Billing Code: 3510 33 P

DEPARTMENT OF COMMERCE

Bureau of Industry and Security

15 CFR Parts 740, 742, 748, 772, 774

[Docket No. 150304218-5218-01]

RIN 0694-AG49

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

AGENCY: Bureau of Industry and Security, Commerce.

ACTION: Proposed rule, with request for comments.

SUMMARY: The Bureau of Industry and Security (BIS) proposes to implement the agreements by the Wassenaar Arrangement (WA) at the Plenary meeting in December 2013 with

regard to systems, equipment or components specially designed for the generation, operation or delivery of, or communication with, intrusion software; software specially designed or modified for the development or production of such systems, equipment or components; software specially designed for the generation, operation or delivery of, or communication with, intrusion software; technology required for the development of intrusion software; Internet Protocol (IP) network communications surveillance systems or equipment and test, inspection, production equipment, specially designed components therefor, and development and production software and technology therefor. BIS proposes a license requirement for the export, reexport, or transfer (in-country) of these cybersecurity items to all destinations, except Canada. Although these cybersecurity capabilities were not previously designated for export control, many of these items have been controlled for their "information security" functionality, including encryption and cryptanalysis. This rule thus continues applicable Encryption Items (EI) registration and review requirements, while setting forth proposed license review policies and special submission requirements to address the new cybersecurity controls, including submission of a letter of explanation with regard to the technical capabilities of the cybersecurity items.

BIS also proposes to add the definition of "intrusion software" to the definition section of the EAR pursuant to the WA 2013 agreements.

DATES: Submit comments on or before [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Comments on this rule may be submitted to the Federal rulemaking portal (www.regulations.gov). The regulations.gov ID for this rule is: BIS-2015-0011 Comments may also be submitted via e-mail to publiccomments@bis.doc.gov or on paper to Regulatory Policy Division, Bureau of Industry and Security, Room 2099B, U.S. Department of Commerce, 14th St. and Pennsylvania Ave., N.W., Washington, DC 20230. Please refer to RIN 0694-AG49 in all comments and in the subject line of e-mail comments.

FOR FURTHER INFORMATION CONTACT: Catherine Wheeler, Director, Information Technology Control Division, Phone: (202) 482-0707 or by email at Catherine.Wheeler@bis.doc.gov

SUPPLEMENTARY INFORMATION:

Background

The Wassenaar Arrangement (WA) on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is a group of 41 like-minded states committed to promoting responsibility and transparency in the global arms trade, and preventing destabilizing accumulations of arms. As a Participating State, the United States has committed to controlling for export all items on the WA control lists. The lists were first established in 1996 and have been revised annually thereafter. Proposals for changes to the WA control lists that achieve consensus are approved by Participating States at annual December Plenary meetings. Participating States are charged with implementing the agreed list changes as soon as possible after approval. Implementation of WA list changes ensures U.S. companies have a level playing field with their competitors in other WA member states.

In 2013, WA agreed to add the following to their list of dual-use goods: systems, equipment or components specially designed for the generation, operation or delivery of, or communication with, intrusion software; software specially designed or modified for the development or production of such systems, equipment or components; software specially designed for the generation, operation or delivery of, or communication with, intrusion software; technology required for the development of intrusion software; Internet Protocol (IP) network communications surveillance systems or equipment and test, inspection, production equipment, specially designed components therefor, and development and production software and technology therefor. BIS, the Departments of Defense and State, as well as other agencies have been discussing the best way to add these items, which we have named "cybersecurity items," to the Commerce Control List (CCL) (Supplement No. 1 to part 774 of the Export Administration Regulations) without reducing encryption controls and while balancing the national security and foreign policy. For resource planning purposes, as well as license requirements, license exceptions, license submission requirements, and internal license reviews and processing planning purposes, this rule is published as a proposed rule.

Scope of the New Entries

Systems, equipment, components and software specially designed for the generation, operation or delivery of, or communication with, intrusion software include network penetration testing products that use intrusion software to identify vulnerabilities of computers and network-capable devices. Certain penetration testing products are currently classified as encryption items due to their cryptographic and/or cryptanalytic functionality. Technology for the development of intrusion software includes proprietary research on the vulnerabilities and exploitation of computers and network-capable devices. The new entry on the CCL that would control Internet Protocol (IP) network communications surveillance systems or equipment is restricted to products that perform all of the functions listed; however, the Export Administration Regulations (EAR) also prohibits the export of equipment if the exporter intends it will be combined with other equipment to comprise a system described in the new entry.

Addition of ECCNs 4A005 and 4D004 to the Commerce Control List

This rule proposes to add Export Control Classification Number (ECCN) 4A005 ("systems," "equipment," or "components" therefor, "specially designed" for the generation, operation or delivery of, or communication with, "intrusion software") and ECCN 4D004 ("software" "specially designed" for the generation, operation or delivery of, or communication with, "intrusion software") to the CCL. These ECCNs are proposed to be controlled for national security (NS), regional stability (RS), and anti-terrorism (AT) reasons to all destinations, except Canada. No license exceptions would be available for these items, except certain provisions of License Exception GOV, e.g., exports to or on behalf of the United States Government pursuant to § 740.11(b) of the EAR. This rule also proposes adding a License Requirement Note and a Note in the Related Controls paragraph for these ECCNs, to alert exporters to include all relevant information when submitting classification requests and licensing applications.

ECCN 4D001

This rule also proposes to amend ECCN 4D001 by adding ECCN 4A005 to Items paragraph 4D001.a in order to add control of "software" "specially designed" or modified for the "development" or "production," of equipment controlled by 4A005; adding an RS:1 license requirement paragraph for 4D001.a (as it applies to 4A005 or 4D004), removing License Exceptions TSR and STA eligibility; and adding the same explanatory License Requirement

Note and Related Controls Note that would be added to ECCNs 4A005 and 4D004.

As a technical correction, this rule proposes to remove from the "Reason for control" paragraph "NP," and from the License Requirement section the two sentences, "NP applies, unless a license exception is available. See § 742.3(b) of the EAR for information on applicable licensing review policies." That text does not articulate any license requirement, and no nuclear non-proliferation license requirement for software classified as 4D001 is set forth elsewhere in the EAR. BIS's regular practice is to impose a license requirement for nuclear non-proliferation reasons on items that are specified on the "List of Nuclear-Related Dual-Use Equipment, Materials, Software, and Related Technology" by the Nuclear Suppliers Group. ECCN 4D001 software is not so specified.

ECCN 4E001

This rule also proposes to amend ECCN 4E001 by adding a new Items paragraph 4E001.c to control "technology" "required" for the "development" of "intrusion software." ECCN 4E001.a controls ""technology" according to the General Technology Note, for the "development," "production," or "use" of equipment or "software" controlled by 4A (except 4A980 or 4A994) or 4D (except 4D980, 4D993 or 4D994)." Therefore, ECCN 4E001.a would control "technology" for the newly added 4A005 and 4D004, as well as 4D001.a (for 4A005 and 4D004). This rule also proposes to add an RS:1 license requirement paragraph for 4E001.a "technology" (as it applies to 4A005, 4D001.a (as it applies to 4A005 or 4D004) or 4D004) and 4E001.c, which would require a license to export, reexport, and transfer (in-country) to all destinations, except Canada. BIS also proposes to remove License Exception Technology and Software Under Restriction (TSR) and Strategic Trade Authorization (STA) eligibility and add the same explanatory License Requirement Note and Related Controls Note added to ECCNs 4A005, 4D001 and 4D004. Also, a reference to § 772.1 is proposed to be added to ECCNs 4A005, 4D001 and 4E001 to point to the location of the "intrusion software" definition, as this rule may be of interest to many new exporters that would not otherwise know that double quoted terms in the EAR are defined in § 772.1.

