HEINONLINE

Citation: 7 Bernard D. Reams Jr. Law of E-SIGN A Legislative
of the Electronic Signatures in Global and National
Act Public Law No. 106-229 2000 62600 2002

Content downloaded/printed from
HeinOnline (http://heinonline.org)
Sun Apr 21 23:12:34 2013

-- Your use of this HeinOnline PDF indicates your acceptance
of HeinOnline's Terms and Conditions of the license
agreement available at http://heinonline.org/HOL/License

-- The search text of this PDF is generated from
uncorrected OCR text.

U.S. Department of Commerce, 14th Street and Constitution Avenue, Washington, DC 20230; telephone: (202) 482–4060, FAX: (202) 482–5650, and E-Mail: bbotwin@bxa.doc.gov.

SUPPLEMENTARY INFORMATION:

Background

Section 232 of the Trade Expansion Act of 1962, as amended (19 U.S.C. 1862) (the Act) authorizes investigations to determine the effects on the national security of imports of articles which are the subject of a request or application for an investigation. The implementing regulation, "Effect of Imported Articles on the National Security" (15 CFR Part 705)), prescribes procedures to be followed by the Department of Commerce (the Department) to commence and conduct such investigations.

Consistent with amendments in 1995 to the Paperwork Reduction Act of 1980 to reduce the paperwork burden on persons submitting a request or application for an investigation, section 705.5 of this regulation is being amended to reduce the number of copies of a request or application for and investigation to be filed with the Department from 12 copies to 1 copy, plus the original.

Accordingly, section 705.5 of the regulation is revised to require that an original and 1 copy of a request or application for an investigation be filed with the Director, Office of Strategic Industries and Economic Security, Room 3876, U.S. Department of Commerce, Washington, DC 20230.

Rulemaking Requirements

The Department has made certain determinations with respect to the following rulemaking requirements:

1. This final rule has been determined to be not significant for purposes of Executive Order 12866.

2. Notwithstanding any other provision of law, no person is required to, nor shall a person be subject to a penalty for failure to comply with a collection of information, subject to 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 (U.S.C. 3501 *et seq.*). This regulation involves collections previously approved by the Office of Management and Budget under Control Number 0694–0120, "Procedure to Initiate an Investigation Under the Trade Expansion Act of 1962", which carries a burden hour estimate of 12 hours per submission.

3. *Executive Order 13132:* This proposed rule does not contain policies with Federalism implications sufficient to warrant preparation of a Federalism assessment under E.O. 13132.

4. *Administrative Procedure Act and Regulatory Flexibility Act:* 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 relates to agency procedures (Sec. 5 U.S.C. 553 (b)(A)). Further, no other law requires that a notice of proposed rulemaking and an opportunity for public comment be given for this 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. 553 or by any other law, the analytical requirements of the Regulatory Flexibility Act (5 U.S.C. 601 *et seq.*) are not applicable.

List of Subjects in 15 CFR Part 705

Administrative practice and procedure, Business and industry, Classified information, Confidential business information, Imports, Investigations, National Security.

For the reasons set forth in the preamble, part 705 of Chapter VIII, Subchapter A, National Security Industrial Base Regulations (15 CFR part 705) is amended as follows:

PART 705—[AMENDED]

1. The authority citation for Part 705 is revised to read as follows:

Authority: Sec 232, Trade Expansion Act of 1962, as amended (19 U.S.C. 1862)

2. Section 705.5 is amended by revising paragraph (a) to read as follows:

§ 705.5 Request or application for an investigation.

(a) A request or application for an investigation shall be in writing. The original and 1 copy shall be filed with the Director, Office of Strategic Industries and Economic Security, Room 3876, U.S. Department of Commerce, Washington, DC 20230.

* * * * *

Dated: October 11, 2000.

R. Roger Majak,

Assistant Secretary for Export Administration.

[FR Doc. 00–26780 Filed 10–18–00; 8:45 am]

BILLING CODE 3510–JT–P

DEPARTMENT OF COMMERCE

Bureau of Export Administration

15 CFR Parts 732, 734, 740, 742, 744, 748, 770, 772 and 774

[Docket No. 001006282–0282–01]

RIN 0694–AC32

Revisions to Encryption Items

AGENCY: Bureau of Export Administration, Commerce.

ACTION: Final rule.

SUMMARY: This rule amends the Export Administration Regulations (EAR) and implements the July 17 White House announcement to streamline the export and reexport of encryption items to European Union (EU) member states, Australia, Czech Republic, Hungary, Japan, New Zealand, Norway, Poland and Switzerland under License Exception ENC. The 30-day waiting period and the previous distinction between government and non-government end-users are removed by this rule for these destinations. This rule makes further revisions and clarifications to the rule published on January 14, 2000 including changes in the treatment of products incorporating short-range wireless technologies, open cryptographic interfaces, beta test software, encryption source code, and U.S. content (*de minimis*) requirements. This rule also allows, for the first time, exporters to self-classify unilateral controlled encryption products (that fall under Export Control Classification Numbers (ECCNs) 5A992, 5D992 and 5E992) upon notification to the Bureau of Export Administration (BXA). Restrictions on exports by U.S. persons to terrorist-supporting states (Cuba, Iran, Iraq, Libya, North Korea, Sudan or Syria), their nationals and other sanctioned entities are not changed by this rule.

DATES: This rule is effective October 19, 2000.

FOR FURTHER INFORMATION CONTACT: James A. Lewis, Director, Office of Strategic Trade, at (202) 482–4196.

SUPPLEMENTARY INFORMATION:

Background

On July 17, 2000, the United States announced further updates to its encryption export policy coinciding with the recent regulations adopted by the European Union which ease exports among 23 countries. This action is consistent with the Administration's decision to ensure that U.S. companies are not disadvantaged by such changes and will be able to compete effectively

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 62600 2002

in these markets. Post-export reports were examined and action taken for the requirements to more accurately reflect companies' business models. The rule further streamlines reexport controls by considering certain components and software for *de minimis* treatment. The review of *de minimis* eligibility will take into account national security interests. These steps continue to serve the full range of national interests: promote electronic commerce, support law enforcement and national security and protect privacy.

Specifically, this rule amends the EAR in the following ways:

1. In § 732.2 (Steps Regarding Scope of the EAR) conforming changes are made with respect to *de minimis* consideration for encryption items controlled under ECCNs 5A002 and 5D002, as described in paragraph (2) below.

2. In § 734.4 (*De Minimis* U.S. Content), software controlled under ECCN 5D002 eligible for export under the "retail" or "source code" provisions of license exception ENC and parts and components controlled under ECCN 5A002 may be made eligible for *de minimis* treatment after review and classification by BXA. As a result of this change, certain U.S. origin encryption items, incorporated into foreign products, which were previously prohibited from *de minimis* consideration, may now be made eligible in a process similar to that used now for retail determinations. Examples include retail operating systems and desktop applications (e.g. e-mail, browsers, games, word processing, database, financial applications or utilities) designed for, bundled with, or pre-loaded on single CPU computers, laptops, hand-held devices, or components or software designed for use in retail communication devices (e.g. wireless devices or smart cards), or decontrolled products. Exporters applying for *de minimis* eligibility must explain why the part or component would qualify for *de minimis* treatment in the support documents included with the classification request. *De minimis* eligibility continues to apply to encryption items controlled under ECCNs 5A992, 5D992 and 5E992.

