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 U.S. 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 743
SPECIAL REPORTING

Sec.

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; Notice of August 15,

1995, 3 CFR, 1995 Comp., p. 501; Notice of August 14, 1996, 3 CFR, 1996 Comp., p. 289; and Notice of August 13, 1997 (62 FR 43629, August 15, 1997).

§743.1 Wassenaar Arrangement.

(a) *Scope.* This section outlines special reporting requirements for exports of certain commodities, software and technology controlled under the Wassenaar Arrangement. Such reports must be submitted to BXA semiannually in accordance with the provisions of paragraph (f) of this section, and records of all exports subject to the reporting requirements of this section must be kept in accordance with part 762 of the EAR. This section does not require reports for reexports.

(b) *Requirements.* You must submit two (2) copies of each report required under the provisions of this section and maintain accurate supporting records (see §762.2(b) of the EAR) for all exports of items specified in paragraph (c) of this section under any of the following License Exceptions authorized by part 740 of the EAR: icense Exceptions GBS, CIV, TSR, LVS, CTP, and GOV. For purposes of this part 743, ''you'' has the same meaning as ''U.S. exporter'', as defined in part 772 of the EAR.

(c) *Items for which reports are required.*

(1) You must submit reports to BXA under the provisions of this section only for exports of items controlled under the following ECCNs:

(i) *Category 1:* 1A002, 1C007.c and .d, 1C010.c and .d, 1D002, 1E001, 1E002.e, and 1E002.f.;

(ii) *Category 2:* 2B001.a or .b (certain items only; see Note to this paragraph) 2B001.f, 2B003, 2D001, 2E001, and 2E002;

Note to paragraph (c)(1)(ii): The following are not controlled for NP reasons: turning machines controlled by 2B001.a with a capacity equal to or less than 35 mm diameter; bar machines (Swisstурn), limited to machining only bar feed through, if maximum bar diameter is equal to or less than 42 mm and there is no capability of mounting chucks (machines may have drilling and/or milling capabilities for machining parts with diameters less than 42 mm); or milling machines controlled by 2B001.b with x-axis travel greater than two meters and overall ''positioning accuracy'' on the x-axis more (worse) than 0.030 mm. Therefore, exports of such items under License Exception GOV are subject to reporting requirements.

(iii) *Category 3:* 3A002.g.2, 3B001.a.2, 3D001, and 3E001;

(iv) *Category 4:* 4A001.a.2 and .b, 4A003.b and .c (see paragraph (c)(2) of this section), 4D001, 4D003.c, and 4E001;

(v) *Category 5:* 5A001.b.8, 5B001 (items specially designed for 5A001.b.8), 5D001.a and .b, 5E001.a, 5A002, 5B002, 5D002, and 5E002;

(vi) *Category 6:* 6A001.a.1.b, .a.2.c, .a.2.d, and .a.2.e; 6A002.b, 6A004.c and d, 6A006.g and h, 6A008.d, .h, and .k; 6D001, 6D003.a, 6E001, and 6E002;

(vii) *Category 8:* 8A001.c; 8A002.b, .h, .j, .o.3.a, and .p; 8D001, 8D002, 8E001, and 8E002.a; and

(viii) *Category 9:* 9B001.b, 9D001, 9D002, 9D004.a and .c, 9E001, 9E002, 9E003.a.1, 9E003.a.2, .a.3, .a.4, .a.5, .a.8, and .a.9.

(2) Reports for ''digital computers'' and ''electronic assemblies'' controlled under ECCN 4A003.b and .c are required only for computers with a composite theoretical performance (CTP) exceeding 4,000 MTOPS or computer enhancements thereof such that the CTP exceeds 4,000 MTOPS. Records for software controlled by 4D001 are required for software specially designed for the development or production of computers having a CTP exceeding 4,000 MTOPS. For the calculation of CTP, see the Technical Note for Category 4 in the Commerce Control List (Supplement No. 2 to part 774 of the EAR).