Lastly, the same technical correction regarding the Nuclear Non-proliferation (NP) control is proposed for 4E001 as is proposed for 4D001, see explanation above.

ECCN 5A001.j: Internet Protocol (IP) network communications surveillance systems or equipment and test, inspection, production equipment, specially designed components therefor

Network communication traffic analysis systems are becoming an increasingly sensitive issue, which is why WA agreed to add the control of these items to the WA dual-use list. These systems are using the process of intercepting and analyzing messages to produce personal, human and social information from the communications traffic. BIS proposes to add these items in paragraph 5A001.j and group them with cybersecurity items. The license requirements for these items are proposed to under NS Column 1, RS Column 1 and AT Column 1 on the Commerce Country Chart (Supplement No. 1 to part 738 of the EAR) and would require a license for export, reexport, and transfer (in-country) to all destinations, except Canada. Only certain provisions of License Exception GOV, e.g., exports to or on behalf of the United States Government pursuant to § 740.11(b) of the EAR, would be available for these items.

The same addition of a License Requirement Note and Related Control Note is proposed for ECCNs 5A001, 5D001, and 5E001 as is proposed for ECCNs 4A005, 4D001, 4D004 and

4E001 (see explanation under 4A005 and 4D005 above).

§740.13 - License Exception TSU

BIS proposes to remove cybersecurity software from the mass market provision of License Exception TSU eligibility by adding a new paragraph (d)(2)(ii). This is consistent with the existing encryption exclusion.

Cybersecurity items that are designed or modified to use "cryptography" or cryptanalysis

As previously introduced and explained in the preamble, this rule proposes to add a Related Control note to ECCNs 4A005, 4D004, 4E001, 5A001, 5A002, 5D002 and 5E002 that states that cybersecurity items are classified in cybersecurity ECCNs, even if the items are designed or modified to use "cryptography" or cryptanalysis; however, all such cybersecurity items using or incorporating encryption or other "information security" functionality classified under ECCNs 5A002, 5D002, 5A992.c, 5D992.c or 5E002, must also satisfy the registration, review and reporting requirements set forth in §§ 740.17, 742.15(b) and 748.3(d) of the EAR, including submissions to the ENC Encryption Request Coordinator, Ft. Meade, MD. This note is added so that people will not be confused under which ECCN to classify their products and when a cybersecurity item is designed or modified to use "cryptography" or cryptanalysis, after the relevant Encryption Items (EI) requirements for registration and review have been separately satisfied. One effect this will have is that these cybersecurity items will not be eligible for License Exception ENC. However, BIS anticipates licensing broad authorizations to certain types of end users and destinations that will counterbalance the loss of the use of License Exception ENC.

Information to be submitted with a license application to export, reexport, or transfer (in-country) cybersecurity items

In addition to the general information required by §748.3(b) of the EAR and the requirement that all encryption registration and review provisions must be separately satisfied with BIS and the ENC Encryption Request Coordinator, Ft. Meade, MD, this rule proposes to add a requirement to submit specific technical information in support of applications to export, reexport, or transfer (in-country) cybersecurity items. The specified technical information is set forth in newly added paragraph (z) of Supplement No. 2 to part 748 "Unique application and submission requirements." The Commodity Classification Application Tracking System (CCATS) number(s) or license number(s) for the cyber security item(s) must be included in the license application. If no classification or license application has been done for the cybersecurity item, then the answers to three (3) questions are to be submitted in a letter of explanation.

Also, this rule proposes that upon request from BIS, the applicant must include a copy of the sections of source code and other software (e.g., libraries and header files) that implement or invoke the controlled cybersecurity functionality.

License Reviewpolicy for cybersecurity items

The license review policies for cybersecurity items controlled under NS and AT will not be revised. A new license review policy for cybersecurity items is proposed under § 742.6(b) for regional stability. Cybersecurity items controlled for RS are proposed to be reviewed favorably if destined to a U.S. company or subsidiary not located in Country Group D:1 or E:1, foreign commercial partners located in Country Group A:5, government end users in Australia, Canada, New Zealand or the United Kingdom, and on a case-by-case basis to determine whether the transaction is contrary to the national security or foreign policy interests of the United States, including the foreign policy interest of promoting the observance of human rights throughout the world. Note that there is a policy of presumptive denial for items that have or support rootkit or zero-day exploit capabilities. The governments of Australia, Canada, New Zealand or the United Kingdom have partnered with the United States on cybersecurity policy and issues, which affords these countries with favorable treatment for license applications. A note that describes "foreign commercial partner" is proposed to be added to § 742.6(b). Any "information security" functionality incorporated in the cybersecurity item will also receive a focused case-by-case review for reasons of Encryption Items (EI) control.

§ 772.1 Definitions of terms as used in the EAR: Addition of definition for "intrusion software"

The WA-agreed definition for "intrusion software" is proposed to be added to § 772.1 of the EAR. The definition also includes a Note that describes some items not included as "intrusion software," e.g., hypervisors, debuggers or Software Reverse Engineering (SRE).

Request for comments

BIS is seeking information about the effect of this rule and would appreciate the submission of comments, and especially answers to the following questions:

1. How many additional license applications would your company be required to submit per year under the requirements of this proposed rule? If any, of those applications:

a. How many additional applications would be for products that are currently eligible for license exceptions?

b. How many additional applications would be for products that currently are classified EAR99?

2. How many deemed export, reexport or transfer (in-country) license applications would your company be required to submit per year under the requirements of this rule?

3. Would the rule have negative effects on your legitimate vulnerability research, audits, testing or screening and your company's ability to protect your own or your client’s networks? If so, explain how.

4. How long would it take you to answer the questions in proposed paragraph (z) to Supplement No. 2 to part 748? Is this information you already have for your products?

* The “Addresses” section of this proposed rule includes information about how to submit comments.

Rulemaking Requirements

1. Executive Orders 13563 and 12866 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches

that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This rule has been designated a "significant regulatory action," under 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 of 1995 (44 U.S.C. 3501 *et seq.*) (PRA), unless that collection of information displays a currently valid Office of Management and Budget (OMB) Control Number. This rule would involve one collection of information subject to the PRA. One of the collections has been approved by OMB under control number 0694-0088, "Multi-Purpose Application," and carries a burden hour estimate of 58 minutes for a manual or electronic submission. The additional information proposed to be required under Supplement No. 2 to part 748 paragraph (z) falls under the usual technical information that is submitted with applications to describe the abilities of the items on the license application. This information allows the licensing officer to verify the classification of the product and determine the effect it would have on U.S. national security and foreign policy. Send comments regarding these burden estimates or any other aspect of these collections of information, including suggestions for reducing the burden, to OMB Desk Officer, New Executive Office Building, Washington, DC 20503; and to Jasmeet Seehra, OMB Desk Officer, by e-mail at Jasmeet_K._Seehra@omb.eop.gov or by fax to (202) 395-7285; and to the Office of Administration, Bureau of Industry and Security, Department of Commerce, 1401 Constitution Ave., NW, Room 6622, Washington, DC 20230.