3. § 740.9 (Temporary imports, exports and reexports (TMP)), now includes encryption software controlled for EI reasons under ECCN 5D002 to be allowed under the beta test provisions of License Exception TMP. The exporter must provide BXA the information described in Supplement 6 to Part 742 by the time of export. Exporters should note that any final resulting product will require review and classification under the provisions of § 740.17. Names and addresses of the testers, except individual consumers, and the name and version of the beta software are to be reported every six months consistent with § 740.17(e)(5). Encryption software controlled under ECCN 5D992 is eligible for this beta test provision.

4. § 740.13 (Technology and Software Unrestricted (TSU)) clarifies the treatment of open source object code. Object code compiled from source code eligible for License Exception TSU can also be exported under the provisions of License Exception TSU if the requirements of § 740.13 are met and no fee or payment is required for object code (other than reasonable and customary fees for reproduction and distribution). Object code for which there is a fee or payment can be exported under the provisions of 740.17(b)(4)(i). The intent of this section is to release publicly available software available without charge (e.g. "freeware") from control. Also in § 740.13, crypt@bxa.doc.gov address is added to prompt exporters to notify BXA electronically. Exporters should note the intent of the phrase "released from EI controls" in 740.13(e) means that 5D002 software eligible for TSU is released from the mandatory access controls procedures described in 734.2(b)(9)(ii).

5. In § 740.17 (Encryption Commodities and Software (ENC)), language is added to further streamline the export and reexport of encryption items under License Exception ENC and to parallel the changes adopted by the EU. Please note that the paragraph numbering was changed in this section to simplify the structure and provide for more changes to License Exception ENC. License Exception ENC (Encryption Commodities and Software) is revised as follows:

a. § 740.17 begins with an introductory paragraph describing the commodity and country scope of License Exception ENC.

b. § 740.17(a) adds a provision to allow all encryption items, except for "cryptanalytic products," as specified in ECCN 5A002.a.2 and the software and technology relating to these cryptanalytic commodities (defined in part 772), to be exported to EU member states, Australia, Czech Republic, Hungary, Japan, New Zealand, Norway, Poland and Switzerland (listed in Supplement 3 to Part 740), under License Exception ENC provided the exporter has submitted to BXA a completed classification request by the time of export. Exports and reexports to foreign subsidiaries or offices of firms, organizations and governments headquartered in Canada or in the above-listed countries for internal use are also eligible under this provision.

c. § 740.17(b) adds an introductory paragraph for the provisions set out under License Exception ENC for exports to countries outside of those listed in Supplement 3 to part 740, as well as for exports and reexports of items which provide an open cryptographic interface.

d. § 740.17(b)(1) (Encryption Items to U.S. Subsidiaries) is revised to clarify that foreign nationals, who may not be permanent employees (contractors, interns, etc.) working for U.S. companies are eligible to receive technology controlled under ECCN 5E002 in the United States under License Exception ENC. Note that all encryption items produced or developed by U.S. subsidiaries continue to be subject to the EAR and require review and classification before any sale or retransfer outside of the U.S. company.

e. In § 740.17(b)(2)(i) (Encryption Commodities and Software), any encryption commodity, general purpose toolkit, software and component is authorized for export or reexport, after review and classification by BXA under ECCNs 5A002 and 5D002, to any individual, commercial firm or other non-government end-user located outside the countries listed in Supplement 3 to Part 740 under License Exception ENC. Exporters should note that a license is still required for exports to government end-users in these destinations. In addition, to further streamline License Exception ENC, the provisions for general purpose toolkits is moved from paragraph (a)(5) to this paragraph (b)(2)(i).

f. In § 740.17(b)(2)(ii) (Encryption Commodities and Software), to simplify the regulation, the paragraph on Internet or telecommunications service providers was deleted and the part relating to products not classified as retail was moved to this paragraph. Note that Internet and telecommunications service providers may now provide services to the governments of the countries listed in Supplement 3 to Part 740 under License Exception ENC. Such exports previously required a license under former paragraph (a)(4). Exporters should note that a license is still required for exports to government end-users located in other destinations.

g. In § 740.17(b)(3) (Retail Encryption Commodities and Software), License Exception ENC is revised to authorize, without prior review and classification or reporting, those items which are controlled only because they incorporate components providing

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 62601 2002

encryption functionality which is limited to short-range wireless encryption, such as those based on the Bluetooth and Home Radio Frequency (HomeRF) specifications. Examples of such products include audio devices, cameras and videos, computer accessories, handheld devices, mobile phones and consumer appliances (*e.g.*, refrigerators, microwaves and washing machines). The part of the Internet or telecommunications service providers paragraph relating to obtaining retail products under License Exception ENC and using them to provide service to any entity is moved to this paragraph. As a result of this revision, former paragraph (a)(4) (Internet and Telecommunications Service Providers) is removed.

h. Additional changes are made under § 740.17(b)(3). In paragraph (i)(C), a clarification is made to allow the retail provisions to include anticipated sales by changing the phrase "sold in large volume" to "which are sold or will be sold in large volume." To further streamline the encryption controls, exporters may now export and reexport finance-specific encryption products and 56-bit products (with key exchange mechanisms greater than 512 bits and up to and including 1024 bits) immediately after submitting a completed classification request to BXA. As a result, the former paragraphs (a)(3)(vi) and (vii), which relate to these items, are combined into one paragraph.

i. § 740.17(b)(4) (Commercial encryption source code) is revised to clarify that object code resulting from the compiling of source code which would be considered publicly available and eligible for export under License Exception ENC or TSU can also be exported or reexported under ENC if the requirements of § 740.17(b)(4)(i) are otherwise met. Commercial encryption source code which would not be considered publicly available may now be exported or reexported using License Exception ENC to any non-government end-user immediately after submitting a completed classification request. Requirements for source code containing an open cryptographic interface are addressed separately in paragraph (b)(5). For the purpose of streamlining the provisions of License Exception ENC, references to general purpose toolkits are removed and are now addressed in § 740.17(b)(2) and (c).

j. § 740.17(b)(5) (Cryptographic interfaces) is added to authorize the export and reexport of encryption commodities, software and components which provide an open cryptographic interface to any end-user located in the countries listed in Supplement 3 to Part 740 under License Exception ENC. Exports and reexports to other destinations continue to require a license except to subsidiaries of a U.S. company for their internal use. This paragraph also permits encryption products that enable foreign developed products to operate with U.S. products (e.g. digitally signing) to be exported or reexported to any eligible end-user. The foreign "enabled" product is not subject to review, however, and limited reporting is required as specified in § 740.17(e)(3).

