

**CATEGORY 5 - TELECOMMUNICATIONS
AND "INFORMATION SECURITY"**

II. "Information Security"

Note 1: The control status of "information security" equipment, "software", systems, application specific "electronic assemblies", modules, integrated circuits, components, or functions is determined in Category 5, part 2 even if they are components or "electronic assemblies" of other equipment.

N.B. to Note 1: Commodities and software specially designed for medical end-use that incorporate an item in Category 5, part 2 are not classified in any ECCN in Category 5, part 2.

Note 2: Category 5, part 2, encryption products, when accompanying their user for the user's personal use or as tools of trade, are eligible for License Exceptions TMP or BAG, subject to the terms and conditions of these License Exceptions.

Note 3: Cryptography Note: ECCNs 5A002 and 5D002 do not control items that meet all of the following:

a. Generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of the following:

1. Over-the-counter transactions;
2. Mail order transactions;
3. Electronic transactions; or
4. Telephone call transactions;

b. The cryptographic functionality cannot be easily changed by the user;

c. Designed for installation by the user without further substantial support by the supplier; and

d. When necessary, details of the items are accessible and will be provided, upon request, to the appropriate authority in the exporter's country in order to ascertain compliance with conditions described in paragraphs (a) through (c) of this note.

N.B. to Cryptography Note: Mass market encryption commodities and software eligible for the Cryptography Note employing a key length greater than 64 bits for the symmetric algorithm must be reviewed in accordance with the requirements of §742.15(b) of the EAR in order to be released from the "EI" and "NS" controls of ECCN 5A002 or 5D002.

A. SYSTEMS, EQUIPMENT AND COMPONENTS

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

License Requirements

Reason for Control: NS, AT, EI

<i>Control(s)</i>	<i>Country Chart</i>
-------------------	----------------------

NS applies to entire entry	NS Column 1
----------------------------	-------------

AT applies to entire entry	AT Column 1
----------------------------	-------------

EI applies to 5A002.a.1, a.2, a.5, a.6 and a.9. Refer to §742.15 of the EAR.

License Exceptions

LVS: Yes: \$500 for components and spare

parts only. N/A for equipment.
 GBS: N/A
 CIV: N/A
 ENC: Yes for certain EI controlled commodities, see §740.17 of the EAR for eligibility.

is assessed individually.

List of Items Controlled

Unit: \$ value

Related Controls:(1) [5A002](#) does not control the commodities listed in paragraphs (a) through (f) 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. (2) After a review and 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.

Related Definitions: N/A

Items:

Note: *5A002 does not control any of the following. However, these items are instead controlled under 5A992:*

(a) *“Personalized smart cards” having any of the following:*

- (1) *Where the cryptographic capability is restricted for use in equipment or systems excluded from entries (b) through (g) of this Note; or*
- (2) *For general public-use applications where the cryptographic capability is not user-accessible and it is specially designed and limited to allow protection of personal data stored within;*

N.B.: If a “personalized smart card” has multiple functions, the status of each function

(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) *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 contents stored on 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;*

(3) *Copying control of copyright protected audio/video data; or*

(4) *Encryption and/or decryption for protection of libraries, design attributes, or associated data for the design of semiconductor devices or integrated circuits;*

(d) *Cryptographic equipment specially designed and limited for banking use or ‘money transactions’;*

Technical Note: The term ‘money transactions’ includes the collection and settlement of fares or credit functions.

(e) *Portable or mobile radiotelephones for civil use (e.g., for use with commercial civil cellular radio communication systems) that*

are not capable of transmitting encrypted data directly to another radiotelephone or equipment (other than Radio Access Network (RAN) equipment), nor of passing encrypted data through RAN equipment (e.g., Radio Network Controller (RNC) or Base Station Controller (BSC));