3. This rule does not contain policies with Federalism implications as that term is defined under Executive Order 13132.

4. The provisions of the Administrative Procedure Act (APA) (5 U.S.C. 553) requiring notice of proposed rulemaking, the opportunity for public participation, and a 30-day delay in effective date, are inapplicable because this regulation involves a military and foreign affairs function of the United States (5 U.S.C. 553(a)(1)). Nonetheless, BIS is providing the public with an opportunity to review and comment on this rule, despite its being exempted from that requirement of the APA. Because this rule is not required by the APA to undergo a period of notice and comment, the requirements of the Regulatory Flexibility Act, 5 U.S.C. 601 *et seq*., do not apply. Accordingly, no regulatory flexibility analysis is required, and none has been prepared.

BIS is interested in the potential impacts to businesses of this rule. Because most of the items impacted by this rule have encryption capabilities, BIS believes they are already being controlled under Category 5 part 2 of the EAR. Even though most encryption items are eligible for License Exception ENC and these cybersecurity items will not be eligible for License Exception ENC, BIS anticipates issuing broad licenses for these items. The impact of this rule is unknown to BIS, therefore the implementation of the Wassenaar Arrangement agreement of 2013 with regard to cybersecurity items is issued as a proposed rule with request for comments concerning the impact of the rule. Comments should be submitted to Sharron Cook, Office of Exporter Services, Bureau of Industry and Security, Department of Commerce, 14th and Pennsylvania Ave., NW, Room 2099, Washington, DC 20230 or e-mailed to publiccomments@bis.doc.gov. Please refer to RIN 0694-AG49 in all comments and in the subject line of e-mail comments.

List of Subjects

15 CFR Part 740

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

15 CFR Part 742

Exports, Terrorism.

15 CFR Part 748

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

15 CFR Part 772

Exports.

15 CFR Part 774

Exports, Reporting and recordkeeping requirements.

Accordingly, parts 740, 742, 748, 772, and 774 of the Export Administration Regulations (15 CFR parts 730 through 774) are proposed to be amended as follows:

PART 740 [AMENDED]

1. 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.*; 22 U.S.C. 7201 *et seq.*; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783; Notice of August 7, 2014, 79 FR 46959 (August 11, 2014).

2. Section 740.2 is amended by adding paragraph (a)(19) to read as follows:

§ 740.2 Restrictions on all License Exceptions.

(a) ***

(19) The item is a cybersecurity item, i.e., those controlled by ECCNs 4A005, 4D001.a ("specially designed" or modified for 4A005 or 4D004 items), 4D004, 4E001.a ("required" for 4A005, 4D001.a ("specially designed" or modified for 4A005 or 4D004) or 4D004 items), 4E001.c, 5A001.j, 5B001.a ("specially designed" for 5A001.j items), 5D001.a ("specially designed" for 5A001.j items), 5D001.c ("specially designed" for 5A001.j or 5B001.a items) or 5E001.a ("required" for 5A001.j, 5B001.a, 5D001.a (for 5A001.j items) or 5D001.c ("specially designed" for 5A001.j or 5B001.a items) and the export, reexport or transfer (in-country) is not authorized by § 740.11(b)(2)(ii) (made by or consigned to a department or agency of the U.S. government), or § 740.11(b)(2)(iii) (made for or on behalf of a department or agency of the U.S. Government).

* * * * *

3. Section 740.11 is amended by:

a. Adding paragraph (a)(2)(vi);

b. Removing the "or" from the end of paragraph (c)(3)(vi);

c. Removing the period from paragraph (c)(3)(vii) and adding a semicolon in its place; and

d. Adding paragraph (c)(3)(viii).

The revisions and addition read as follows:

§ 740.11 Governments, international organizations, international inspections under the Chemical Weapons Convention, and the International Space Station (GOV).

(a) * * *

(2) * * *

(vi) Cybersecurity items, i.e., those controlled by ECCNs 4A005, 4D001.a ("specially designed" or modified for 4A005 or 4D004 items), 4D004, 4E001.a ("required" for 4A005, 4D001.a ("specially designed" or modified for 4A005 or 4D004) or 4D004 items), 4E001.c, 5A001.j, 5B001.a ("specially designed" for 5A001.j items), 5D001.a ("specially designed" or modified for 5A001.j items), 5D001.c ("specially designed" or modified for 5A001.j or 5B001.a items) or 5E001.a ("required" for 5A001.j, 5B001.a, 5D001.a ("specially designed" or modified for 5A001.j items) or 5D001.c ("specially designed" or modified for 5A001.j or 5B001.a items).

* * * * *

(c) * * *

(3) * * *

(viii) Cybersecurity items, i.e., those controlled by ECCNs 4A005, 4D001.a ("specially designed" or modified for 4A005 or 4D004 items), 4D004, 4E001.a ("required" for 4A005, 4D001.a ("specially designed" or modified for 4A005 or 4D004) or 4D004 items), 4E001.c, 5A001.j, 5B001.a ("specially designed" for 5A001.j items), 5D001.a ("specially designed" or modified for 5A001.j items), 5D001.c ("specially designed" or modified for 5A001.j or 5B001.a items) or 5E001.a ("required" for 5A001.j, 5B001.a, 5D001.a ("specially designed" or modified for 5A001.j items) or 5D001.c ("specially designed" or modified for 5A001.j or 5B001.a) items).

*****

4. Section 740.13 is amended by revising the section heading and paragraph (d)(2) to read as follows:

§ 740.13 Technology and Software--Unrestricted (TSU).

* * * * *

(d) ***

(2) *Exclusions*--(i) *Encryption software*. The provisions of this paragraph (d) are not available for encryption software controlled for "EI" reasons under ECCN 5D002 or for encryption software with symmetric key length exceeding 64-bits that qualifies as mass market encryption software under the criteria in the Cryptography Note (Note 3) of Category 5, Part 2, of the Commerce Control List (Supplement No. 1 to part 774 of the EAR). (Once such mass market encryption software has been reviewed by BIS and released from "EI" and "NS" controls pursuant to §742.15(b) of the EAR, it is controlled under ECCN 5D992.c and is thus outside the scope of License Exception TSU.) See §742.15(b) of the EAR for exports and reexports of mass market encryption products controlled under ECCN 5D992.c.

(ii) *Cybersecurity software*. The provisions of this paragraph (d) are not available for cybersecurity "software" that is classified under ECCNs 4D001.a ("specially designed" or modified for 4A005 or 4D004 items), 4D004, or for "software" under ECCN 5D001.a or .c ("specially designed" for "production," "development" or "use" of 5A001.j equipment or systems, or providing the characteristics, functions or features of 5A001.j or 5B001.a equipment or systems).

* * * * *

5. Section 740.17 is amended by revising paragraph (b)(3)(iii) introductory text to read as follows:

§ 740.17 Encryption commodities, software and technology (ENC).