k. § 740.17(c) (Reexports and Transfers) is added by combining the transfer provisions of paragraph (c) with former paragraph (d) relating to exports and reexports of foreign products incorporating U.S. encryption source code, components or general purpose encryption toolkits, former paragraph (h) relating to distributors and resellers, and the related provisions of former paragraph (b)(5)(iv).

l. In § 740.17(d),(Eligibility for License Exception ENC), conforming changes are made to review and classification requirements and grandfathering provisions to take into account the new policy that allows most exports of encryption to the countries listed in Supplement 3 to Part 740.

m. In § 740.17(e) (Reporting requirements), new paragraphs are added to eliminate reporting requirements for consumer products incorporating short-range wireless encryption, client Internet appliance and client wireless LAN cards, and for retail operating systems or desktop applications (e.g., browsers, e-mail, word processing, database, games, financial applications or utilities) designed for, bundled with, or preloaded on single CPU computers , laptops or handheld devices. In addition, a new paragraph is added to eliminate reporting requirements for foreign products developed by bundling or compiling of source code. This rule clarifies that exporters must report only exports to subsidiaries of U.S. companies when the U.S. subsidiary is reselling or distributing the product. The reporting obligation is consistent with the provisions for distributors or resellers. Lastly, since exporters may now export technology to the countries listed in Supplement 3 to Part 740 under License Exception ENC, the semi-annual reports require the name and address of the manufacturer using the technology when intended for use in foreign products developed for commercial sale and a non-proprietary technical description of what is being developed using that technology. For further streamlining, the requirement of reporting exports to Internet and telecommunication service providers immediately is removed. These exports are now reported consistent with the semi-annual time frames.

n. Remaining reporting requirements are streamlined to reflect business models normally used by exporters. Note that reporting for exports and reexports of encryption components can be adjusted or reduced, on a case-by-case basis, provided an exporter supplies BXA with sufficient information during the initial technical review of the U.S. encryption component concerning its incorporation in a final foreign product. Companies should request such adjustments or reductions from BXA to ensure that reporting requirements reflect their business model.

o. Supplement No. 3 to Part 740 is created to identify those countries which are now eligible for the expanded treatment under License Exception ENC based on the new policy.

6. § 742.15 (Encryption Items) revises the licensing policy for export and reexports of encryption items, as follows:

a. The license requirements section is streamlined.

b. Combines into one paragraph (1)(i) the former subparagraphs which individually described the eligibility for 56-bit encryption items, key management products and 64-bit mass market encryption commodities and software. In addition, adds a provision to allow exporters to self-classify these encryption items under ECCNs 5A992, 5D992, and 5E992. After submitting the information described in paragraphs (a) through (e) of Supplement 6 to part 742 to BXA, these encryption items may be exported and reexported as "NLR" (No License Required). This submission is not a classification and no response is required from BXA for shipment.

c. Removes the requirement that all products developed using U.S. encryption items are subject to the EAR. This clarifies that *de minimis* eligibility applies for encryption commodities controlled under ECCNs 5A992, 5D992 and 5E992. In addition, BXA may apply, on a case-by-case basis, the *de minimis* rule to foreign products incorporating 5A002 and 5D002 parts, components and software which are eligible for export under the "retail" or "source code" provisions of License Exception ENC.

d. Adds the provision that any end-user located in the countries listed in Supplement 3 to Part 740 is eligible to receive encryption items classified by BXA under ECCNs 5A002, 5D002 and 5E002. Exports and reexports to foreign

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 62602 2002

subsidiaries or offices of firms, organizations and governments headquartered in the above-listed countries are also eligible under this provision.

7. Supplement No. 6 to Part 742 is further streamlined to provide more detailed guidelines for submitting a classification request for encryption items.

8. § 744.9 is revised to expressly provide that the restrictions imposed by that section do not prohibit technical assistance abroad by U.S. persons in connection with the discussion of information in the work of groups or bodies engaged in standards development.

9. In § 748.3 (Classification and Advisory Opinions), is revised to clarify that exporters may self-classify 5A992, 5D992 and 5E992 items after submitting by the time of export the information described in paragraphs 1–5 of Supplement 6 to Part 742.

10. In § 770.2 (Interpretation 14), conforming changes are made to regulatory citations.

11. In Part 772 (Definition of Terms), the definition of "cryptanalytic items" is added.

12. In Part 774, ECCNs 5A002, 5A992, 5D992, and 5E992 are revised to clarify that items previously classified under 5A002, 5D002 and 5E002 continue to be controlled for AT1 reasons.

Licenses required for export or reexports to governments for network management products not classified as retail which do not allow for encryption of data by the network users may be considered favorably for civil end-uses.

For further clarity, this rule makes clear that the seven terrorist designated countries are not eligible under the provisions of License Exception ENC.

BXA received a number of comments on the January 14 regulation (65 FR 2492). These comments all reflected certain common themes: that the regulation was too complex; that the United States needed to match any EU action; that reporting should be reduced or eliminated and that encryption items should be made eligible for *de minimis* treatment. These comments were carefully considered by the Interagency Working Group on Cryptography in the development of this regulation, and a number of the concerns are explicitly addressed by this regulation. Section 740.17 (License Exception ENC) has been shortened and simplified. It also implements a number of changes to streamline U.S. practice and bring it into line with EU licensing practice. Reporting requirements have been greatly reduced by the elimination of reporting required from foreign subsidiaries of U.S. firms and for software used on low level computers. Finally, this regulation institutes a process whereby certain retail encryption products can now be made eligible for *de minimis* treatment.

Although the Export Administration Act (EAA) expired on August 20, 1994, the President invoked the International Emergency Economic Powers Act and continued in effect the EAR, and, to the extent permitted by law, the provisions of the EAA in Executive Order 12924 of August 19, 1994, as extended by the President's notices of August 15, 1995 (60 FR 42767), August 14, 1996 (61 FR 42527), August 13, 1997 (62 FR 43629), August 13, 1998 (63 FR 44121), August 10, 1999 (64 F.R. 44101), and August 8, 2000 (65 FR 48347).

Rulemaking Requirements

1. This final rule has been determined to be significant for purposes of Executive Order 12866.

2. Notwithstanding any other provision of law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with a collection of information, subject to the requirements of the Paperwork Reduction Act (PRA), unless that collection of information displays a currently valid OMB Control Number. This rule involves collections of information subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*). These collections have been approved by the Office of Management and Budget under control numbers 0694–0088, "Multi-Purpose Application" and 0694–0104, "Commercial Encryption Items Transferred from the Department of State to the Department of Commerce." Collection 0694–0088 carries a burden hour estimate of 45 minutes per manual submission and 40 minutes per electronic submission. Miscellaneous and recordkeeping activities account for 12 minutes per submission. For collection 0694–0104, it is estimated it will take companies 5 minutes to complete notifications for source code under License Exceptions TSU and ENC. It will take companies 15 minutes to complete upgrade notifications. For reporting under License Exception ENC and licenses for encryption items, it will take companies 8 hours to complete semi-annual reporting requirements.

