

Part 2-"Information Security"

Notes:

1. The 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. (L.N. 226 of 2009; L.N. 45 of 2010)
2. Category 5-Part 2 does not apply to products when accompanying their user for the user's personal use. (L.N. 45 of 2010)
3. Cryptography Note:
 - 5A002 and 5D002 do not apply to items that meet all of the following: (L.N. 45 of 2010)
 - (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 transaction;
 - (3) Electronic transactions; or
 - (4) Telephone call transactions;
 - (b) The cryptographic functionality cannot easily be changed by the user;
 - (c) Designed for installation by the user without further substantial support by the supplier; and (L.N. 132 of 2001)
 - (d) Deleted; (L.N. 132 of 2001)
 - (e) 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) to (c) above. (L.N. 132 of 2001)
4. Category 5-Part 2 does not apply to items incorporating or using "cryptography" and meeting all of the following:
 - (a) The primary function or set of functions is not any of the following:
 - (1) "Information security";
 - (2) A computer, including operating systems, parts and components of the computer;
 - (3) Sending, receiving or storing information (except in support of entertainment, mass commercial broadcasts, digital rights management or medical records management);
 - (4) Networking (includes operation, administration, management and provisioning);
 - (b) The cryptographic functionality is limited to supporting their primary function or set of functions;

(c) 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) and (b) above.

(L.N. 45 of 2010)

Technical Note:

In Category 5-Part 2, parity bits are not included in the key length.

5A2 SYSTEMS, EQUIPMENT AND COMPONENTS

5A002 "Information security" systems, their equipment and components, as follows:

(a) Systems, equipment, application specific "electronic assemblies", modules and integrated circuits for "information security", as follows, and their components specially designed for "information security":

N.B.:

For Global Navigation Satellite Systems (GNSS) receiving equipment containing or employing decryption, see 7A005.

(L.N. 45 of 2010)

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

Technical Notes:

1. Authentication and digital signature functions include their associated key management function.
2. Authentication includes all aspects of access control where there is no encryption of files or text except as directly related to the protection of passwords, Personal Identification Numbers (PINs) or similar data to prevent unauthorized access.
3. "Cryptography" does not include "fixed" data compression or coding techniques.

Note:

5A002(a)(1) includes equipment designed or modified to use "cryptography" employing

analogue principles when implemented with digital techniques.

(a) A "symmetric algorithm" employing a key length in excess of 56 bits; or

(b) An "asymmetric algorithm" where the security of the algorithm is based on any of the following:

- (1) Factorization of integers in excess of 512 bits (e.g., RSA);
- (2) Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g., Diffie-Hellman over $\mathbb{Z}/p\mathbb{Z}$); or
- (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);

(2) Designed or modified to perform cryptanalytic functions;

(3) Deleted;

(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;

(5) Designed or modified to use cryptographic techniques to generate the spreading code for "spread spectrum" systems not controlled by 5A002(a)(6), including the hopping code for "frequency hopping" systems; (L.N. 132 of 2001; L.N. 95 of 2006)

(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 characteristics:

- (a) A bandwidth exceeding 500 MHz; or
 - (b) A "fractional bandwidth" of 20% or more;
- (L.N. 95 of 2006)

(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; (L.N. 226 of 2009)

(8) Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion; (L.N. 65 of 2004)

(9) Designed or modified to use "quantum cryptography";

Technical Note:

"Quantum cryptography" is also known as quantum key distribution (QKD). (L.N. 95 of 2006)

Note:

5A002 does not include any of the following: (L.N. 254 of 2008)

(a) Smart cards and smart card 'readers/writers' as follows:

(1) A smart card or an electronically readable personal document (e.g., token coin, e-passport) that meets any of the following:

(a) The cryptographic capability is restricted for use in equipment or systems excluded from 5A002 by Note 4 in Category 5, Part 2 or paragraphs (d), (e), (f), (g) and (i) of this Note, and cannot be reprogrammed for any other use;

(b) Having all of the following:

(1) It is specially designed and limited to allow protection of 'personal data' stored within;

(2) Has been, or can only

be, personalized for public or commercial transactions or individual identification;

(3) Where the cryptographic capability is not user-accessible;

Technical Note:

'Personal data' includes any data specific to a particular person or entity, such as the amount of money stored and data necessary for authentication.

(2) 'Readers/writers' specially designed or modified, and limited, for items specified by (a)(1) of this Note;

Technical Note:

'Readers/writers' include equipment that communicates with smart cards or electronically readable documents through a network. (L.N. 45 of 2010)

(b) Deleted; (L.N. 45 of 2010)

(c) Deleted; (L.N. 45 of 2010)

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

Technical Note:

"Money transactions" in 5A002 Note (d) 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 radiocommunications 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)); (L.N. 254 of 2008)

(f) Cordless telephone equipment not capable of end-to-end encryption where the maximum effective range of unboosted cordless operation (i.e. a single, unrelayed hop between terminal and home basestation) is less than 400 metres according to the manufacturer's specifications; (L.N. 254 of 2008)

(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 (e) 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; (L.N. 254 of 2008; L.N. 226 of 2009)

(h) Deleted; (L.N. 45 of 2010)

(i) Wireless "personal area network" equipment that implement only published or commercial cryptographic standards, where the cryptographic capability is limited to a nominal operating range not exceeding 30 metres according to the manufacturer's specifications. (L.N. 226 of 2009)

5B2 TEST, INSPECTION AND PRODUCTION EQUIPMENT (L.N. 65 of 2004)

5B002 "Information security" test, inspection and "production" equipment, as follows:

- (a) Equipment specially designed for the "development" or "production" of equipment specified in 5A002 or 5B002(b);
- (b) Measuring equipment specially designed to evaluate and validate the "information security" functions of the equipment specified in 5A002 or "software" specified in 5D002(a) or 5D002(c);

(L.N. 226 of 2009)

5C2 MATERIALS

None;

5D2 SOFTWARE

5D002 (a) "Software" specially designed or modified for the "development", "production" or "use" of equipment specified in 5A002 or "software" specified in 5D002(c);

(b) "Software" specially designed or modified to support "technology" specified in 5E002;

(c) Specific "software", as follows:

(1) "Software" having the characteristics, or performing or simulating the functions of the equipment, specified in 5A002;

(2) "Software" to certify "software" specified in 5D002(c)(1);

Note:

5D002 does not control:

(a) "Software" required for the "use" of equipment excluded from control under the Note to 5A002;

(b) "Software" providing any of the functions of equipment excluded from control under the Note to 5A002.

(L.N. 226 of 2009)

5E2 TECHNOLOGY

5E002 (a) "Technology" according to the General Technology Note for the "development", "production" or "use" of equipment specified in 5A002 or 5B002 or "software" specified in 5D002(a) or 5D002(c);

(L.N. 183 of 1999; L.N. 226 of 2009)