(d) *Country Exceptions.* You must report each export subject to the provisions of this section, except for exports to countries identified in Country Group A:1 (see Supplement No. 1 to part 740 of the EAR).

(e) *Information that must be included in each report.*

(1) Each report submitted to BXA for items other than those identified in paragraph (e)(2) of this section must include the following information for each export during the time periods specified in paragraph (f) of this section:

(i) Export Control Classification Number and paragraph reference as identified on the Commerce Control List;

(ii) Number of units in the shipment; and

(iii) Country of ultimate destination.

(2) Reports for ''digital computers'' and ''electronic assemblies'' controlled under ECCN 4A003.b and .c must include the following information:

(i) Date of shipment;

(ii) Name and address of the end-user and each intermediate consignee;

(iii) CTP of each computer or aggregation of computing elements in shipment;

(iv) Quantity shipped; and

(v) End-use.

(f) *Frequency and timing of reports.* You must submit reports subject to the provisions of this section semiannually. The reports must be labeled with the exporting company's name and address at the top of each page and must include for each such export all the information specified in paragraph (e) of this section. The reports shall cover exports made during six month time periods spanning from January 1 through June 30 and July 1 through December 31.

(1) The first report must be submitted to and received by BXA no later than August 1, 1998 for the partial reporting period beginning January 15, 1998 and ending June 30, 1998. Thereafter, reports are due according to the provisions of paragraphs (f)(2) and (f)(3) of this section.

(2) Reports for the reporting period ending June 30 must be submitted to and received by BXA no later than August 1.

(3) Reports for the reporting period ending December 31 must be submitted to and received by BXA no later than February 1.

(g) *Mailing address and facsimile number:*

(1) Two (2) copies of reports required under this section shall be delivered to one of the following addresses. BXA will not accept reports sent C.O.D.

(i) For deliveries by U.S. postal service:

Bureau of Export Administration, U.S. Department of Commerce, P.O. Box 273, Attn: ''Wassenaar Reports'', Washington, D.C. 20044

(ii) For courier deliveries:

Bureau of Export Administration, U.S. Department of Commerce, Attn: ''Wassenaar Reports'', Room 2705, 14th Street and Pennsylvania Ave., N.W., Washington, D.C. 20230

(2) Reports may also be sent by facsimile to: (202) 482-3345, Attn: ''Wassenaar Reports''.

(h) *Contacts.* General information concerning the Wassenaar Arrangement and reporting obligations thereof is available from the Office of Strategic Trade and Foreign Policy Controls, Tel. (202) 482-0092, Fax: (202) 482-4094.

§743.2 [Reserved]

PART 744
CONTROL POLICY: END-USER AND END-USE BASED

Sec.

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. 915; E.O. 12938, 59 FR 59099, 3 CFR, 1994 Comp., p. 950; Notice of August 14, 1996, 3 CFR, 1996 Comp., p. 298; and Notice of August 13, 1997 (62 FR 43629, August 15, 1997).

§744.1 General provisions.

(a) *Introduction.* In this part, references to the EAR are references to 15 CFR chapter VII, subchapter C. This part contains prohibitions against exports, reexports, and selected transfers to certain end-users and end-uses as introduced under General Prohibition Four (Denial Orders) and prohibitions against exports or reexports to certain end-uses as introduced, under General Prohibition Five (End-use/End-users). Sections 744.2, 744.3, 744.4, and 744.5 prohibit exports and reexports of items subject to the EAR to defined nuclear, missile, chemical and biological weapons, and nuclear maritime end-uses. Section 744.6 prohibits certain activities by U.S. persons in support of certain nuclear, missile, chemical, or biological end-uses regardless of whether that support involves the export or reexport of items subject to the EAR. Sections 744.7 and 744.8 prohibit exports and reexports of certain items for certain aircraft and vessels. In addition, these sections include license review standards for export license applications submitted as required by these sections. It should also be noted that part 764