3. This rule does not contain policies with Federalism implications sufficient to warrant preparation of a Federalism assessment under Executive Order 13132.

4. The provisions of the Administrative Procedure Act (5 U.S.C. 553) requiring notice of proposed Rulemaking, the opportunity for public participation, and a delay in effective date, are inapplicable because this regulation involves a military and foreign affairs function of the United States (Sec. 5 U.S.C. 553(a)(1)). Further, no other law requires that a notice of proposed rulemaking and an opportunity for public comment be given for this 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. 553, or by any other law, the analytical requirements of the Regulatory Flexibility Act (5 U.S.C. 601 *et seq.*) are not applicable. Therefore, this regulation is issued in final form. Although there is no formal comment period, public comments on this regulation are welcome on a continuing basis. Comments should be submitted to Kirsten Mortimer, Office of Exporter Services, Bureau of Export Administration, Department of Commerce, P.O. Box 273, Washington, D.C. 20044.

Copies of the public record concerning these regulations may be requested from: Bureau of Export Administration, Office of Administration, U.S. Department of Commerce, Room 6883, 14th and Constitution Avenue, NW, Washington, DC 20230; (202) 482–0637. This component does not maintain a separate public inspection facility. Requesters should first view BXA's website (which can be reached through *http://www.bxa.doc.gov*). If requesters cannot access BXA's website, please call the number above for assistance.

List of Subjects

15 CFR Parts 732, 740 and 748

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

15 CFR Part 734

Administrative practice and procedure, Exports, Foreign trade.

15 CFR Parts 742, 770, 772 and 774

Exports, Foreign trade.

15 CFR Part 744

Exports, Foreign trade, reporting and recordkeeping requirements.

Accordingly, parts 732, 734, 740, 742, 744, 748, 770, 772 and 774 of the Export Administration Regulations (15 CFR parts 730 through 799) are amended as follows:

1. The authority citation for parts 732, 748, 770, and 772 are revised to read as follows:

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 62603 2002

Authority: 50 U.S.C. app. 2401 *et seq.*; 50 U.S.C. 1701 *et seq.*; E.O. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; Notice of August 3, 2000 (65 FR 48347, August 8, 2000).

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

Authority: 50 U.S.C. app. 2401 *et seq.*; 50 U.S.C. 1701 *et seq.*; E.O. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; E.O. 12938, 59 FR 59099, 3 CFR, 1994 Comp., p. 950; E.O. 13020, 61 FR 54079, 3 CFR, 1996 Comp. p. 219; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; Notice of November 12, 1998, 63 FR 63589, 3 CFR, 1998 Comp., p. 305; Notice of August 3, 2000 (65 FR 48347, August 8, 2000).

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

Authority: 50 U.S.C. app. 2401 *et seq.*; 50 U.S.C. 1701 *et seq.*; E.O. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; Notice of August 3, 2000 (65 FR 48347, August 8, 2000).

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

Authority: 50 U.S.C. app. 2401 *et seq.*; 50 U.S.C. 1701 *et seq.*; 18 U.S.C. 2510 *et seq.*; 22 U.S.C. 3201 *et seq.*; 42 U.S.C. 2139a; E.O. 12058, 43 FR 20947, 3 CFR, 1978 Comp., p. 179; E.O. 12851, 58 FR 33181, 3 CFR, 1993 Comp., p. 608; E.O. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; E.O. 12938, 59 FR 59099, 3 CFR, 1994 Comp., p. 950; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; Notice of November 12, 1998, 63 FR 63589, 3 CFR, 1998 Comp., p. 305; Notice of August 3, 2000 (65 FR 48347, August 8, 2000).

5. The authority citation for part 744 continues 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; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; Notice of November 12, 1998, 63 FR 63589, 3 CFR, 1998 Comp., p. 305; Notice of August 3, 2000 (65 FR 48347, August 8, 2000).

6. The authority citation for part 774 continues to read as follows:

Authority: 50 U.S.C. app. 2401 *et seq.*; 50 U.S.C. 1701 *et seq.*; 10 U.S.C. 7420; 10 U.S.C. 7430(e); 18 U.S.C. 2510 *et seq.*; 22 U.S.C. 287c, 22 U.S.C. 3201 *et seq.*, 22 U.S.C. 6004; 30 U.S.C. 185(s), 185(u); 42 U.S.C. 2139a; 42 U.S.C. 6212; 43 U.S.C. 1354; 46 U.S.C. app. 466c; 50 U.S.C. app. 5; E.O. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; Notice of August 3, 2000 (65 FR 48347, August 8, 2000).

PART 732—[AMENDED]

7. Section 732.2 is amended by revising paragraph (d) introductory text to read as follows:

§ 732.2 Steps regarding scope of the EAR.

* * * * *

(d) *Step 4: Foreign-made items incorporating less than the* de minimis *level of U.S. parts, components, and materials.* This step is appropriate only for items that are made outside the United States and not currently in the United States. Note that encryption items controlled for EI reasons under ECCNs 5A002, 5D002 or 5E002 on the Commerce Control List (refer to Supplement No.1 to Part 774 of the EAR) are subject to the EAR even if they incorporate less than the *de minimis* level of U.S. content. However, exporters may, as part of a classification request, ask that certain 5A002 and 5D002 parts, components and software also be made eligible for *de minimis* treatment (see § 734.4(b) of the EAR). The review of *de minimis* eligibility will take into account national security interests.

* * * * *

8. Section 732.3 is amended by revising paragraph (e)(2) to read as follows:

§ 732.3 Steps regarding the ten general prohibitions.

* * * * *

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

* * * * *

(2) *Guidance for calculations.* For guidance on how to calculate the U.S.-controlled content, refer to Supplement No. 2 to part 734 of the EAR. Note that certain rules issued by the Office of Foreign Assets Control, certain exports from abroad by U.S.-owned or controlled entities may be prohibited notwithstanding the *de minimis* provisions of the EAR. In addition, the *de minimis* exclusions from the parts and components rule do not relieve U.S. persons of the obligation to refrain from supporting the proliferation of weapons of mass-destruction and missiles as provided in General Prohibition Seven (U.S. Person Proliferation Activity) described in § 736.2(b)(7) of the EAR. Note that encryption items controlled for EI reasons under ECCNs 5A002, 5D002 or 5E002 on the Commerce Control List (refer to Supplement No.1 to Part 774 of the EAR) are subject to the EAR even if they incorporate less than the *de minimis* level of U.S. content. However, exporters may, as part of a classification request, ask that certain 5A002 and 5D002 parts, components and software also be made eligible for *de minimis* treatment (see § 734.4(b) of the EAR).

