by ECCN 5D002.c.1.

PART 742 - [AMENDED]

10. Part 742 is amended by adding a new §742.15, and new Supplements 4 and 5 to read as follows:

§742.15 Key escrow encryption items.

(a) License requirements. Licenses are required for all destinations, except Canada, for key escrow encryption software controlled under ECCN 5D002.c.1; and equipment designed or modified to use key escrow encryption items controlled under ECCN 5A002.a.

(b) Licensing policy. BXA will accept license applications for the export and reexport of key escrow encryption software controlled by ECCN 5D002.c.1 and equipment designed or modified to use key escrow encryption software controlled by ECCN 5A002.a in unlimited quantities for all destinations except Country Groups E:1 and E:2 (see Supplement No. 1 to part 742), Iran, Syria, and Sudan. Such applications will receive favorable consideration

provided that, prior to the export or reexport, keys are escrowed with a key holder satisfactory to the Department of Commerce (see Supplement No. 5 to this part) and procedures for safeguarding the key as described in Supplement No. 5 to this part are established to the satisfaction of the Department of Commerce and are maintained after export or reexport as required by the EAR and any license conditions. In addition, the key escrow system must meet the criteria identified in Supplement No. 4 to this part. This includes a legally binding arrangement between the exporter or reexporter and the key holder, satisfactory to BXA, which ensures that appropriate key escrow safeguard procedures will be carried out by the key holder. If the exporter or reexporter intends to be the key holder, then the exporter or reexporter must meet all of the requirements of a key holder. Continuing compliance by the key holder with the key safeguard procedures shall be made a condition of any license issued. Because BXA will be relying on representations and undertakings of the key holder to make decisions on license applications, the key holder is required to comply with all applicable record requirements in the EAR, including the record retention requirements. In addition, the key holder shall be required to 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. Applicants should list in their license applications those countries for which they seek approval to export or reexport, or identify that you seek export or reexport to all destinations except Country Groups E:1 and E:2, Iran, Syria, and Sudan.

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

(d) [Reserved]

* * * * *

SUPPLEMENT NO. 4 TO PART 742 - KEY CRITERIA

Key Recovery Feature

1) The key(s) required to decrypt the product's key escrow cryptographic functions ciphertext shall be accessible through a key escrow feature.

2) The product's key escrow cryptographic functions shall be inoperable until the key is or the keys are escrowed in accordance with the criteria identified in Supplement 5 to this part.

3) The product's key escrow cryptographic functions ciphertext shall contain, in an accessible format and with a reasonable frequency, the identity of the key escrow holder(s) and information sufficient for the recovery holder(s) to identify the keys required to decrypt the ciphertext.

4) The product's key escrow feature shall allow access to the key(s) needed to decrypt the product s ciphertext regardless of whether the product generated or received the ciphertext.

5) The product's key escrow feature shall allow for the recovery of multiple decryption keys during the period of authorized access without requiring repeated presentations of access authorization to the key escrow holder(s).

Key Length Feature

6) The product's key escrow functions shall use an unclassified encryption algorithm.

Interoperability Feature

7) The product's cryptographic functions shall interoperate only with other key escrow

products that meet these criteria, and shall not interoperate with products whose key escrow feature has been altered, bypassed, disabled, or otherwise rendered inoperative. Key escrow products shall interoperate with non-key escrow products only when the key escrow product permits access to the keys or other escrowed material/information needed to decrypt ciphertext generated or received by the key escrow product.

Design, Implementation and Operational Assurance

8) The product shall be resistant to efforts to disable or circumvent the attributes described in criteria one through seven.

SUPPLEMENT NO. 5 TO PART 742 - KEY HOLDER REQUIREMENTS; SAFEGUARD PROCEDURES; KEY ESCROW PROCEDURES

This Supplement sets forth criteria that BXA, in consultation with other departments and agencies, will use to approve key holders to support approval of the export or reexport of key escrow encryption items controlled by ECCNs 5A002.a and 5D002.c.1. Any arrangements between the exporter or reexporter and the key holder must reflect the provisions contained in this Supplement in a manner satisfactory to BXA. This Supplement also outlines the criteria for employing key holder personnel and key escrow procedures. An applicant for a license to export or reexport key escrow encryption items shall provide, or cause the proposed key holder to provide, to BXA sufficient information concerning any proposed key holder arrangements to permit BXA to evaluate the key holder's safeguard procedures, suitability and trustworthiness to maintain the confidentiality of the key and key components, and its key escrow procedures. The key holder may be the applicant for the export or reexport license or another party legally obligated to the applicant to provide recovery services, as approved by BXA. BXA retains the right, in addition to any other remedies, to revoke export or reexport licenses if a key holder no longer meets these criteria. The safeguard procedures, procedures

related to the key holder's suitability and trustworthiness, and key escrow procedures of the key holder generally shall be made terms and conditions of the export or reexport license for key escrow encryption software if granted. BXA may require the key holder to provide a representation that it will comply with such terms and conditions.

(a) Key holder requirements.

(1) To become a qualified key holder, the key holder's personnel involved in the recovery of keys with access to escrowed keys or key escrow access request information, or in responding to key escrow requests, and persons in control of the key holder with access or authority to obtain access to keys or key components must be suitable and trustworthy as determined by the Bureau of Export Administration prior to export or reexport of the recovery product, and BXA may evaluate and determine the suitability and trustworthiness of such personnel thereafter from time to time. Evidence of an individual's suitability and trustworthiness could include:

(i) Information indicating the individual(s):

(A) Have no felony convictions or pending felony charges;

(B) Are not currently serving a term of probation;

(C) Have satisfactorily performed any positions of a fiduciary nature, for example have had no violations of surety or performance bonds; and

(D) Have favorable results of criminal background and credit checks; or

(ii) Have an active U.S. government security clearance of secret or higher issued or updated within the last five years.

