Category 5 Part 1 – "Telecommunications"

5D001 "Software"

ECCN 5D001 is amended by removing and reserving Items paragraph .b, "Software" "specially designed" or modified to support "technology" controlled by 5E001, because this control is outdated and no longer in use.

5E001 "Technology"

ECCN 5E001 is amended by revising Items paragraph c.1, infrastructure transmission and switching "technology", to raise the "total digital transfer rate" from 120 Gbit/s to 560 Gbit/s in order to accommodate advances in technology and in public standards.

Category 5 Part 2 – "Information Security"

Category 5 Part 2 is amended to revise Note 1 to Category 5 Part 2, 5A002.a and 5A002.b to clarify that these entries apply to any system, equipment or component that meet the control parameters specified in a particular 5A002 or 5B002 entry. Prior to this revision there was a risk that exporters would interpret the current language to exclude some items that have "information security" functionality but are not specifically listed. The definition of "cryptanalytic items" in § 772.1 of the EAR is similarly revised, for the same reasons.

ECCN 5A002 is amended by revising the Related Controls paragraph in the List of Items Controlled section to add recently added paragraphs, i.e., (k), (l), and (m) to Related Controls Note 2.

This rule also revises paragraph (j) in the Note at the beginning of the Items section, 5A002.b, 5D002.d and 5E002.b and the definition of "cryptographic activation" in order to address a loophole regarding the 'cryptographic activation' controls. The concept of "cryptographic activation" was introduced in 2010. The purpose of (j) is to release from control cryptographic equipment where the cryptographic capability cannot be enabled without some kind of additional mechanism such as a license key that is securely kept and bound to the equipment being activated. However, it was found that the original wording of the definition did not explicitly exclude certain circumstances by which export controls on cryptography could be circumvented by a manufacturer.

A new paragraph (l) is added to the Note at the beginning of Items paragraph to exclude from 5A002 routers, switches or relays, where the "information security" functionality is limited to the tasks of "Operations, Administration or Maintenance – OAM," implementing only published or commercial cryptographic standards. In addition, a definition for "Operations, Administration or Maintenance" ("OAM") is added to § 772.1 of the EAR, as well as a new Note under 5D002.c.

New paragraph (m) is added to the Note at the beginning of the Items paragraph to exclude from 5A002 general purpose computing equipment or servers having standard 'information security' functionality from their embedded mass market microprocessors (CPUs) and operating systems, in addition to OAM functionality.

The Note to 5A002.a.2 (Equipment performing cryptanalytic functions) is amended by replacing the word 'cryptanalysis' with 'cryptanalytic functions' and adding a new Technical Note to clarify the meaning of 'cryptanalytic functions'. This eliminates ambiguity by explicitly defining the term 'cryptanalytic functions' for purposes of the control, while keeping the term

'cryptanalysis' as a local definition to the overall definition of "information security."

The definition of "cryptanalytic items" in § 772.1 of the EAR is similarly revised to make clear references to 'cryptanalytic functions' and 'cryptanalysis.'

Items paragraph a.9 and the Technical Note following Items paragraph a.9 are corrected by replacing the single quotes with double quotes around the term "quantum cryptography" and removing Technical Note 1, which is the definition for "quantum cryptography," because that term is now defined in § 772.1 of the EAR. See § 774.1(d) regarding the quote system used in the CCL.

Category 6 - Sensors and Lasers

6A001 Acoustic systems, equipment and "components"

ECCN 6A001 is amended by revising Items paragraph a.1.a.2.a.2; the Technical Note after Items paragraph a.1.a.2.a.2; and Items paragraph a.1.a.3. Items paragraph a.1.a.2.a.2 (Underwater survey equipment designed for seabed topographic mapping) is amended to add the unit "m/s" to the sounding rate parameter. The Technical Note that defines 'sounding rate' is amended by adding the guidance, "for systems that produce soundings in two directions (3D sonars), the maximum of the 'sounding rate' in either direction should be used."

Items paragraph a.1.a.3 (Side Scan Sonar (SSS) or Synthetic Aperture Sonar (SAS), designed for seabed imaging) is amended by adding a control for "specially designed transmitting and receiving acoustic arrays therefor," because the quality and size of the transmitting and receiving hydrophone arrays is a key component to the performance of the overall system.

reporting requirements with the revised Regional Stability requirements for these items in § 742.6 and the overall national security country group amendments.

Part 772 Definitions

Section 772.1 is amended by adding in alphabetical order the terms: fly-by-light system, fly-by-wire system, library, operations, administration or maintenance (OAM), plasma atomization, quantum cryptography, spacecraft bus, and spacecraft payload; and revising the terms: civil aircraft, cryptanalytic items, cryptographic activation, end-effectors, information security, local area network, and technology.