* * * * *

PART 734—[AMENDED]

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

§ 734.4 De minimis U.S. content.

* * * * *

(b) There is no *de minimis* level for items controlled for EI reasons under ECCNs 5A002, 5D002 and 5E002 absent written authorization from BXA. Exporters may, as part of a classification request, ask that software controlled under ECCN 5D002 and eligible for export under the "retail" or "source code" provisions of license exception ENC, and parts and components controlled under ECCN 5A002, be made eligible for *de minimis* treatment. The review of *de minimis* eligibility will take into account national security interests.

* * * * *

PART 740—[AMENDED]

10. Section 740.9 is amended by adding a sentence at the end of paragraph (c)(2) and by revising paragraphs (c)(3) and (c)(4)(i) to read as follows:

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

* * * * *

(c) *Exports of beta test software* * * *

(2) * * * In addition, encryption software under ECCN 5D002 is further restricted from being exported or reexported to Cuba, Iran, Iraq, Libya, North Korea, Sudan or Syria.

(3) *Eligible 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 (c). Encryption software controlled for EI reasons under ECCN 5D002 is eligible for export and reexport under this paragraph (c) provided the exporter has submitted by the time of export the information described in paragraphs (a) through (e) of Supplement 6 to Part 742 to BXA, with a copy to the ENC Encryption Request Coordinator. The names and addresses of the testing consignees, except names and addresses of individual consumers, and the name and version of the beta software should be reported consistent with § 740.17(e)(5). Any final product must

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 62604 2002

be reviewed and classified under the requirements of § 740.17.

(4) * * *

(i) The software producer intends to market the software to the general public after completion of the beta testing, as described in the General Software Note found in Supplement 2 to Part 774 or the Cryptography Note in Category 5—part II of the Commerce Control List (Supplement No. 1 to part 774 of the EAR);

* * * * *

11. Section 740.13 is amended by revising paragraph (e) to read as follows:

§ 740.13 Technology and software—unrestricted (TSU).

* * * * *

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

(2) Object code resulting from the compiling of source code which would be considered publicly available can be exported under TSU if the requirements of this section are otherwise met and no fee or payment (other than reasonable and customary fees for reproduction and distribution) is required for the object code. See § 740.17(b)(4)(i) for the treatment of object code where a fee or payment is required.

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

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

12. Section 740.17 is revised to read as follows:

§ 740.17 Encryption commodities and software (ENC).

License Exception ENC authorizes the export and reexport of encryption items classified under ECCNs 5A002, 5D002 and 5E002. No encryption item(s) may be exported under this license exception to Cuba, Iran, Iraq, Libya, North Korea, Sudan or Syria. Reporting requirements apply to exports made under the authority of License Exception ENC; see paragraph (e) of this section for these requirements.

(a) *Exports and reexports of encryption items.* Exports and reexports of encryption items classified under ECCNs 5A002, 5D002 and 5E002 are authorized to any end-user located in the countries listed in Supplement 3 to this part 740, except for exports of cryptanalytic items (as defined in Part 772 of the EAR) to government end-users. These items may also be exported or reexported to any destination for the internal use of foreign subsidiaries or offices of firms, organizations and governments headquartered in Canada or in countries listed in Supplement 3 to this part 740.

(b) For all other countries, you may export and reexport encryption commodities, software and components (as defined in part 772 of the EAR) under the provisions of License Exception ENC as enumerated in this section. For exports and reexports of encryption items which contain an open cryptographic interface (as defined in part 772 of the EAR), see paragraph (b)(5) of this section.

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

(2) *Encryption commodities and software.* (i) Exports and reexports of any encryption commodity, general purpose toolkit, software and component are authorized after review and classification by BXA under ECCNs 5A002 and 5D002 to any individual, commercial firm or other non-government end-user outside the countries (except Cuba, Iraq, Iran, Libya, North Korea, Sudan or Syria) listed in Supplement 3 to this part 740. Encryption products classified under this paragraph require a license before export and reexport to governments (as defined in part 772 of the EAR) outside the countries listed in Supplement 3 to this part 740. The restriction limiting exports or reexports to internal company proprietary use is removed.

(ii) Certain restrictions apply to Internet and telecommunications service providers. Internet and telecommunications service providers can obtain and use any encryption product for their internal use and to provide any service under License Exception ENC. However, a license is required for the use of any product not classified as retail to provide services specific to government end-users outside the countries listed in Supplement 3 to this part 740, e.g., WAN, LAN, VPN, voice and dedicated-link services; application specific and e-commerce services and PKI encryption services specifically for government end-users.

(3) *Retail encryption commodities and software.* Exports and reexports to any end-user of encryption commodities, software and components are authorized after review and classification by BXA as retail under ECCNs 5A002 and 5D002. Encryption products exported or reexported under this paragraph (b)(3) can be used to provide services to any entity. Internet or telecommunications service providers can obtain retail products under License Exception ENC and use them to provide any service to any entity. Retail encryption commodities, software and components are products:

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

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

(B) Specifically designed for individual consumer use and sold or

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 62605 2002

transferred through tangible or intangible means; or

(C) Which are sold or will be sold in large volume without restriction through mail order transactions, electronic transactions, or telephone call transactions; and

(ii) Meeting all of the following:

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

(B) Substantial support is not required for installation and use;

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

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

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

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

(v) 56-bit products with key exchange mechanisms greater than 512 bits and up to and including 1024 bits, or equivalent products not classified as mass market, or finance-specific encryption commodities and software of any key length restricted by design (e.g., highly field-formatted with validation procedures and not easily diverted to other end-uses) and used to secure financial communications such as electronic commerce may be exported under the retail provisions of this section immediately after submitting a completed classification request to BXA.

(vi) Items which would be controlled only because they incorporate components or software which provide short-range wireless encryption functions may be exported without review and classification by BXA and without reporting under the retail provisions of this section.

(4) *Commercial encryption source code.* Exports and reexports of encryption source code not released under § 740.13(e) are authorized subject to the following provisions:

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

(ii) Encryption source code which would not be considered publicly available and which does not include source code that when compiled provides an open cryptographic interface (see paragraph (b)(5) of this section), may be exported or reexported using License Exception ENC to any individual, commercial firm or other non-government end-user after submitting a complete classification request to BXA with a copy to the ENC Coordinator.

(5) *Cryptographic interfaces.* (i) Exports or reexports of encryption commodities, software and components which provide an open cryptographic interface (as defined in part 772 of the EAR) may be exported under License Exception ENC to any end-user located in any country listed in Supplement 3 to this part 740. Exports or reexports to other destinations of encryption commodities, software and components which provide an open cryptographic interface are not eligible to use License Exception ENC and require a license (unless exported to a subsidiary of a U.S. company under paragraph (b)(1) of this section). This does not apply to source code that would be considered publicly available under § 734.3(b)(3) of the EAR.