(2) Suitable evidence of the key holder's corporate viability and financial responsibility (e.g. a certificate of good standing from the state of incorporation, credit reports, and errors/omissions insurance) must be submitted with an application to export or reexport key escrow item.

(3) Key holder operating procedures shall provide for the designation of individual(s) to be responsible as security and operations officers.

(4) Upon the request of BXA, key holders shall provide to BXA information concerning compliance with or violations of federal, state, and local laws and regulations determined by BXA to be relevant to the evaluation of trustworthiness of the key holders, its personnel, and persons in control of the key holder.

(5) Policies and procedures shall be designed and implemented to preclude disclosure of keys or key components to additional persons in control not previously authorized by BXA. For purposes of these criteria in this Supplement No. 5, a person in control is each of the following:

(A) A person with the power, direct or indirect, whether exercised or not exercised, and whether or not exercisable, through the ownership of the key holder's securities, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of the key holder in a manner which may result in the unauthorized disclosure of a key or key component or a breach of the terms and conditions of an export or reexport license;

(B) A person with ownership or beneficial ownership, direct or indirect, of 5 percent or more of the key holder's voting securities;

(C) A person with ownership or beneficial ownership, direct or indirect, of 25

percent or more of the key holder's non-voting securities;

(D) Management positions, such as directors, officers, or executive personnel of the key holder held by non U.S. citizens;

(E) A person with the power, direct or indirect, to control the election, appointment, or tenure of directors, officers, or executive personnel of the key holder; or

(F) A person with a contract, agreement, understanding, or arrangement to manage the key holder.

(b) Safeguard procedures.

(1) Key holders must implement safeguard procedures that assure the confidentiality, integrity, and availability of the key to key escrow encryption software or key products.

(i) Procedures to assure the confidentiality of this information may include:

(A) Encrypting all keys or key components while in storage, transmission, or transfer; or

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

(ii) Procedures to assure the integrity of the recovery database (i.e. assuring the recovered key/key components are protected against unauthorized changes) may include the use of access controls based on an appropriate use of database password controls, digital signatures, system auditing, and physical access restrictions.

(iii) Procedures to assure the availability of the recovery database (i.e. assuring recovered keys/key components are retrievable at any time) may include system redundance, physical security, and the use of cryptography to control access.

(2) Policies and procedures shall be designed and implemented so that a failure by a single person, procedures, or mechanism does not compromise key or key component confidentiality, integrity and availability. Such measures could include two person control of access to recoverable keys, split keys, and back-up capabilities.

(3) Key holders shall implement policies that protect against unauthorized disclosure of information regarding the identity of owners or end users of encryption products whose keys are recoverable, the fact that a key or key component was requested or provided, and the identity of a requester. Procedures to assure the confidentiality of this information could include those described in paragraph (a)(1)(i).

(4) Policies and procedures shall be designed and implemented to provide notice to BXA of a compromise of the confidentiality of a key or key component, or other safeguards.

(c) Key escrow procedures.

(1) In the event the key holder dissolves or otherwise terminates recovery operations, or if BXA determines that there is a risk of such dissolution or termination, or if BXA determines the key holder is no longer suitable or trustworthy, then the key holder must transfer all of its recovery equipment and recovered information to another key holder that is approved by the Bureau of Export Administration.

(2) Key holders will maintain the ability to make the key available in accordance with appropriate State and Federal legal authority until notified otherwise by BXA. Key holders shall make requested keys and key components 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 that requires or compels the key holder to produce the key or key components. The requesting government agency will be responsible for obtaining the keys or key components from the key holder.

(3) Key holders shall enter keys and key components into the recovery data base upon receipt of new or replacement keys and key components.

(4) Key holders must agree to maintain data regarding key requests received, keys and key components released, database changes, system administration access, dates of such events, etc., for purposes of audits by BXA.

11. Section 762.2 is amended by redesignating paragraphs (b)(6) through (b)(34) as (b)(7) through (b)(35) and adding a new paragraph (b)(6) to read as follows:

§762.2 Records to be retained.

(a) * * *

(b) * * *

(6) Section 742.15;

PART 774 - [AMENDED]

12. In Supplement No. 1 to part 774 (the Commerce Control List), Category 5 (Telecommunications and Information Security), the Information Security category, ECCNs 5A002 and 5D002 are amended to read as follows:

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

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";

Note: 5A002.a includes controls key escrow encryption items transferred from the U.S. Munitions List following a case- by-case determination by the Department of State through the commodity jurisdiction procedure. (See §742.15 of the EAR)

b. Designed or modified to perform cryptoanalytic 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 Be 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

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

Note: Key escrow encryption software controlled under 5D002.c.1. remain subject to the EAR even when made publicly available in accordance with §734.7 of the EAR, and it is not eligible for mass market treatment under License Exception TSU for mass market software. See §742.15(b)(1) of the EAR.

License Exceptions

GBS: N/A
CIV: N/A

List of Items Controlled

Unit: $ value
Related Controls: NA
Related Definitions: N/A
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;

Note: 5D002.c.1 includes controls key escrow encryption software transferred from the U.S. Munitions List following a case-by-case determination by the Department of State through the commodity jurisdiction procedure. See §742.15 of the EAR.

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.

13. Supplement No 2 to Part 774 is revised to read as follows:

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

NOTES

* * * * *

2. General Software Note. License Exception TSU (mass market software) is available to all destinations, except Cuba, Iran, 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 key escrow encryption software controlled under ECCN 5D002.c.1. that has been transferred from the U.S. Munitions List following a commodity jurisdiction determination by the Department of State.

DATED:

Sue E. Eckert
Assistant Secretary for
Export Administration