- (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 base station) is less than 400 meters according to the manufacturer's specifications;
- (g) Portable or mobile radiotelephones and similar client wireless devices for civil use, that implement only published or commercial cryptographic standards (except for anti-piracy functions, which may be non-published) and also meet the provisions of paragraphs b. to d. of the Cryptography Note (Note 3 in Category 5 - Part 2), that have been customized for a specific civil industry application with features that do not affect the cryptographic functionality of these original non-customized devices;
- (h) Equipment specially designed for the servicing of portable or mobile radiotelephones and similar client wireless devices that meet all the provisions of the Cryptography Note (Note 3 in Category 5, Part 2), where the servicing equipment meets all of the following:
- (1) The cryptographic functionality of the servicing equipment cannot easily be changed by the user of the equipment;
 - (2) The servicing equipment is designed for installation without further substantial support by the supplier; and
 - (3) The servicing equipment cannot change

the cryptographic functionality of the device being serviced; or

- (i) Wireless "personal area network" equipment that implement only published or commercial cryptographic standards and where the cryptographic capability is limited to a nominal operating range not exceeding 30 metres according to the manufacturer's specifications.
- a. Systems, equipment, application specific "electronic assemblies", modules and integrated circuits for "information security", as follows and other specially designed components therefor:

N.B.: For the control of Global Navigation Satellite Systems (GNSS) receiving equipment containing or employing decryption (i.e., GPS or GLONASS) see 7A005.

a.1. Designed or modified to use "cryptography" employing digital techniques performing any cryptographic function other than authentication or digital signature and 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, not controlled in 5A002.a.6., including the hopping code for “frequency hopping” systems;

a.6. Designed or modified to use cryptographic techniques to generate channelizing codes, scrambling codes or network identification codes, for systems using ultra-wideband modulation techniques and having any of the following:

a.6.a. A bandwidth exceeding 500 MHz;
or

a.6.b. A “fractional bandwidth” of 20% or more;

a.7. Non-cryptographic information and communications technology (ICT) security systems and devices evaluated to an assurance level exceeding class EAL-6 (evaluation assurance level) of the Common Criteria (CC) or equivalent;

a.8. Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion;

a.9. Designed or modified to use ‘quantum cryptography.’

Technical Notes:

1. ‘Quantum cryptography’ 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).

2. ‘Quantum cryptography’ is also known as Quantum Key Distribution (QKD).

5A992 Equipment not controlled by 5A002.

License Requirements

Reason for Control: AT

Control(s) Country Chart

AT applies to entire entry AT Column 1

License Exceptions

LVS: N/A
GBS: N/A
CIV: N/A

LVS: N/A
GBS: N/A
CIV: N/A
ENC: Yes for certain EI controlled equipment, see §740.17 of the EAR for eligibility.

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.
- c. Commodities that have been reviewed and determined to be mass market encryption commodities in accordance with §742.15(b) of the EAR.

List of Items Controlled

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

- a. Equipment specially designed for the “development” or “production” of equipment controlled by 5A002 or 5B002.b;
- b. Measuring equipment specially designed to evaluate and validate the “information security” functions of equipment controlled by 5A002 or “software” controlled by 5D002.a or 5D002.c.

B. TEST, INSPECTION AND PRODUCTION EQUIPMENT

5B002 “Information Security” test, inspection and “production” equipment, as follows (see List of Items Controlled).

License Requirements

Reason for Control: NS, AT

<i>Control(s)</i>	<i>Country Chart</i>
NS applies to entire entry	NS Column 1
AT applies to entire entry	AT Column 1

License Exceptions

C. MATERIALS - [RESERVED]

D. SOFTWARE

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

License Requirements

Reason for Control: NS, AT, EI

<i>Control(s)</i>	<i>Country Chart</i>
NS applies to entire entry	NS Column 1
AT applies to entire entry	AT Column 1
EI applies to “software” in 5D002.a or c.1 for	

equipment controlled for EI reasons in ECCN 5A002. Refer to §742.15 of the EAR.

Note: Encryption software is controlled because of its functional capacity, and not because of any informational value of such software; such software is not accorded the same treatment under the EAR as other “software”; and for export licensing purposes, encryption software is treated under the EAR in the same manner as a commodity included in ECCN 5A002.

Note: Encryption software controlled for “EI” reasons under this entry remains subject to the EAR even when made publicly available in accordance with part 734 of the EAR. See §740.13(e) of the EAR for information on releasing certain source code (and corresponding object code) which would be considered publicly available from “EI” controls.

License Exceptions

- CIV: N/A
- TSR: N/A
- ENC: Yes for certain EI controlled software, see §740.17 of the EAR for eligibility.

List of Items Controlled

Unit: \$ value
Related Controls: 1) This entry does not control “software” “required” for the “use” of equipment excluded from control under the Related Controls paragraph or the Technical Notes in ECCN [5A002](#) or “software” providing any of the functions of equipment excluded from control under ECCN [5A002](#). This software is classified as ECCN [5D992](#).
 2) After a review and classification by BIS, mass market encryption software that meet eligibility requirements are released from “EI” and “NS” controls. This software is classified under ECCN [5D992.c](#). See §742.15(b) of the EAR.

Related Definitions: 5D002.a controls “software” designed or modified to use “cryptography” employing digital or analog techniques to ensure “information security”.

Items:

- a. “Software” specially designed or modified for the “development”, “production” or “use” of equipment controlled by 5A002 or “software” controlled by 5D002.c;
- b. “Software” specially designed or modified to support “technology” controlled by 5E002;
- c. Specific “software” as follows:
 - c.1. “Software” having the characteristics, or performing or simulating the functions of the equipment, controlled by 5A002;
 - c.2. “Software” to certify “software” controlled by 5D002.c.1.

5D992 “Information Security” “software” not controlled by 5D002.

License Requirements

Reason for Control: AT

<i>Control(s)</i>	<i>Country Chart</i>
AT applies to entire entry	AT Column 1

License Exceptions

- CIV: N/A
- TSR: N/A

List of Items Controlled

Unit: \$ value
Related Controls: This entry does not control “software” designed or modified to protect against malicious computer damage, e.g.,

viruses, where the use of “cryptography” is limited to authentication, digital signature and/or the decryption of data or files.

Related Definitions: N/A

Items:

- a. “Software” specially designed or modified for the “development,” “production,” or “use” of equipment controlled by ECCN [5A992.a](#) or [5A992.b](#).
- b. “Software” having the characteristics, or performing or simulating the functions of the equipment controlled by ECCN [5A992.a](#) or [5A992.b](#).
- c. “Software” that has been reviewed and determined to be mass market encryption software in accordance with §742.15(b) of the EAR.

E. TECHNOLOGY

5E002 “Technology” according to the General Technology Note for the “development,” “production” or “use” of equipment controlled by 5A002 or 5B002 or “software” controlled by 5D002.a or 5D002.c.

License Requirements

Reason for Control: NS, AT, EI

<i>Control(s)</i>	<i>Country Chart</i>
NS applies to entire entry	NS Column 1
AT applies to entire entry	AT Column 1

EI applies to “technology” for the “development,” “production,” or “use” of commodities or “software” controlled for EI reasons in ECCNs 5A002 or 5D002.a or 5D002.c. Refer to § 742.15 of the EAR.

License Requirement Note: *When a person performs or provides technical assistance that incorporates, or otherwise draws upon, “technology” that was either obtained in the United States or is of US-origin, then a release of the “technology” takes place. Such technical assistance, when rendered with the intent to aid in the “development” or “production” of encryption commodities or software that would be controlled for “EI” reasons under ECCN 5A002 or 5D002.a or 5D002.c, may require authorization under the EAR even if the underlying encryption algorithm to be implemented is from the public domain or is not of U.S. origin.*

License Exceptions

- CIV: N/A
- TSR: N/A
- ENC: Yes for certain EI controlled technology, see §740.17 of the EAR for eligibility.

List of Items Controlled

Unit: N/A
Related Controls: 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](#).
Related Definitions: N/A
Items:

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

5E992 "Information Security" "technology" according to the General Technology Note, not controlled by 5E002.

License Requirements

Related Definitions: N/A

Items:

Reason for Control: AT

Control(s)

Country Chart

AT applies to entire entry

AT Column 1

a. “Technology” n.e.s., for the “development”, “production” or “use” of equipment controlled by [5A992.a](#), “information security” or cryptologic equipment controlled by [5A992.b](#) or “software” controlled by [5D992.a or b](#).

License Exceptions

CIV: N/A

TSR: N/A

b. “Technology”, n.e.s., for the “use” of mass market commodities controlled by [5A992.c](#) or mass market “software” controlled by [5D992.c](#).

List of Items Controlled

Unit: N/A

Related Controls: N/A

EAR99 Items subject to the EAR that are *not* elsewhere specified in this CCL Category *or* in any other category in the CCL are designated by the number **EAR99**.