(ii) Encryption items which are limited to allowing foreign-developed cryptographic products to operate with U.S. products (e.g. signing) can be exported or reexported under License Exception ENC to any end-user. Such exports are subject to reporting requirements (see paragraph (e)(3) of this section). No review of the foreign-developed cryptography is required.

(c) *Reexports and Transfers.* U.S. or foreign distributors, resellers or other entities who are not original manufacturers of encryption commodities and software are permitted to use License Exception ENC only in instances where the export or reexport meets the applicable terms and conditions of this section. Transfers of encryption items listed in paragraph (b) of this section to government end-users or end-uses within the same country are prohibited unless otherwise authorized by license or license exception. Foreign products developed with or incorporating U.S.-origin encryption source code, components or toolkits remain subject to the EAR but do not require review and classification by BXA and can be exported or reexported without further authorization.

(d) *Eligibility for License Exception ENC.* (1) *Review and classification.* You may initiate review and classification of your encryption items as required by this section by submitting a classification request in accordance with the provisions of § 748.3(b) and Supplement 6 to Part 742 of the EAR. Indicate "License Exception ENC" in Block 9: Special purpose, on form BXA–748P. Submit the original request to BXA and send a copy of the request to ENC Encryption Request Coordinator (see paragraph (e)(5) of this section for mailing addresses).

(i) Exporters may immediately export and reexport any encryption item except "cryptanalytic items" as defined in part 772 of the EAR to any end-user located in the countries listed in Supplement 3 to this part 740 provided the exporter has submitted to BXA a completed classification request by the time of export.

(ii) Exporters may, thirty days after receipt of a completed classification request by BXA, export and reexport to any non-government end-user located outside the countries listed in Supplement 3 to this part 740 any encryption product eligible under

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 62606 2002

paragraph (b)(2), (b)(3) or (b)(4) of this section unless otherwise notified by BXA. No exports to government end-users located outside of countries listed in Supplement 3 to this part 740 are allowed under this provision. BXA reserves the right to suspend eligibility to export under this provision while a classification is pending.

(2) *Grandfathering.* Finance-specific and 56-bit products previously reviewed and classified by BXA can be exported and reexported to any end-user without further review. Other encryption commodities, software or components previously approved for export can be exported and reexported without further review to any end-user in countries listed in Supplement 3 to this part 740 countries and to any non-government end-user outside of the countries listed in Supplement 3 to this part 740. This includes products approved under a license, an Encryption Licensing Arrangement, or classified as eligible to use License Exception ENC (except for those products which were only authorized for export to U.S. subsidiaries). Exports of products not classified by BXA as "retail" to governments of countries not listed in Supplement 3 to this part 740 require a license.

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

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

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

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

(i) Any encryption to U.S. subsidiaries for internal company use;

(ii) Finance-specific products;

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

(iv) Retail products exported to individual consumers;

(v) Items exported via free or anonymous download;

(vi) Encryption items from or to a U.S. bank, financial institution or their subsidiaries, affiliates, customers or contractors for banking or financial operations;

(vii) Items which incorporate components limited to providing short-range wireless encryption functions;

(viii) Retail operating systems, or desktop applications (e.g. e-mail, browsers, games, word processing, data base, financial applications or utilities) designed for, bundled with, or pre-loaded on single CPU computers, laptops or hand-held devices;

(ix) Client Internet appliance and client wireless LAN cards;

(x) Foreign products developed by bundling or compiling of source code.

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

(i) For items exported to a distributor or other reseller, including subsidiaries of U.S. firms, the name and address of the distributor or reseller, the item and the quantity exported and, if collected as part of the distribution process by the exporter, the end-user's name and address;

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

(iii) For exports of 5E002 items to be used for technical assistance and which are not released by § 744.9 of the EAR, the name and address of the end-user.

(3) For direct sales or transfers of encryption components, commercial source code described under paragraph (b)(4) of this section, technology or general purpose encryption toolkits to foreign manufacturers when intended for use in foreign products developed for commercial sale, you must submit the names and addresses of the manufacturers using these items and, when the product is made available for commercial sale, a non-proprietary technical description of the foreign products for which the component, source code or toolkit are being used (e.g., brochures, other documentation, descriptions or other identifiers of the final foreign product; the algorithm and key lengths used; general programming interfaces to the product, if known; any standards or protocols that the foreign product adheres to; and source code, if available.).

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

(5) You must submit reports required under this section semi-annually to BXA, unless otherwise provided in this paragraph (e)(5). For exports occurring between January 1 and June 30, a report is due no later than August 1 of that year. For exports occurring between July 1 and December 31, a report is due no later than February 1 the following year. Reports must include the classification or other authorization number. These reports must be provided in electronic form to BXA; suggested file formats for electronic submission include spreadsheets, tabular text or structured text. Exporters may request other reporting arrangements with BXA to better reflect their business models. Reports should be sent electronically to crypt@bxa.doc.gov, or disks and CDs can be mailed to the following addresses:

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

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

13. A new Supplement No. 3 is added to part 740 to read as follows:

Supplement No. 3 to Part 740—License Exception ENC Country Group

Austria
Australia
Belgium
Czech Republic
Denmark
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Japan
Luxembourg
Netherlands
New Zealand
Norway
Poland
Portugal
Spain
Sweden

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 62607 2002

Switzerland
United Kingdom

PART 742—[AMENDED]

14. Section 742.15 is amended by revising paragraphs (a), (b) introductory text, (b)(1), and (b)(2) to read as follows:

§ 742.15 Encryption items.

* * * * *

(a) *License requirements.* Licenses are required for exports and reexports of encryption items (EI) classified under ECCNS 5A002, 5D002 and 5E002 to all destinations except Canada. Refer to part 740 of this EAR for licensing exceptions and to part 772 of the EAR for the definition of "encryption items."

(b) *Licensing policy.* The following licensing policies apply to items identified in paragraph (a) of this section. Except as otherwise noted, applications will be reviewed on a case-by-case basis by BXA, in conjunction with other agencies, to determine whether the export or reexport is consistent with U.S. national security and foreign policy interests. For subsequent bundling and updates of these items see paragraph (n) of § 770.2 of the EAR. No exports without a license are authorized to Cuba, Iran, Iraq, Libya, North Korea, Sudan or Syria.

(1) *Encryption items under ECCNs 5A992, 5D992 and 5E992.* Certain encryption commodities, software and technology may be classified under ECCNs 5A992, 5D992 or 5E992. These items continue to be subject to AT1 controls. Such items include encryption commodities, software and technology with key lengths up to and including 56-bits with an asymmetric key exchange algorithm not exceeding 512 bits; products which only provide key management with asymmetric key exchange algorithms not exceeding 512 bits; and mass market encryption commodities and software with key lengths not exceeding 64-bits for the symmetric algorithm. Refer to the Cryptography Note (Note 3) to part II of Category 5 of the CCL for a definition of mass market encryption commodities and software. Key exchange mechanisms, proprietary key exchange mechanisms, or company proprietary commodities and software implementations may also be eligible for this treatment. Exporters may self-classify such 5A992, 5D992 or 5E992 items and export them without review and classification by BXA provided you have submitted to BXA and the ENC Encryption Request Coordinator by the time of export the information described in paragraphs (a) through (e) of Supplement 6 to this part 742. Notification should be made by e-mail to crypt@bxa.doc.gov.