* * * * *

(b) * * *

(3) * * *

(iii) Encryption commodities and software not described by paragraph (b)(2) of this section, and not further controlled for NS and RS reasons under ECCNs 5A001.j, 5B001.a ("specially designed" for 5A001.j), 5D001.a ("specially designed" or modified for 5A001.j) or 5D001.c ("specially designed" or modified for 5A001.j or 5B001.a), that provide or perform vulnerability analysis, network forensics, or computer forensics functions characterized by any of the following:

* * * * *

6. Section 740.20 is amended by adding paragraph (b)(2)(ix) to read as follows:

§ 740.20 License Exception Strategic Trade Authorization (STA).

* * * * *

(b) * * *

(2) * * *

(ix) License Exception STA may not be used for any cybersecurity items, i.e., those controlled by ECCNs 4A005, 4D001.a ("specially designed" or modified for 4A005 or 4D004 items), 4D004, 4E001.a ("required" for 4A005, 4D001.a ("specially designed" or modified for 4A005 or 4D004items) or 4D004 items), 4E001.c, 5A001.j, 5B001.a ("specially designed" for 5A001.j items), 5D001.a ("specially designed" or modified for 5A001.j items), 5D001.c ("specially designed" or modified for 5A001.j or 5B001.a items) or 5E001.a ("required" for 5A001.j, 5B001.a, 5D001.a ("specially designed" or modified for 5A001.j items) or 5D001.c ("specially designed" or modified for 5A001.j or 5B001.a items) items).

* * * * *

PART 742 [AMENDED]

7. 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.*; 22 U.S.C. 3201 *et seq.*; 42 U.S.C. 2139a; 22 U.S.C. 7201 *et seq.*; 22 U.S.C. 7210; Sec. 1503, Pub. L. 108–11, 117 Stat. 559; 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. 12938, 59 FR 59099, 3 CFR, 1994 Comp., p. 950; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783; Presidential Determination 2003–23 of May 7, 2003, 68 FR 26459, May 16, 2003; Notice of August 7, 2014, 79 FR 46959 (August 11, 2014); Notice of November 7, 2014, 79 FR 67035 (November 12, 2014).

8. Section 742.6 is amended by adding paragraph (b)(5) to read as follows:

§ 742.6 Regional stability.

* * * * *

(b) ***

(5) *Licensing policy for cybersecurity items.* Applications for exports, reexports and transfers of cybersecurity items, i.e., those controlled by ECCNs 4A005, 4D001.a ("specially designed" or modified for 4A005 or 4D004 items), 4D004, 4E001.a ("required" for 4A005, 4D001.a ("specially designed" or modified for 4A005 or 4D004 items) or 4D004 items), 4E001.c, 5A001.j, 5B001.a ("specially designed" for 5A001.j items), 5D001.a ("specially designed" or modified for 5A001.j items), 5D001.c ("specially designed" or modified for 5A001.j or 5B001.a items) or 5E001.a ("required" for 5A001.j, 5B001.a, 5D001.a ("specially designed" or modified for 5A001.j items) or 5D001.c ("specially designed" or modified for 5A001.j or 5B001.a items) items), controlled for RS will be reviewed favorably if destined to a U.S. company or subsidiary not located in Country Group D:1 or E:1, 'foreign commercial partners' located in Country Group A:5, Government end users in Australia, Canada, New Zealand or United Kingdom and on a case-by-case basis to determine whether the transaction is contrary to the national security or foreign policy interests of the United States, including the foreign policy interest of promoting the observance of human rights throughout the world, except that there is a policy of presumptive denial for items that have or support rootkit or zero-day exploit capabilities. Any "information security" functionality incorporated in the cybersecurity item will also receive a focused case-by-case review for reasons of Encryption Items (EI) control.

Note to paragraph (b)(5): *A 'foreign commercial partner' means a foreign-based non-governmental end-user that has a business need to share the proprietary information of the U.S. company and is contractually bound to the U.S. company (e.g., has an established pattern of continuing or recurring contractual relations). In addition to the information required in §748.3(c)(1),(c)(2) and paragraph (z) of Supplement No. 2 to part 748 of the EAR, you must* *explain in a letter of explanation how the end user meets the criteria of a 'foreign commercial partner' and how the end user will safeguard the items from unauthorized transfers (in*-country) *and reexports.*

*****

PART 748 – [AMENDED]

9. The authority citation for part 748 continues to read as follows:

Authority: 50 U.S.C. app. 2401 *et seq.*; 50 U.S.C. 1701 *et seq.*; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783; Notice of August 7, 2014, 79 FR 46959 (August 11, 2014).

10. Section 748.8 is amended by adding paragraph (z) to read as follows:

§748.8 Unique application and submission requirements.

*****

(z) Cybersecurity Items.

11. Supplement No. 2 is amended by adding paragraph (z) to read as follows:

Supplement No. 2 to Part 748—Unique Application and Submission Requirements

*****

(z) *Cybersecurity items*. For license applications to export, reexport, transfer (in-country) cybersecurity items, i.e., ECCNs 4A005, 4D001.a ("specially designed" or modified for 4A005 or 4D004 items), 4D004, 4E001.a (“required” for 4A005, 4D001.a (“specially designed” or modified for 4A005 or 4D004) or 4D004 items), 4E001.c, 5A001.j, 5B001.a (“specially designed” for 5A001.j items), 5D001.a (“specially designed” or modified for 5A001.j items), 5D001.c (“specially designed” or modified for 5A001.j or 5B001.a items) or 5E001.a (“required” for 5A001.j, 5B001.a, 5D001.a (“specially designed” or modified for 5A001.j items) or 5D001.c (“specially designed” or modified for 5A001.j or 5B001.a items) items) you must follow the unique application requirements set forth in this paragraph (z). If the cybersecurity item has encryption or other “information security” functionality classified under ECCNs 5A002, 5D002, 5A992.c, 5D992.c or 5E002, all encryption registration and review requirements must be separately completed with BIS and the ENC Encryption Request Coordinator, Ft. Meade, MD, before license applications for a cybersecurity item will be considered, see §§ 740.17 and 742.15 of the EAR.

(1) In block 9 of the application (Special Purpose) indicate the phrase “Cybersecurity Item.” In addition to the information required by §748.3(b) of the EAR, submit the following information in a letter of explanation:

(i) Whether the cybersecurity item has encryption or other “information security” functionality, Encryption Registration Number (ERN) and encryption Commodity Classification Application Tracking System (CCATS) number(s);

(ii) Whether the cybersecurity item has been previously classified or included in a license application submitted on or after [INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER] for which all requirements of this section (including the questions set forth in paragraph (z)(1)(iii) of this section) have been satisfied. If so, then provide the Commodity Classification Automated Tracking System (CCATS) number(s) or issued license number(s).

(iii) If the cybersecurity item has not been previously classified or included in a license application, then:

(A) Describe the cybersecurity functions and user interfaces (e.g., Application Programming Interfaces (APIs), Command Line Interfaces (CLIs) or Graphical User Interfaces (GUIs)) that are implemented and/or supported. Explain which are for internal use private to the developer of the product, and/or which are for use by the customer or other operator.

(B) Describe the cybersecurity functionality (including as related to "intrusion software") that is provided by third-party frameworks, platforms, tools, modules or components (if any). Identify the manufacturers of the cybersecurity items, including specific part numbers and version information as needed to describe the item. As applicable, describe whether the third-party cybersecurity software is statically or dynamically linked.

(C) For items related to "intrusion software," describe how rootkit or zero-day exploit functionality is precluded from the item. Otherwise, for items that incorporate or otherwise support rootkit or zero-day exploit functionality, this must be explicitly stated in the application.