See § 774.1(d) regarding the quote system used in the CCL. If a term on the CCL uses double quotes it means there is a defined term in part 772. However, the absence of double quotes does not mean that a term used on the CCL is not defined in part 772.

The reason for revising the definition of the term "civil aircraft" is stated under the explanation for amendments of ECCN 7A003 above.

The definition of "cryptographic activation" was restructured, and in places reworded, to more clearly and precisely reflect the 2010 Wassenaar agreements, without changing the scope. The words "of an item" were added after "Any technique that activates or enables cryptographic capability," and additional wording makes clear that the 'mechanism for "cryptographic activation"' must be "uniquely bound" to "a single instance of the item" or to "one customer, for multiple instances of the item." These clarifications convey that "cryptographic activation" does not include changing or upgrading the controlled cryptographic functionality of a previously exported item, or using a single license key or digitally-signed certificate to activate multiple

types of items. For editorial reasons, the explanation that license keys or digitally-signed certificates can be 'mechanisms for "cryptographic activation" was moved into the Technical Notes.

The definition for the term "end-effectors" is amended by replacing the double quotes with single quotes around the term "active tooling units," because the definition for "active tooling unit" is in the Note to the definition of "end-effectors" and is not a separate term defined in Section 772.1 of the EAR.

The terms "fly-by-wire" and "fly-by-light" are added to Section 772.1 in order to help the exporting community understand the scope of the new controls in ECCNs 7D004 and 7E004.

The reference for the term "information security" is amended by replacing the reference to (Cat 5) with (Cat 4, 5P1, 5P2, 8, GSN) because this term is used in all these locations. In addition, double quotes are replaced by single quotes around the term 'cryptanalysis' because this term is defined in the Technical Note to the definition of "information security."

The definition of "local area network" is amended by replacing double quotes with single quotes around the term 'data devices,' because the term is defined in a Note to the term "local area network."

The terms "operations, administration or maintenance" ("OAM") and "quantum cryptography" are added to § 772.1 and the term "cryptanalytic items" is revised for reasons stated under "Category 5 Part 2 – "Information Security" above.

The term "plasma atomization" is added to § 772.1 for reasons stated under ECCN 1C002 above.

The terms "spacecraft bus" and "spacecraft payload" are added to § 772.1 for reasons stated

14. Section 772.1 is amended by:

a. Adding definitions in alphabetical order for: "Fly-by-light system", "Fly-by-wire system", "Library", "Operations, Administration or Maintenance (OAM)", "Plasma atomization", "Quantum cryptography", "Spacecraft bus", "Spacecraft payload", and "Unidirectional positioning repeatability";

b. Removing the definition for "Cooperating country"; and

c. Revising the definitions for: "Civil aircraft", "Cryptanalytic items", "Cryptographic activation", "End-effectors", "Information security", "Local area network", and "Technology".

The additions and revisions read as follows:

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

*****

Civil aircraft. (Cat 1, 3, 4, 7 and 9) Those "aircraft" listed by designation in published airworthiness certification lists by civil aviation authorities of one or more Wassenaar Arrangement Participating States to fly commercial civil internal and external routes or for legitimate civil, private or business use. (see also "aircraft")

*****

Cryptanalytic items. (Cat 5P2) Systems, equipment or components 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.

NOTES: 1. 'Cryptanalytic functions' are functions designed to defeat cryptographic mechanisms in order to derive confidential variables or sensitive data, including clear text, passwords or cryptographic keys. These functions may include 'cryptanalysis,' which is the analysis of a cryptographic system or its inputs and outputs to derive confidential variables or sensitive data, including clear text. (ISO 7498-2-1988 (E), paragraph 3.3.18).

***2.** Functions specially designed and limited to protect against malicious computer damage or unauthorized system intrusion (e.g., viruses, worms and trojan horses) are not construed to be 'cryptanalytic functions.').*

Cryptographic activation. (Cat 5P2) Any technique that activates or enables cryptographic capability of an item, by means of a secure mechanism implemented by the manufacturer of the item, where this mechanism is uniquely bound to any of the following:

(a) A single instance of the item; or

(b) One customer, for multiple instances of the item.

***Technical Notes to definition of "Cryptographic activation**": 1. "Cryptographic activation" techniques and mechanisms may be implemented as hardware, "software" or "technology".*

2. Mechanisms for "cryptographic activation" can, for example, be serial number-based license keys or authentication instruments such as digitally signed certificates.

*****

End-effectors. (Cat 2) Grippers, 'active tooling units' and any other tooling that is attached to the baseplate on the end of a "robot" manipulator arm.

Technical Note to definition of "End-effectors": 'Active tooling unit': a device for applying motive power, process energy or sensing to the workpiece.

*****

Fly-by-light system. (Cat 7) A primary digital flight control system employing feedback to control the aircraft during flight, where the commands to the effectors/actuators are optical signals.