(2) *Encryption items under ECCNs 5A002, 5D002 and 5E002.* All encryption commodities, software and components classified by BXA under ECCNs 5A002, 5D002 and 5E002 except cryptanalytic items are authorized for export and reexport to any end-user in the countries listed in Supplement 3 to Part 740 of the EAR. Items classified by BXA as retail products under ECCNs 5A002 and 5D002 are authorized for export and reexport to any end-user. All 5A002, 5D002 and 5E002 encryption items are authorized for export or reexport to any individual, commercial firm or other non-government end-user in countries not listed in Supplement 3 to Part 740 of the EAR. No exports of such items are authorized without a license to Cuba, Iran, Iraq, North Korea, Libya, Sudan or Syria. Any encryption item (including technology classified under ECGN 5E002) is authorized for export or reexport to U.S. subsidiaries (as defined in part 772).

* * * * *

15. Supplement No. 6 to part 742 is revised to read as follows:

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

Classification requests for encryption items must be submitted on Form BXA–748P, in accordance with § 748.3 of the EAR. Insert the phrase "License Exception ENC" in Block 9: Special Purpose in Form BXA–748P. Failure to insert this phrase will delay processing. BXA 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. For electronic submissions via SNAP, you may fax a copy of the support documents to BXA at (202) 501–0784. In addition, you must send a copy of the classification request and all support documents to: Attn: ENC Encryption Request Coordinator, 9800 Savage Road, Suite 6131, Fort Meade, MD 20755–6000. For all classification requests of encryption items provide brochures or other documentation or specifications related to the technology, commodity or software, relevant product descriptions, architecture specifications, and as necessary for the technical review, source code. Also, indicate any prior reviews and classifications of the product, if applicable to the current submission. Provide the following information in a cover letter with the classification request:

(a) State the name of the encryption item being submitted for review.

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

(c)For classification request for a commodity or software, provide the following information:

(1) Description of all the symmetric and asymmetric encryption algorithms and key lengths and how the algorithms are used. Specify which encryption modes are supported (e.g., cipher feedback mode or cipher block chaining mode).

(2) State the key management algorithms, including modulus sizes, that are supported.

(3) For products with proprietary algorithms, include a textual description and the source code of the algorithm.

(4) Describe the pre-processing methods (e.g., data compression or data interleaving) that are applied to the plaintext data prior to encryption.

(5) Describe the post-processing methods (e.g., packetization, encapsulation) that are applied to the cipher text data after encryption.

(6) State the communication protocols (e.g., X.25, Telnet or TCP) and encryption protocols (e.g., SSL, IPSEC or PKCS standards) that are supported.

(7) Describe the encryption-related Application Programming Interfaces (APIs) that are implemented and/or supported. Explain which interfaces are for internal (private) and/or external (public) use.

(8) Describe whether the cryptographic routines are statically or dynamically linked, and the routines (if any) that are provided by third-party modules or libraries. Identify the third-party manufacturers of the modules or toolkits.

(9) For commodities or software using Java byte code, describe the techniques (including obfuscation, private access modifiers or final classes) that are used to protect against decompilation and misuse.

(10) State how the product is written to preclude user modification of the encryption algorithms, key management and key space.

(11) For products that qualify as "retail", explain how the product meets the listed criteria in § 740.17(b)(3) of the EAR.

(12) For products which incorporate an open cryptographic interface as defined in part 772 of the EAR, describe the Open Cryptographic Interface.

(d) For classification requests regarding components, provide the following additional information:

(1) Reference the application for which the components are used in, if known;

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

(3) State whether the component is constrained by function; and

(4) the encryption component and include the name of the manufacturer, component model number or other identifier.

(e) For classification requests for source code, provide the following information:

(1) If applicable, reference the executable (object code) product that was previously reviewed;

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

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

(f) For step-by-step instructions and guidance on submitting classification requests for License Exception ENC, visit our webpage at www.bxa.gov/Encryption.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 62608 2002

PART 744—[AMENDED]

16. Section 744.9 is amended by revising paragraph (a) 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 authorization 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. Technical assistance may be exported immediately to nationals of the countries listed in Supplement 3 to part 740 of the EAR (except for technical assistance to government end-users for cryptanalytic items) provided the exporter has submitted to BXA a completed classification request by the time of export. 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 or in the work of groups or bodies engaged in standards development, by itself would not establish the intent described in this section, even where foreign persons are present.

* * * * *

PART 748—[AMENDED]

17. Section 748.3 is amended by revising paragraph (b)(3) to read as follows:

§ 748.3 Classification and Advisory Opinions.

* * * * *

(b) * * *

(3) Classification requests for a Department of Commerce review of encryption software transferred from the U.S. Munitions List consistent with Executive Order 13026 of November 15, 1996 (3 CFR, 1996 Comp., p. 228) and pursuant to the Presidential Memorandum of that date are required prior to export to determine eligibility for release from EI controls. Exporters may self-classify 5A992, 5D992 or 5E992 items after submitting to BXA and the ENC Encryption Request Coordinator by the time of export the information described in paragraphs 1–5 of Supplement 6 to Part 742 of the EAR. Refer to § 742.15(b) and Supplement No. 6 to Part 742 of the EAR for instructions on submitting such requests for mass market encryption software.

* * * * *

PART 770—[AMENDED]

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

§ 770.2 Item interpretations.

* * * * *

(n) *Interpretation 14: Encryption commodity and software reviews.* Classification of encryption commodities or software is required to determine eligibility for certain licensing mechanisms (see §§ 740.13(e) and 740.17 of the EAR) and exports to subsidiaries of U.S. companies (see § 740.17(b)(1) of the EAR). Note that subsequent bundling, patches, upgrades or releases, including name changes, may be exported or reexported under the applicable provisions of the EAR without further review as long as the functional encryption capacity of the originally reviewed product has not been modified or enhanced. This does not extend to products controlled under a different category on the CCL.

PART 772—[AMENDED]

18. Part 772 is amended by designating the existing text as § 772.1 and adding a section heading, by adding the definition of "Cryptanalytic items" in alphabetical order, and by revising the definition of "Open cryptographic interface", to read as follows:

§ 772.1 Definitions of terms as used in the Export Administration Regulations (EAR).

* * * * *

"Cryptanalytic items". Systems, equipment, applications, specific electronic assemblies, modules and integrated circuits designed or modified to perform cryptanalytic functions, software having the characteristics of cryptanalytic hardware or performing cryptanalytic functions, or technology for the development, production or use of cryptanalytic commodities or software.