(2) Upon request, include a copy of the sections of source code and other software (e.g., libraries and header files) that implement or invoke the controlled cybersecurity functionality.

PART 772 [AMENDED]

12. The authority citation for part 772 continues to read as follows:

Authority: 50 U.S.C. app. 2401 *et seq.*; 50 U.S.C. 1701 *et seq.*; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783; Notice of August 7, 2014, 79 FR 46959 (August 11, 2014).

13. Section 772.1 is amended by adding the term "Intrusion software" in alphabetic order to read as follows:

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

*****

Intrusion software. (Cat 4) "Software" "specially designed" or modified to avoid detection by 'monitoring tools,' or to defeat 'protective countermeasures,' of a computer or network-capable device, and performing any of the following:

(a) The extraction of data or information, from a computer or network-capable device, or the modification of system or user data; or

(b) The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.

Notes: *1. "Intrusion software" does not include any of the following:*

a. Hypervisors, debuggers or Software Reverse Engineering (SRE) tools;

b. Digital Rights Management (DRM) "software"; or

c. "Software" designed to be installed by manufacturers, administrators or users, for the purposes of asset tracking or recovery.

2. Network-capable devices include mobile devices and smart meters.

Technical Notes: *1. 'Monitoring tools': "software" or hardware devices, that monitor system behaviors or processes running on a device. This includes antivirus (AV) products, end point security products, Personal Security Products (PSP), Intrusion Detection Systems (IDS),* *Intrusion Prevention Systems (IPS) or firewalls.*

2. 'Protective countermeasures': techniques designed to ensure the safe execution of code, such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR) or sandboxing.

* * * * *

PART 774 [AMENDED]

14. 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); 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; 15 U.S.C. 1824a; 50 U.S.C. app. 5; 22 U.S.C. 7201 *et seq*.; 22 U.S.C. 7210; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783; Notice of August 7, 2014, 79 FR 46959 (August 11, 2014).

Supplement No. 1 to Part 774 – [Amended]

15. In Supplement No. 1 to Part 774 (the Commerce Control List), Category 4 is amended by adding ECCN 4A005 after ECCN 4A004 to read as follows:

Supplement No. 1 to Part 774 – The Commerce Control List

*****

4A005 "Systems," "equipment," or "components" therefor, "specially designed" or

modified for the generation, operation or delivery of, or communication with, “intrusion software”.

License Requirements

Reason for Control: NS, RS, AT

Control(s)	**Country Chart** **(See Supp. No.** **1 to part 738).**
NS applies to entire entry	NS Column 1
RS applies to the entire entry	RS Column 1
AT applies to entire entry	AT Column 1

License Requirement Note: *All license applications for 4A005 must include the information required in Supplement No. 2 to part 748 of the EAR, paragraph (z). Also, all such cybersecurity items using or incorporating encryption or other “information security” functionality classified under ECCNs 5A002, 5D002, 5A992.c, 5D992.c or 5E002, must also satisfy the registration, review and reporting requirements set forth in §§ 740.17, 742.15(b) and 748.3(d) of the EAR, including submissions to the ENC Encryption Request Coordinator, Ft. Meade, MD prior to applying for a license.*

List Based License Exceptions (See Part 740 for a description of all license exceptions)

LVS: N/A

GBS: N/A

CIV: N/A

Special Conditions for STA

STA: License Exception STA may not be used to export, reexport, or transfer (in-country) commodities controlled by ECCN 4A005 to any destination.

List of Items Controlled

Related Controls: (1) “Systems”, “equipment” and “components” described under ECCN 4A005 are classified under this ECCN, even if the “systems”, “equipment” or “components” are designed or modified to use “cryptography” or cryptanalysis. (2) See Categories XI(b) and XIII in the International Traffic in Arms Regulations (ITAR) (22 CFR parts 120 through 130) and the U.S. Munitions List (22 CFR part 121). (3) See also ECCN 4D001.a (“development” and “production” “software”), 4D004 and 4E001.a and .c.

Related Definitions: See § 772.1 of this EAR for the definition of “intrusion software.”

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

16. In Supplement No. 1 to Part 774 (the Commerce Control List), Category 4, ECCN 4D001 is amended by:

a. Revising the Reason for Control paragraph in the License Requirements section;

b. Adding an entry for “RS” after the entry for “NS” in the table in the License Requirements section;

c. Removing the NP note after the table in the License Requirements section and adding in its place a License Requirement Note;

d. Revising the TSR paragraph in the List Based License Exceptions section;

e. Revising the Special Conditions for STA section;

f. Revising the Related Controls paragraph in the List of Items Controlled section;

g. Revising Items paragraph a.

The revisions and addition read as follows:

4D001 "Software" as follows (see List of Items Controlled).

License Requirements

Reason for Control: NS, RS, CC, AT

Control(s)	Country Chart (See Supp. No. 1 to part 738)
*******	
RS applies to 4D001.a (if "specially designed" or modified for 4A005 or 4D004)	RS Column 1
*******	

License Requirement Note: *All license applications for 4D001.a (if "specially designed" or modified for 4A005 or 4D004) must include the information required in Supplement No. 2 to part 748 of the EAR, paragraph (z). Also, all such cybersecurity items using or incorporating encryption or other "information security" functionality classified under ECCNs 5A002, 5D002, 5A992.c, 5D992.c or 5E002, must also satisfy the registration, review and reporting* *requirements set forth in §§ 740.17, 742.15(b) and 748.3(d) of the EAR, including submissions to the ENC Encryption Request Coordinator, Ft. Meade, MD prior to applying for a license.*

******

List Based License Exceptions (See Part 740 for a description of all license exceptions)

*****

TSR: Yes, except for: (1) "software" "specially designed" or modified for the "development" or "production" of commodities with an "Adjusted Peak Performance" ("APP") exceeding 1.0 WT; or (2) "software" if "specially designed" or modified for the "development" or "production" of commodities or "software" specified by ECCNs 4A005 or 4D004.

*****

Special Conditions for STA

STA: License Exception STA may not be used to: (1) ship or transmit "software" "specially designed" or modified for the "development" or "production" of equipment specified by ECCN 4A001.a.2 or for the "development" or "production" of "digital computers" having an 'Adjusted Peak Performance' ('APP') exceeding 1.0 Weighted TeraFLOPS (WT) to any of the destinations listed in Country Group A:6 (See Supplement No.1 to part 740 of the EAR); or (2) ship or transmit "software" "specially designed" or modified for the "production" or "development" of commodities or "software" specified by ECCNs 4A005 or 4D004, to any destination.

List of Items Controlled

Related Controls: (1) "Software" described under ECCN 4D001 (if "specially designed" or modified for 4A005 or 4D004) is classified under this ECCN, even if the "software" is designed or modified to use “cryptography” or cryptanalysis. (2) See also the International Traffic in Arms Regulations (ITAR) (22 CFR parts 120 through 130) and the U.S. Munitions List (22 CFR part 121).

*****

Items: a. “Software” “specially designed” or modified for the “development” or “production”, of equipment controlled by 4A001, 4A003, 4A004, 4A005 or “software” controlled by 4D (except 4D980, 4D993 or 4D994).

