Part 2—"Information Security"

Notes:

1. *(Repealed L.N. 89 of 2021)*

2. Category 5—Part 2 does not apply to products when accompanying their user for the user's personal use.

3. *Cryptography Note:*

   5A002, 5D002(a)(1), 5D002(b) and 5D002(c)(1) do not apply to items as follows: *(L.N. 89 of 2021)*

   (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. A simple price enquiry is not considered to be a consultation. *(L.N. 89 of 2021)*
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. *(Repealed L.N. 89 of 2021)*

(L.N. 45 of 2010)

Technical Notes:

(Repealed L.N. 27 of 2015)

5A2 SYSTEMS, EQUIPMENT AND COMPONENTS

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

N.B.:

For "satellite navigation system" receiving equipment containing or employing decryption, see 7A005, and for related decryption "software" and "technology", see 7D005 and 7E001.

(a) Designed or modified to use 'cryptography for data confidentiality' having a 'described security algorithm', where that cryptographic capability is usable, has been activated, or can be activated by means of "cryptographic activation" not employing a secure mechanism, as follows:
   (1) Items having "information security" as a primary function;
   (2) Digital communication or networking systems, equipment or components, not specified in 5A002(a)(1);
   (3) Computers, other items having information storage or processing as a primary function, and components of those items, not specified in 5A002(a)(1) or 5A002(a)(2);

   N.B.:

   For operating systems, see also 5D002(a)(1) and 5D002(c)(1).
   (4) Items, not specified in 5A002(a)(1), 5A002(a)(2) and 5A002(a)(3), where the 'cryptography for data confidentiality' having a 'described security algorithm' meets all of the following:
      (a) It supports a non-primary function of the item;
      (b) It is performed by incorporated equipment or "software" that would, as a stand-alone item, be specified in Category 5—Part 2;

Technical Notes:

1. For the purposes of 5A002(a), 'cryptography for data confidentiality' means "cryptography" that employs digital techniques and performs any cryptographic function other than any of the following:
   (a) "Authentication";
   (b) Digital signature;

(c) Data integrity;

(d) Non-repudiation;

(e) Digital rights management, including the execution of copy-protected "software";

(f) Encryption or decryption in support of entertainment, mass commercial broadcasts or medical records management;

(g) Key management in support of any function described in paragraphs (a) to (f) of this Note.

2. For the purposes of 5A002(a), 'described security algorithm' means any of the following:

(a) A "symmetric algorithm" employing a key length in excess of 56 bits, not including parity bits;

(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 Z/pZ);

(3) Discrete logarithms in a group other than mentioned in paragraph (b)(2) of this Note in excess of 112 bits (e.g. Diffie-Hellman over an elliptic curve);

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

(1) Shortest vector or closest vector problems associated with lattices (e.g. NewHope, Frodo, NTRUEncrypt, Kyber, Titanium);

(2) Finding isogenies between Supersingular elliptic curves (e.g. Supersingular Isogeny Key Encapsulation);

(3) Decoding random codes (e.g. McEliece, Niederreiter).

Technical Note:

An algorithm described by Technical Note 2(c) may be referred to as being post-quantum, quantum-safe or quantum-resistant.

Notes:

1. When necessary as determined by the appropriate authority in the exporter's country, details of items must be accessible and provided to the authority on request, in order to establish any of the following:

(a) Whether the item meets the criteria of 5A002(a)(1) to 5A002(a)(4);

(b) Whether the cryptographic capability for data confidentiality specified in 5A002(a) is usable without "cryptographic activation".

2. 5A002(a) does not control any of the following items, or specially designed "information security" components of those items:

(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 meets all of the following:

(1) It is restricted for use in any of the following:

(a) Equipment or systems not described by 5A002(a)(1) to 5A002(a)(4);

(b) Equipment or systems not using 'cryptography for data confidentiality' having a 'described security algorithm';

(c) Equipment or systems, excluded from 5A002(a), by paragraphs (b) to (f) of this Note;

(2) It 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 in 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) Cryptographic equipment specially designed and limited for banking use or 'money transactions';

Technical Note:

'Money transactions' in 5A002(a) Note 2(b) includes the collection and settlement of fares or credit functions.