* * * * *

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

* * * * *

PART 774—[AMENDED]

19. In Supplement No. 1 to part 774 (the Commerce Control List), Category 5—Telecommunications and "Information Security", part II. "Information Security", Export Control Classification Numbers (ECCNs) 5A002, 5A992, 5D992, and 5E992 are amended by revising the "List of Items Controlled" section to read as follows:

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

* * * * *

List of Items Controlled

Unit: $ value

Related Controls: See also 5A992. This entry does not control: (a) "Personalized smart cards" where the cryptographic capability is restricted for use in equipment or systems excluded from control paragraphs (b) through (f) of this note. Note that if a "personalized smart card" has multiple functions, the control status of each function is assessed individually; (b) Receiving equipment for radio broadcast, pay television or similar restricted audience broadcast of the consumer type, without digital encryption except that exclusively used for sending the billing or program-related information back to the broadcast providers; (c) Portable or mobile radiotelephones for civil use (e.g., for use with commercial civil cellular radio communications systems) that are not capable of end-to-end encryption; (d) Equipment where the cryptographic capability is not user-accessible and which is specially designed and limited to allow any of the following: (1) Execution of copy-protected "software"; (2) access to any of the following: (a) Copy-protected read-only media; or (b) Information stored in encrypted form on media (e.g., in connection with the protection of intellectual property rights) where the media is offered for sale in identical sets to the public; or (3) one-time encryption of copyright protected audio/video data; (e) Cryptographic equipment specially designed and limited for banking use or money transactions; (f) Cordless telephone equipment not capable of end-to-end encryption where the maximum effective range of unboosted cordless operation (e.g., a single, unrelayed hop between terminal and home basestation) is less than 400 meters

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 62609 2002

according to the manufacturer's specifications. These items are controlled under ECCN 5A992.

Related Definitions: (1) The term "money transactions" in paragraph (e) of Related Controls includes the collection and settlement of fares or credit functions. (2) For the control of global navigation satellite systems receiving equipment containing or employing decryption (e.g., GPS or GLONASS) see 7A005.

Items:

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

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

a.1. Designed or modified to use "cryptography" employing digital techniques performing any cryptographic function other than authentication or digital signature having any of the following:

Technical Notes: 1. Authentication and digital signature functions include their associated key management function.

2. Authentication includes all aspects of access control where there is no encryption of files or text except as directly related to the protection of passwords, Personal Identification Numbers (PINs) or similar data to prevent unauthorized access.

3. "Cryptography" does not include "fixed" data compression or coding techniques.

Note: 5A002.a.1 includes equipment designed or modified to use "cryptography" employing analog principles when implemented with digital techniques.

a.1.a. A "symmetric algorithm" employing a key length in excess of 56-bits; *or*

a.1.b. An "asymmetric algorithm" where the security of the algorithm is based on any of the following:

a.1.b.1. Factorization of integers in excess of 512 bits (*e.g.*, RSA);

a.1.b.2. Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (*e.g.*, Diffie-Hellman over Z/pZ); or

a.1.b.3. Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2 in excess of 112 bits (*e.g.*, Diffie-Hellman over an elliptic curve);

a.2. Designed or modified to perform cryptanalytic functions;

a.3. [Reserved]

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

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

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

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

5A992 Equipment not controlled by 5A002.

* * * * *

List of Items Controlled

Unit: $ value
Related Controls: N/A
Related Definitions: N/A
Items:

a. Telecommunications and other information security equipment containing encryption.

b. "Information security" equipment, n.e.s., (*e.g.*, cryptographic, cryptanalytic, and cryptologic equipment, n.e.s.) and components therefor.

5D992 "Information Security" "software" not controlled by 5D002.

* * * * *

List of Items Controlled

Unit: $ value
Related Controls: N/A
Related Definitions: N/A
Items: 1

a. "Software", as follows:

a.1 "Software" specially designed or modified for the "development", "production", or "use" of telecommunications and other information security equipment containing encryption (*e.g.*, equipment controlled by 5A992.a);

a.2. "Software" specially designed or modified for the "development", "production", or "use" of information security or cryptologic equipment (*e.g.*, equipment controlled by 5A992.b).

b. "Software", as follows:

b.1. "Software" having the characteristics, or performing or simulating the functions of the equipment controlled by 5A992.a.

b.2. "Software" having the characteristics, or performing or simulating the functions of the equipment controlled by 5A992.b.

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

5E992 "Information Security" "technology", not controlled by 5E002.

* * * * *

List of Items Controlled

Unit: N/A
Related Controls: N/A
Related Definitions: N/A
Items:

a. "Technology" n.e.s., for the "development", "production" or "use" of telecommunications equipment and other information security and containing encryption (*e.g.*, equipment controlled by 5A992.a) or "software" controlled by 5D992.a.1 or b.1.

b. "Technology", n.e.s., for the "development", "production" or "use" of "information security" or cryptologic equipment (*e.g.*, equipment controlled by 5A992.b), or "software" controlled by 5D992.a.2, b.2, or c.

Dated: October 11, 2000.

R. Roger Majak,

Assistant Secretary for Export Administration.

[FR Doc. 00-26646 Filed 10-18-00; 8:45 am]

BILLING CODE 3510-33-P

DEPARTMENT OF LABOR

Occupational Safety and Health Administration

29 CFR Part 1952

North Carolina State Plan: Coverage of the American National Red Cross; Change in Level of Federal Enforcement

AGENCY: Occupational Safety and Health Administration (OSHA), U.S. Department of Labor.

ACTION: Final rule.

SUMMARY: This document amends OSHA regulations to reflect the Assistant Secretary's approval of a change to the North Carolina occupational safety and health state plan excluding coverage of the American National Red Cross and its facilities from the plan and assumption of Federal enforcement authority over the American National Red Cross in North Carolina.

EFFECTIVE DATE: October 19, 2000.

FOR FURTHER INFORMATION CONTACT: Bonnie Friedman, Director, Office of Information and Consumer Affairs, Occupational Safety and Health Administration, U.S. Department of Labor, Room N3637, 200 Constitution Avenue NW., Washington, DC 20210, (202) 693-1999.

SUPPLEMENTARY INFORMATION:

A. Background

Section 18 of the Occupational Safety and Health Act of 1970 (the Act), 29 U.S.C. 667, provides that States which wish to assume responsibility for developing and enforcing their own occupational safety and health standards may do so by submitting and obtaining Federal approval of a State plan. State plan approval occurs in stages which include initial approval under section 18(b) of the Act and, ultimately, final approval under section 18(e).

The North Carolina State plan was initially approved on February 1, 1973 (38 FR 3041). On December 18, 1996, OSHA announced the final approval of the North Carolina State plan pursuant to section 18(e) and amended Subpart I of 29 CFR part 1952 to reflect the Assistant Secretary's decision (61 FR

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 62610 2002

Document No. 165

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [i] 2002

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [ii] 2002