*****

17. In Supplement No. 1 to Part 774 (the Commerce Control List), Category 4 is amended by adding ECCN 4D004 after ECCN 4D002 to read as follows:

4D004 “Software” “specially designed” or modified for the generation, operation or delivery of, or communication with, “intrusion software”.

License Requirements

Reason for Control: NS, RS, AT

Control(s)	**Country Chart** **(See Supp. No.** **1 to part 738).**

NS applies to entire entry	NS Column 1
RS applies to entire entry	RS Column 1
AT applies to entire entry	AT Column 1

License Requirement Note: *All license applications for 4D004 must include the information required in Supplement No. 2 to part 748 of this EAR, paragraph (z). Also, all such cybersecurity items using or incorporating encryption or other "information security" functionality classified under ECCNs 5A002, 5D002, 5A992.c, 5D992.c or 5E002, must also satisfy the registration, review and reporting requirements set forth in §§ 740.17, 742.15(b) and 748.3(d) of the EAR, including submissions to the ENC Encryption Request Coordinator, Ft. Meade, MD prior to applying for a license.*

List Based License Exceptions (See Part 740 for a description of all license exceptions)

CIV: N/A

TSR: N/A

Special Conditions for STA

STA: License Exception STA may not be used to export, reexport, or transfer (in-country) "software" controlled by ECCN 4D004 to any destination.

List of Items Controlled

Related Controls: (1) "Software" described under ECCN 4D004 is classified under this ECCN, even if the "software" is designed or modified to use "cryptography" or cryptanalysis.

(2) See also the International Traffic in Arms Regulations (ITAR) (22 CFR parts 120 through 130) and the U.S. Munitions List (22 CFR part 121). (3) See also ECCN 4E001.a.

Related Definitions: See § 772.1 of the EAR for the definition of "intrusion software."

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

18. In Supplement No. 1 to Part 774 (the Commerce Control List), Category 4, ECCN 4E001 is amended by:

a. Revising the Reasons for Control paragraph in the License Requirements section;

b. Adding an entry for "RS" after the entry for "MT" in the table in the License Requirements section;

c. Removing the NP note after the table in the License Requirements section and adding in its place a License Requirement Note;

d. Revising the TSR paragraph in the List Based License Exceptions section;

e. Revising the Special Conditions for STA section;

f. Revising the Related Controls and Related Definitions paragraphs in the List of Items Controlled section;

g. Adding paragraph c to the Items paragraph of the List of Items Controlled section.

The revisions and additions read as follows:

4E001 "Technology" as follows (see List of Items Controlled).

License Requirements

Reason for Control: NS, MT, RS, CC, AT

Control(s)	**Country Chart (See Supp. No. 1 to part 738)**
*******	
RS applies to 4E001.a "technology" (if "required" for 4A005, 4D001.a (if "specially designed" or modified for 4A005 or 4D004) or 4D004) and if "required" for 4E001.c	RS Column 1
*******	

License Requirement Note: *All license applications for 4E001.a "technology" (if "required" for 4A005, 4D001.a (if "specially designed" or modified for 4A005 or 4D004) or 4D004) and if "required" for 4E001.c must include the information required in Supplement No. 2 to part 748 of the EAR, paragraph (z). Also, all such cybersecurity items using or incorporating encryption or other "information security" functionality classified under ECCNs 5A002, 5D002, 5A992.c, 5D992.c or 5E002, must also satisfy the registration, review and reporting requirements set forth in §§ 740.17, 742.15(b) and 748.3(d) of the EAR, including submissions to the ENC Encryption Request Coordinator, Ft. Meade, MD prior to applying for a license.*

****

List Based License Exceptions (See Part 740 for a description of all license exceptions)

*****

TSR: Yes, except for: "technology" for the "development" or "production" of "commodities" with an "Adjusted Peak Performance" ("APP") exceeding 1.0 WT, "commodities" in 4A005 or "software" in 4D001.a (if "specially designed" or modified for 4A005 or 4D004) or "required" for 4D004; or "technology" specified by 4E001.c.

*****

Special Conditions for STA

STA: License Exception STA may not be used to ship or transmit "technology" according to the General Technology Note for the "development" or "production" of any of the following equipment or "software": a. Equipment specified by ECCN 4A001.a.2; b. "Digital computers" having an 'Adjusted Peak Performance' ('APP') exceeding 1.0 Weighted TeraFLOPS (WT); or .c "software" specified in the License Exception STA paragraph found in the License Exception section of ECCN 4D001 to any of the destinations listed in Country Group A:6 (See Supplement No.1 to part 740 of the EAR); or to ship any "technology" specified by 4E001.a "required" for "commodities" in 4A005 or "software" in 4D001.a (if "specially designed" or modified for 4A005 or 4D004), 4D004, or by 4E001.c, to any destination.

List of Items Controlled

Related Controls: (1) "Technology" described under ECCN 4E001.a ("required" for equipment in 4A005 or "software" in 4D001.a (if "specially designed" or modified for 4A005 or 4D004) or 4D004) or 4E001.c is classified under this ECCN, even if it includes "technology" for the "development" or "production" of cryptographic or cryptanalytic items.

(2) See also the International Traffic in Arms Regulations (ITAR) (22 CFR parts 120 through 130) and the U.S. Munitions List (22 CFR part 121).

Related Definitions: See § 772.1 for the definition of "intrusion software."

Items:***

c. "Technology" "required" for the "development" of "intrusion software".

19. In Supplement No. 1 to Part 774 (the Commerce Control List), Category 5, ECCN 5A001 is amended by:

a. Revising the Reason for Control paragraph in the License Requirements section;

b. Revising the first entry in the table in the License Requirements section;

c. Adding an entry for "RS" after the second entry in the table in the License Requirements section;

d. Adding a License Requirement Note after the table in the License Requirements section;

e. Revising the List Based License Exceptions section;

f. Revising the Special Conditions for STA section;

g. Revising the Related Controls paragraph of the List of Items Controlled section; and

h. Adding paragraph .j to the Items paragraph of the List of Items Controlled section.

The revisions and additions read as follows:

5A001 Telecommunications systems, equipment, "components" and "accessories," as follows (see List of Items Controlled).

License Requirements

Reason for Control: NS, RS, SL, AT

Control(s)	**Country Chart (See Supp. No. 1 to part 738)**
NS applies to 5A001.a, .e, .b.5, f.3, .h and .j.	NS Column 1
*******	
RS applies to 5A001.j	RS Column 1
*******	

License Requirement Note: *All license applications for cybersecurity items (5A001.j) must include the information required in Supplement No. 2 to part 748 of the EAR, paragraph (z). Also, all such cybersecurity items using or incorporating encryption or other "information security" functionality classified under ECCNs 5A002, 5D002, 5A992.c, 5D992.c or 5E002, must also satisfy the registration, review and reporting requirements set forth in §§ 740.17, 742.15(b) and 748.3(d) of the EAR, including submissions to the ENC Encryption Request Coordinator, Ft. Meade, MD prior to applying for a license.*

*****

List Based License Exceptions (See Part 740 for a description of all license exceptions)

LVS: N/A for 5A001.a, .b.5, .e, .f, .h, and .j;

$5000 for 5A001.b.1, .b.2, .b.3, .b.6, .d, and .g;

$3000 for 5A001.c.

GBS: Yes, except 5A001.a, .b.5, .e, .f, .h, and .j.