(c) 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));

(d) 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 base station) is less than 400 metres according to the manufacturer's specifications;

(e) 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 (a)(2) to (4) 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;

(f) Items, where the "information security" functionality is limited to wireless "personal area network" functionality, meeting all of the following:

(1) Implement only published or commercial cryptographic standards;

(2) 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;

(g) Mobile telecommunications Radio Access Network (RAN) equipment designed for civil use, which also meet the provisions of paragraphs (a)(2) to (4) 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;

(h) 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;

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

(1) Uses only published or commercial cryptographic standards;

(2) Is any of the following:

(a) Integral to a CPU that meets the provisions of Note 3 in Category 5— Part 2;

(b) Integral to an operating system that is not specified in 5D002;

(c) Limited to "OAM" of the equipment;

(j) Items specially designed for a 'connected civil industry application', meeting all of the following:

(1) Being any of the following:

(a) A network-capable end-point device meeting any of the following:

(1) The "information security" functionality is limited to securing 'non-arbitrary data' or the tasks of "Operations, Administration or Maintenance" ("OAM");

(2) The device is limited to a specific 'connected civil industry application';

(b) Networking equipment meeting all of the following:

(1) Being specially designed to communicate with the devices specified in paragraph (j)(1)(a) of this Note;

(2) The "information security" functionality is limited to supporting the 'connected civil industry application' of devices specified in paragraph (j)(1)(a) of this Note, or the tasks of "OAM" of this networking equipment or of other items specified in paragraph (j) of this Note;

(2) Where the "information security" functionality implements only published or commercial cryptographic standards, and the cryptographic functionality cannot easily be changed by the user.

Technical Notes:

1. 'Connected civil industry application' means a network-connected consumer or civil industry application other than "information security", digital communication, general purpose networking or computing.

2. 'Non-arbitrary data' means sensor or metering data directly related to the stability, performance or physical measurement of a system (e.g.

temperature, pressure, flow rate, mass, volume, voltage, physical location, etc.), that cannot be changed by the user of the device.

(b) Being a 'cryptographic activation token';

Technical Note:

A 'cryptographic activation token' is an item designed or modified for any of the following:

(a) Converting, by means of "cryptographic activation", an item not specified in Category 5—Part 2 into an item specified in 5A002(a) or 5D002(c)(1), and not released by the Cryptography Note (Note 3 in Category 5—Part 2);

(b) Enabling, by means of "cryptographic activation", additional functionality specified in 5A002(a) of an item already specified in Category 5—Part 2.

(c) Designed or modified to use or perform "quantum cryptography";

Technical Note:

"Quantum cryptography" is also known as Quantum Key Distribution (QKD).

(d) 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:

(1) A bandwidth exceeding 500 MHz;

(2) A "fractional bandwidth" of 20% or more;

(e) Designed or modified to use cryptographic techniques to generate the spreading code for "spread spectrum" systems, other than those specified in 5A002(d), including the hopping code for "frequency hopping" systems;

(L.N. 89 of 2021)

5A003 Systems, equipment and components, for non-cryptographic "information security", as follows:

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

Note:

5A003(a) only controls physical layer security. For the purposes of 5A003(a), the physical layer includes Layer 1 of the Reference Model of Open Systems Interconnection (OSI) (ISO/IEC 7498-1).

(b) Specially designed or modified to reduce the compromising emanations of information-bearing signals beyond what is necessary for health, safety or electromagnetic interference standards;

(L.N. 89 of 2021)

5A004 Systems, equipment and components, for defeating, weakening or by-passing "information security", as follows:

(a) Designed or modified to perform 'cryptanalytic functions';

Note:

5A004(a) 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.

(L.N. 89 of 2021)

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, 5A003, 5A004 or 5B002(b);

(b) Measuring equipment specially designed to evaluate and validate the "information security" functions of the equipment specified in 5A002, 5A003 or 5A004, or of "software" specified in 5D002(a) or 5D002(c);

(L.N. 226 of 2009; L.N. 89 of 2021)

5C2 MATERIALS

None;

5D2 SOFTWARE

5D002 (a) "Software" specially designed or modified for the "development", "production" or "use" of any of the following:

(1) Equipment specified in 5A002 or "software" specified in 5D002(c)(1);

(2) Equipment specified in 5A003 or "software" specified in 5D002(c)(2);

(3) Equipment specified in 5A004 or "software" specified in 5D002(c)(3); *(L.N. 89 of 2021)*

(b) "Software" having the characteristics of a 'cryptographic activation token' specified in 5A002(b); *(L.N. 89 of 2021)*

(c) "Software" having the characteristics of, or performing or simulating the functions of, any of the following:

(1) Equipment specified in 5A002(a), 5A002(c), 5A002(d) or 5A002(e);

Note:

5D002(c)(1) does not control "software" limited to the tasks of "OAM" implementing only published or commercial cryptographic standards.

(2) Equipment specified in 5A003;

(3) Equipment specified in 5A004; *(L.N. 89 of 2021)*

(d) *(Repealed L.N. 89 of 2021)*

(L.N. 226 of 2009; L.N. 89 of 2013)

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, 5A003, 5A004 or 5B002, or of "software" specified by 5D002(a) or 5D002(c); *(L.N. 89 of 2021)*

(b) "Technology" having the characteristics of a 'cryptographic activation token' specified in 5A002(b); *(L.N. 89 of 2021)*

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)