Fly-by-wire system. (Cat 7) A primary digital flight control system employing feedback to control the aircraft during flight, where the commands to the effectors/actuators are electrical signals.

*****

Information security. (Cat 4, 5P1, 5P2, 8, GSN)--All the means and functions ensuring the accessibility, confidentiality or integrity of information or communications, excluding the means and functions intended to safeguard against malfunctions. This includes "cryptography", "cryptographic activation", "cryptanalysis", protection against compromising emanations and computer security.

Technical Note to definition of ''Information security'': *'Cryptanalysis': the analysis of a cryptographic system or its inputs and outputs to derive confidential variables or sensitive data, including clear text. (ISO 7498–2–1988 (E), paragraph 3.3.18)*

*****

Library. (Cat 1) (parametric technical database) A collection of technical information, reference to which may enhance the performance of the relevant systems, equipment or components.

*****

Local area network. (Cat 4 and 5 Part 1)--A data communication system that:

(a) Allows an arbitrary number of independent 'data devices' to communicate directly with each other; and

(b) Is confined to a geographical area of moderate size (e.g., office building, plant, campus, warehouse).

Technical Note to definition of "Local area network": *'Data device' means equipment capable of transmitting or receiving sequences of digital information.*

*****

Operations, Administration or Maintenance ("OAM"). (Cat 5P2) Means performing one or more of the following tasks:

(a) Establishing or managing any of the following:

(1) Accounts or privileges of users or administrators;

(2) Settings of an item; or

(3) Authentication data in support of the tasks described in paragraphs (a)(1) or (2) of this definition;

(b) Monitoring or managing the operating condition or performance of an item; or

(c) Managing logs or audit data in support of any of the tasks described in paragraphs (a) or (b) of this definition.

Note to definition of "Operations, Administration or Maintenance": *"OAM" does not include any of the following tasks or their associated key management functions:*

a. Provisioning or upgrading any cryptographic functionality that is not directly related

to establishing or managing authentication data in support of the tasks described in paragraphs (a)(1) or (2) of this definition; or

b. Performing any cryptographic functionality on the forwarding or data plane of an item.

*****

Plasma atomization. (Cat 1) A process to reduce a molten stream or solid metal to droplets of 500 µm diameter or less, using plasma torches in an inert gas environment.

*****

Quantum cryptography. (Cat 5P2) A family of techniques for the establishment of a shared key for "cryptography" by measuring the quantum-mechanical properties of a physical system (including those physical properties explicitly governed by quantum optics, quantum field theory, or quantum electrodynamics).

*****

Spacecraft bus. (Cat 9) Equipment that provides the support infrastructure of the "spacecraft" and location for the "spacecraft payload".

Spacecraft payload. (Cat 9) Equipment, attached to the "spacecraft bus", designed to perform a mission in space (e.g., communications, observation, science).

*****

Technology. (General Technology Note, throughout EAR) Specific information necessary for the "development", "production", or "use" of a product. The information takes the form of 'technical data' or 'technical assistance'.

N.B.: Controlled "technology" is defined in the General Technology Note and in the Commerce Control List (Supplement No. 1 to part 774 of the EAR).

Note 1 to definition of "Technology": "Technology" also is specific information necessary for any of the following: operation, installation (including on-site installation), maintenance (checking), repair, overhaul, refurbishing, or other terms specified in ECCNs on the CCL that control "technology."

Note 2 to definition of "Technology": "Technology" not elsewhere specified on the CCL is designated as EAR99, unless the "technology" is subject to the exclusive jurisdiction of another U.S. Government agency (see § 734.3(b)(1) of the EAR) or is otherwise not subject to the EAR (see § 734.4(b)(2) and (3) and §§ 734.7 through 734.11 of the EAR).

Technical Notes to definition of "Technology": 1. 'Technical data' May take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read only memories.

2. 'Technical assistance' may take forms such as instruction, skills, training, working knowledge, consulting services. 'Technical assistance' may involve transfer of 'technical data'. 'Technical assistance' may involve transfer of 'technical data'.

*****

Unidirectional positioning repeatability. (Cat 2) The smaller of values R↑ and R↓ (forward and

38. In Supplement No. 1 to part 774, ECCN 5A002 is amended by**:**

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

b. Revising paragraphs (j) and (k) of the Note at the beginning of the Items paragraph;

c. Adding paragraphs (l) and (m) to the of the Note at the beginning of the Items paragraph;

d. Revising the introductory text of Items paragraph a;

e. Revising Items paragraph a.2 and the Note to 5A002.a.2;

f. Adding a Technical Note following the Note to 5A002.a.2;

g. Revising Items paragraph a.9 and the Technical Notes following paragraph a.9; and

h. Revising Items paragraph b.