CIV: Yes, except 5A001.a, .b.3, .b.5, .e, .f, .h, and .j.

Special Conditions for STA

STA: License Exception STA may not be used to ship any commodity in 5A001.b.3, .b.5, or .h to any of the destinations listed in Country Group A:6 (See Supplement No.1 to part 740 of the EAR), or to ship any commodity in 5A001.j to any destination.

List of Items Controlled

Related Controls: (1) See USML Category XI for controls on direction-finding "equipment" including types of "equipment" in ECCN 5A001.e and any other military or intelligence electronic "equipment" that is "subject to the ITAR." (2) See USML Category XI(a)(4)(iii) for controls on electronic attack and jamming "equipment" defined in 5A001.f and .h that are subject to the ITAR. (3) "Systems," "equipment" and "components" described under ECCN 5A001.j are classified under this ECCN even if the "systems," "equipment" or "components" are designed or modified to use "cryptography" or cryptanalysis. (4) ECCN 5A001.j includes a note that explicitly excludes equipment designed for marketing purposes, quality of service (QoS) or quality of experience (QoE) purposes. The intent of the entry is to capture only products that are not "specially designed" for legitimate network operator functions. The control has very specific parameters and includes only systems or equipment that perform all five of the capabilities listed in 5A001.j below. Equipment that is not described in the new ECCN 5A001.j entry because it does not have all five capabilities required is likely to be described in ECCNs 5A002 or 5A992 if it has encryption functionality, or ECCNs 5A991 or 4A994 if it does not. However, such equipment may not be sold separately with knowledge that it will be combined with other equipment to comprise a system described in new paragraph ECCN 5A001.j. (see § 764.2(h) of the EAR) (5) See also 5A101, 5A980, and 5A991.

*****

Items: ***

j. IP network communications surveillance “systems” or “equipment”, and “specially designed” components therefor, having all of the following:

j.1. Performing all of the following on a carrier class IP network (e.g., national grade IP backbone):

j.1.a. Analysis at the application layer (e.g., Layer 7 of Open Systems Interconnection (OSI) model (ISO/IEC 7498-1));

j.1.b. Extraction of selected metadata and application content (e.g., voice, video, messages, attachments); *and*

j.1.c. Indexing of extracted data; *and*

j.2. Being “specially designed” to carry out all of the following:

j.2.a. Execution of searches on the basis of ‘hard selectors’; *and* j.2.b. Mapping of the relational network of an individual or of a group of people.

Note: *5A001.j does not apply to "systems" or "equipment", "specially designed" for any of the following:*

a. Marketing purpose;

b. Network Quality of Service (QoS); <u>or</u>

c. Quality of Experience (QoE).

Technical Note: *'Hard selectors': data or set of data, related to an individual (e.g., family name, given name, e-mail or street address, phone number or group affiliations).*

20. In Supplement No. 1 to Part 774 (the Commerce Control List), Category 5, ECCN 5B001 is amended by:

a. Revising the Reasons for Control paragraph of the License Requirements section;

b. Revising the table in the License Requirements section;

c. Adding a License Requirement Note after the table in the License Requirements section;

d. Revising the List Based License Exceptions section; and

e. Revising the Special Conditions for STA section.

The revisions and addition to read as follows:

5B001 Telecommunication test, inspection and production equipment, "components" and "accessories," as follows (See List of Items Controlled).

License Requirements

Reason for Control: NS, RS, AT

Control(s)	**Country Chart (See Supp. No. 1 to part 738)**
NS applies to 5B001.a equipment, "components" and "accessories" "specially designed" for 5A001.j.	NS Column 1
NS applies to entire entry (except 5B001.a for 5A001.j)	NS Column 2
RS applies to 5B001.a equipment, "components" and "accessories" "specially designed" for 5A001.j.	RS Column 1
AT applies to entire entry	AT Column 1

License Requirement Note: *All license applications for cybersecurity items (5B001.a equipment, "components" and "accessories" "specially designed" for 5A001.j) must include the information required in Supplement No. 2 to part 748 of the EAR, paragraph (z). Also, all such cybersecurity items using or incorporating encryption or other "information security" functionality classified under ECCNs 5A002, 5D002, 5A992.c, 5D992.c or 5E002, must also satisfy the registration, review and reporting requirements set forth in §§ 740.17, 742.15(b) and 748.3(d) of the EAR, including submissions to the ENC Encryption Request Coordinator, Ft. Meade, MD prior to applying for a license.*

* * * * *

List Based License Exceptions (See Part 740 for a description of all license exceptions)

LVS: $5000, except N/A for 5B001.a (for 5A001.f.1 or .j)

GBS: Yes, except for 5B001.a (for 5A001.f.1 or .j)

CIV: Yes, except for 5B001.a (for 5A001.f.1 or .j)

Special Conditions for STA

STA: License Exception STA may not be used to ship 5B001.a equipment and "specially designed" "components" or "accessories" therefor, "specially designed" for the "development" or "production" of equipment, functions or features specified by ECCN 5A001.b.3, .b.5 or .h to any of the destinations listed in Country Group A:6 (See Supplement No.1 to part 740 of the EAR), or to ship any commodity in 5B001.a for equipment or systems specified by 5A001.f.1. or .j to any destination.

* * * * *

21. In Supplement No. 1 to Part 774 (the Commerce Control List), Category 5, ECCN 5D001 is amended by:

a. Revising the Reasons for Control paragraph in the License Requirements section;

b. Adding an entry for "RS" after the entry for "NS" in the table in the License Requirements section;

c. Adding a License Requirement Note after the table in the License Requirements section;

d. Revising the List Based License Exceptions section;

e. Revising the Special Conditions for STA section; and

f. Revising the Related Controls paragraph in the List of Items Controlled section.

The revisions and additions read as follows:

5D001 “Software” as follows (see List of Items Controlled).

License Requirements

Reason for Control: NS, RS, SL, AT

Control(s)	Country Chart (See Supp. No. 1 to part 738)
* * * * * * *	
RS applies to 5D001.a “software” “specially designed” or modified for 5A001.j , and 5D001.c “software” “specially designed” or modified for 5A001.j or 5B001.a	RS Column 1
*******	

License Requirement Note: *All license applications for cybersecurity items (5D001.a “software” “specially designed” or modified for 5A001.j , and 5D001.c “software” “specially designed” or modified for 5A001.j or 5B001.a) must include the information required in Supplement No. 2 to part 748 of the EAR, paragraph (z). Also, all such cybersecurity items using or incorporating encryption or other “information security” functionality classified under ECCNs 5A002, 5D002, 5A992.c, 5D992.c or 5E002, must also satisfy the registration, review and reporting requirements set forth in §§ 740.17, 742.15(b) and 748.3(d) of the EAR, including submissions to the ENC Encryption Request Coordinator, Ft. Meade, MD prior to applying for a license.*

*****

List Based License Exceptions (See Part 740 for a description of all license exceptions)

CIV: Yes, except for "software" controlled by 5D001.a and "specially designed" or modified for the "development" or "production" of items controlled by 5A001.b.5, 5A001.f.1, 5A001.h and 5A001.j.

TSR: Yes, except for exports and reexports to destinations outside of those countries listed in Country Group A:5 (See Supplement No. 1 to part 740 of the EAR) of "software" controlled by 5D001.a and "specially designed" or modified for items controlled by 5A001.b.5, 5A001.f.1, 5A001.h and 5A001.j.

Special Conditions for STA

STA: License Exception STA may not be used to ship or transmit 5D001.a "software" "specially designed" or modified for the "development" or "production" of equipment, functions or features, specified by ECCN 5A001.b.3, .b.5, .f.1, .h or .j; and for 5D001.b. for "software" "specially designed" or modified to support "technology" specified by the STA paragraph in the License Exception section of ECCN 5E001 to any of the destinations listed in Country Group A:6 (See Supplement No.1 to part 740 of the EAR); and for 5D001.c. for "software" "specially designed" or modified to provide characteristics, functions or features of equipment or systems classified under ECCNs 5A001.f.1 or .j, or 5B001.a (for 5A001.f.1 or .j)).

List of Items Controlled

Related Controls: (1) "Software" described under ECCN 5D001.a or .c (if "specially designed" or modified for 5A001.j) is classified under this ECCN, even if the "software" is designed or modified to use “cryptography” or cryptanalysis. (2) See also 5D980 and 5D991.

*****

22. In Supplement No. 1 to Part 774 (the Commerce Control List), Category 5, Part 1, ECCN 5E001 is amended by:

a. Revising the Reasons for Control paragraph in the License Requirements section;

b. Adding an entry for “RS” after the entry for “NS” in the table in the License Requirements section;

c. Adding a License Requirement Note after the table in the License Requirements section;

d. Revising the TSR paragraph in the List Based License Exceptions section;

e. Revising the Special Conditions for STA section; and

f. Adding paragraph (3) to the Related Control paragraph in the List of Items Controlled section.

The revisions and additions read as follows:

5E001 “Technology” as follows (see List of Items Controlled).

License Requirements

Reason for Control: NS, RS, SL, AT

Control(s)	**Country Chart (See Supp. No. 1 to part 738)**

*******	
RS applies to 5E001.a for commodities controlled under 5A001.j or “software” controlled under 5D001.a (if “specially designed” or modified for 5A001.j) , and 5D001.c (if “specially designed” or modified for 5A001.j or 5B001.a) for RS reasons	RS Column 1
*******	

License Requirement Note: *All license applications for cybersecurity items (5A001.j or “software” controlled under 5D001.a (if “specially designed” or modified for 5A001.j) , and 5D001.c (if “specially designed” or modified for 5A001.j or 5B001.a)) must include the information required in Supplement No. 2 to part 748 of the EAR, paragraph (z). Also, all such cybersecurity items using or incorporating encryption or other “information security” functionality classified under ECCNs 5A002, 5D002, 5A992.c, 5D992.c or 5E002, must also satisfy the registration, review and reporting requirements set forth in §§ 740.17, 742.15(b) and 748.3(d) of the EAR, including submissions to the ENC Encryption Request Coordinator, Ft. Meade, MD prior to applying for a license.*

*****

List Based License Exceptions (See Part 740 for a description of all license exceptions)

****

TSR: Yes, except: N/A for “technology” controlled by 5E001.a if “required” for the “development” or “production” of items controlled by 5A001.f.1. or .j, 5D001.a (if “specially designed" or modified for 5A001.f.1 or .j) or 5D001.c (if "specially designed" or modified for 5A001.j or 5B001.a) to any destination; or for exports or reexports to destinations outside of those countries listed in Country Group A:5 (See Supplement No. 1 to part 740 of the EAR) of "technology" controlled by 5E001.a for the "development" or "production" of the following:

(1) Items controlled by 5A001.b.5 or 5A001.h; or

(2) "Software" controlled by 5D001.a that is "specially designed" or modified for the "development" or "production" of equipment, functions or features controlled by 5A001.b.5 or 5A001.h.

Special Conditions for STA

STA: License Exception STA may not be used to ship or transmit "technology" according to the General Technology Note for the "development" or "production" of equipment, functions or features specified by 5A001.b.3, .b.5 or .h; or for "software" in 5D001.a that is specified in the STA paragraph in the License Exception section of ECCN 5D001 to any of the destinations listed in Country Group A:6 (See Supplement No.1 to part 740 of the EAR); or to ship any "technology" in 5E001.a if "required" for any commodity in 5A001.f.1 or .j, or if "required" for any "software" in 5D001.a or .c ("specially" or modified designed for any commodity in 5A001.f.1 or .j or 5B001.a ("specially designed" for 5A001.f.1 or .j)), to any destination.

List of Items Controlled

Related Controls: *** (3) "Technology" described under ECCN 5E001.a if "required" for "systems," "equipment" or "components" classified under 5A001.j or "software" classified under 5D001.a ("specially designed" or modified for 5A001.j) or 5D001.c ("specially designed" or modified for 5A001.j or 5B001.a) is classified under this ECCN even if it includes "technology" for the "development" or "production" of cryptographic or cryptanalytic items.

*****

23. In Supplement No. 1 to Part 774 (the Commerce Control List), Category 5 Part 2, ECCN 5A002 is amended by adding paragraph (4) to the Related Controls paragraph in the List of Items Controlled section to read as follows:

5A002 "Information security" systems, equipment "components" therefor, as follows (see List of Items Controlled).

*****

List of Items Controlled

Related Controls: *** (4) "Systems," "equipment" and "components" described under ECCNs 4A005 or 5A001.j are classified under ECCNs 4A005 or 5A001.j, even if the "systems," "equipment" or "components" are designed or modified to use "cryptography" or cryptanalysis.

*****

24. In Supplement No. 1 to Part 774 (the Commerce Control List), Category 5 Part 2, ECCN 5D002 is amended by adding paragraph (3) to the Related Controls paragraph in the List of Items Controlled section to read as follows:

5D002 “Software” as follows (see List of Items Controlled).

*****

List of Items Controlled

Related Controls: *** (3) “Software” described under ECCN 4D001.a (“specially designed” or modified for 4A005 or 4D004), 4D004, 5D001.a (“specially designed” or modified for 5A001.j) or 5D001.c (“specially designed” or modified for 5A001.j or 5B001.a) is classified under those ECCNs, even if the “software” is designed or modified to use “cryptography” or cryptanalysis.

*****

25. In Supplement No. 1 to Part 774 (the Commerce Control List), Category 5 Part 2, ECCN 5E002 is amended by revising the Related Controls paragraph in the List of Items Controlled section to read as follows:

5E002 “Technology” as follows (see List of Items Controlled).

*****

List of Items Controlled

Related Controls: (1) See also 5E992. This entry does not control “technology” “required” for the “use” of equipment excluded from control under the Related Controls paragraph or the Technical Notes in ECCN 5A002 or “technology” related to equipment excluded from control under ECCN 5A002. This “technology” is classified as ECCN 5E992. (2) “Technology” described under ECCN 4E001.a (“required” for equipment in 4A005 or “software” in 4D004), 4E001.c, or 5E001.a (“required” for 5A001.j or 5D001.a) that is designed or modified to use “cryptography” or cryptanalysis is classified under ECCNs 4E001.a or .c, or ECCN 5E001.a, respectively.

*****

Dated: May 11, 2015.

Kevin J. Wolf,

Assistant Secretary for Export Administration.

[FR Doc. 2015-11642 Filed: 5/19/2015 08:45 am; Publication Date: 5/20/2015]