Part 2—“Information Security”

Notes:

1. The status of “information security” items or functions is determined in Category 5, Part 2 even if they are components, “software” or functions of other systems or equipment. *(L.N. 42 of 2017)*

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 as follows:
   (a) Items meeting all of the following:
       (1) Generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of the following:
           (a) Over-the-counter transactions;
           (b) Mail order transactions;
           (c) Electronic transactions;
           (d) Telephone call transactions;
       (2) The cryptographic functionality cannot easily be changed by the user;
       (3) Designed for installation by the user without further substantial support by the supplier;
       (4) Deleted;
       (5) 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 paragraph (a)(1), (2) and (3) above;
   (b) Hardware components, or ‘executable software’, of existing items described in paragraph (a) of this Note, that have been designed for these existing items, meeting all of the following: *(L.N. 27 of 2015)*
       (1) “Information security” is not the primary function or set of functions of the component or ‘executable software’;
       (2) The component or ‘executable software’ does not change any cryptographic functionality of the
existing items, or add new cryptographic functionality to the existing items;

(3) The feature set of the component or ‘executable software’ is fixed and is not designed or modified to customer specification;

(4) When necessary as determined by the appropriate authority in the exporter’s country, details of the component or ‘executable software’ and relevant end-items are accessible and will be provided to the authority upon request, in order to ascertain compliance with conditions described in paragraph (b)(1), (2) and (3) above. (L.N. 27 of 2015)

**Technical Note:**

For the purposes of the Cryptography Note, ‘executable software’ means “software” in executable form, from an existing hardware component excluded from 5A002 by the Cryptography Note. (L.N. 27 of 2015)

**Note:**

‘Executable software’ does not include complete binary images of the “software” running on an end-item. (L.N. 27 of 2015)

**Note to the Cryptography Note:**

1. To meet paragraph (a) of Note 3, all of the following must apply:
   (a) The item is of potential interest to a wide range of individuals and businesses;
   (b) The price and information about the main functionality of the item are available before purchase without the need to consult the vendor or supplier.

2. In determining paragraph (a) of Note 3, national authorities may take into account relevant factors such as quantity, price, required technical skill, existing sales channels, typical customers, typical use or any exclusionary practices of the supplier. (L.N. 89 of 2013)

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 Notes:
(Repealed L.N. 27 of 2015)

5A2 SYSTEMS, EQUIPMENT AND COMPONENTS

5A002 “Information security” systems, their equipment and components, as follows:
   (a) Systems, equipment and components, for “information security”, as follows: (L.N. 42 of 2017)

   N.B.:
   For Global Navigation Satellite Systems (GNSS) receiving equipment containing or employing decryption, see 7A005, and for related decryption “software” and “technology”, see 7D005 and 7E001. (L.N. 45 of 2010; L.N. 42 of 2017)
   (1) Designed or modified to use “cryptography” employing digital techniques performing any cryptographic function other than authentication, digital signature or the execution of copy-protected “software”, and having any of the following: (L.N. 89 of 2013)
Technical Notes:
1. Functions for authentication, digital signature and the execution of copy-protected “software” include their associated key management function. (L.N. 89 of 2013)
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. (Repealed L.N. 27 of 2015)
   Note:
   (Repealed L.N. 27 of 2015)
   (a) A “symmetric algorithm” employing a key length in excess of 56 bits; or
   Technical Note:
   In Category 5, Part 2, parity bits are not included in the key length. (L.N. 27 of 2015)
   (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’; (L.N. 42 of 2017)
   Note:
   5A002(a)(2) includes systems or equipment, designed or modified to perform ‘cryptanalytic functions’ by means of reverse engineering. (L.N. 89
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. (L.N. 42 of 2017)

(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 that have been evaluated and certified by a national authority to exceed class EAL-6 (evaluation assurance level) of the Common Criteria (CC) or equivalent; (L.N. 89 of 2013)

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

Note:
5A002(a)(8) applies to physical layer security only. (L.N. 89 of 2013)

(9) Designed or modified to use or perform “quantum cryptography”; (L.N. 27 of 2015)

(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; (L.N. 161 of 2011; L.N. 42 of 2017)

Note:
5A002 does not include any of the following:

(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 paragraph (a)(1) of this Note;
Technical Note:
‘Readers/writers’ include equipment that communicates with smart cards or electronically readable documents through a network.

(b) Deleted;
(c) Deleted;
(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));

(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;

(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 paragraph (a)(2), (3), (4) and (5) 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. 89 of 2013)

(h) Deleted;

(i) Wireless “personal area network” equipment that implements 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, or not exceeding 100 metres according to the manufacturer's specifications for equipment that cannot interconnect with more than 7 devices; (L.N. 89 of 2013)

(j) Equipment, having no functionality specified by 5A002(a)(2), 5A002(a)(4), 5A002(a)(7), 5A002(a)(8) or 5A002(b) and meeting all of the following descriptions: (L.N. 42 of 2017)

(1) All cryptographic capability specified in 5A002(a) of the equipment:
   (a) Cannot be used; or
   (b) Can only be made useable by means of “cryptographic activation”;

(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 on request, in order to ascertain compliance with the conditions described above; (L.N. 42 of 2017)

N.B.: (L.N. 42 of 2017)

1. See 5A002(a) for equipment that has undergone “cryptographic activation”. (L.N. 42 of 2017)

2. See also 5A002(b), 5D002(d) and 5E002(b). (L.N. 42 of 2017)

(k) Mobile telecommunications Radio Access Network (RAN) equipment designed for civil use, which also meets the provisions of paragraph (a)(2) to (5) of the Cryptography Note (Note 3 in Category 5, Part 2), having an RF output power limited to 0.1 W (20 dBm) or less, and supporting 16 or fewer concurrent users; (L.N. 27 of 2015)

(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; (L.N. 42 of 2017)

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

(1) Uses only published or commercial cryptographic standards;

(2) Meets any of the following descriptions:

(a) Is integral to a CPU that meets the provisions of Note 3 in Category 5, Part 2;

(b) Is integral to an operating system that is not controlled by 5D002;

(c) Is limited to “OAM” of the equipment; (L.N. 42 of 2017)

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(c) does not apply to “software” limited to the tasks of “OAM” implementing only published or commercial cryptographic standards. (L.N. 42 of 2017)

(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; (L.N. 42 of 2017)

5E2 TECHNOLOGY

5E002 “Technology” as follows:

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

(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; (L.N. 42 of 2017)

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. (L.N. 89 of 2013)

(L.N. 161 of 2011)