The revisions and additions read as follows:

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

*****

List of Items Controlled

Related Controls: (1) ECCN 5A002.a controls "components" providing the means or functions necessary for "information security." All such "components" are presumptively "specially designed" and controlled by 5A002.a. (2) 5A002 does not control the commodities listed in paragraphs (a), (d), (e), (f), (g), (i), (j), (k), (l) and (m) in the Note in the items paragraph of this entry. These commodities are instead classified under ECCN 5A992, and

related software and technology are classified under ECCNs 5D992 and 5E992 respectively.

(3) After encryption registration to or classification by BIS, mass market encryption commodities that meet eligibility requirements are released from "EI" and "NS" controls. These commodities are classified under ECCN 5A992.c. See §742.15(b) of the EAR.

*****

Items:

***Note**: * * **

(j) Equipment, having no functionality specified by 5A002.a.2, 5A002.a.4, 5A002.a.7, 5A002.a.8 or 5A002.b, meeting all of the following:

1. All cryptographic capability specified by 5A002.a meets any of the following:

a. It cannot be used; or

b. It can only be made useable by means of "cryptographic activation"; and

2. When necessary as determined by the appropriate authority in the exporter's country, details of the equipment are accessible and will be provided to the authority upon request, in order to ascertain compliance with conditions described above;

***N.B.1**: See 5A002.a for equipment that has undergone "cryptographic activation."*

***N.B.2**: See also 5A002.b, 5D002.d and 5E002.b.*

(k) Mobile telecommunications Radio Access Network (RAN) equipment designed for civil use, which also meet the provisions 2. to 5. of part a. of the Cryptography Note (Note 3 in Category 5, Part 2), having an RF output power limited to 0.1W (20 dBm) or less, and supporting 16 or fewer concurrent users;

(l) Routers, switches or relays, where the "information security" functionality is limited

to the tasks of "Operations, Administration or Maintenance" ("OAM") implementing only published or commercial cryptographic standards; or

(m) General purpose computing equipment or servers, where the "information security" functionality meets all of the following:

1. Uses only published or commercial cryptographic standards; and

2. Is any of the following:

a. Integral to a CPU that meets the provisions of Note 3 to Category 5-Part 2;

b. Integral to an operating system that is not specified by 5D002; or

c. Limited to "OAM" of the equipment.

a. Systems, equipment and components, for "information security", as follows:

*****

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

***Note**: 5A002.a.2 includes systems or equipment, designed or modified to perform 'cryptanalytic functions' by means of reverse engineering.*

***Technical Note:** 'Cryptanalytic functions' are functions designed to defeat cryptographic mechanisms in order to derive confidential variables or sensitive data, including clear text, passwords or cryptographic keys.*

*****

a.9. Designed or modified to use or perform "quantum cryptography."

***Technical Note**: "Quantum cryptography" is also known as Quantum Key Distribution (QKD).*

b. Systems, equipment and components, designed or modified to enable, by means of

"cryptographic activation", an item to achieve or exceed the controlled performance levels for functionality specified by 5A002.a that would not otherwise be enabled.

39. In Supplement No. 1 to part 774, ECCN 5D002 is amended by

a. Adding a Note to 5D002.c after Items paragraph c.2; and

b. Revising Items paragraph d.

The revisions read as follows:

5D002 "Software" as follows (see List of Items Controlled)

*****

List of Items Controlled

*****

Items: ***

c. ***

c.2. ***

***Note**: 5D002.c does not apply to "software" limited to the tasks of "OAM" implementing only published or commercial cryptographic standards.*

d. "Software" designed or modified to enable, by means of "cryptographic activation," an item to achieve or exceed the controlled performance levels for functionality specified by 5A002.a that would not otherwise be enabled.

40. In Supplement No. 1 to part 774, ECCN 5E002 is amended by revising Items paragraph b and the Note to 5E002 to read as follows:

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

*****

List of Items Controlled

*****

*Items:****

b. "Technology" to enable, by means of "cryptographic activation," an item to achieve or exceed the controlled performance levels for functionality specified by 5A002.a that would not otherwise be enabled.

***Note**: 5E002 includes "information security" technical data resulting from procedures carried out to evaluate or determine the implementation of functions, features or techniques specified in Category 5-Part 2.*

41. In Supplement No. 1 to part 774, ECCN 6A001 is amended by:

a. Revising Items paragraph a.1.a.2.a.2 and the Technical Note following Items paragraph a.1.a.2.a.2;

b. Revising the introductory text of Items paragraph a.1.a.3;

c. Revising Note 1 after Items paragraph a.1.c;

d. Revising Items paragraph a.1.c.1;

e. Removing and reserving Items paragraph a.1.c.2 and removing the Technical Note following Items paragraph a.1.c.2; and

f. Adding a N.B. after paragraph a.1.c.2.

The revisions and additions read as follows: