Council of the European Union

Brussels, 8 October 2020
(OR. en)

11646/20
ADD 7

COMER 119
CONOP 65
CFSP/PESC 820
ECO 38
UD 262
ATO 54
COARM 165
DELACT 127

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	7 October 2020
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	C(2020) 6784 final - ANNEX 1 Part 7/11
Subject:	ANNEX 1 Part 7/11 to the Commission Delegated Regulation amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items

Delegations will find attached document C(2020) 6784 final - ANNEX 1 Part 7/11.

Encl.: C(2020) 6784 final - ANNEX 1 Part 7/11

EUROPEAN
COMMISSION

Brussels, 7.10.2020
C(2020) 6784 final

ANNEX 1 – PART 7/11

ANNEX

to the

Commission Delegated Regulation

amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items

ANNEX I (PART VII – Category 5)

CATEGORY 5 - TELECOMMUNICATIONS AND "INFORMATION SECURITY"

Part 1 - TELECOMMUNICATIONS

Note 1: *The control status of components, test and "production" equipment and "software" therefor which are specially designed for telecommunications equipment or systems is determined in Category 5, Part 1.*

N.B. *For "lasers" specially designed for telecommunications equipment or systems, see 6A005.*

Note 2: *"Digital computers", related equipment or "software", when essential for the operation and support of telecommunications equipment described in this Category, are regarded as specially designed components, provided they are the standard models customarily supplied by the manufacturer. This includes operation, administration, maintenance, engineering or billing computer systems.*

5A1 Systems, Equipment and Components

5A001 Telecommunications systems, equipment, components and accessories as follows:

a. Any type of telecommunications equipment having any of the following characteristics, functions or features:

1. Specially designed to withstand transitory electronic effects or electromagnetic pulse effects, both arising from a nuclear explosion;

2. Specially hardened to withstand gamma, neutron or ion radiation;

3. Specially designed to operate below 218 K (-55°C); or

4. Specially designed to operate above 397 K (124°C);

Note 1: *5A001.a.3. and 5A001.a.4. control only electronic equipment.*

Note 2: *5A001.a.2., 5A001.a.3. and 5A001.a.4. do not control equipment designed or modified for use on board satellites.*

5A001 continued

b. Telecommunication systems and equipment, and specially designed components and accessories therefor, having any of the following characteristics, functions or features:

1. Being underwater untethered communications systems having any of the following:

a. An acoustic carrier frequency outside the range from 20 kHz to 60 kHz;

b. Using an electromagnetic carrier frequency below 30 kHz;

c. Using electronic beam steering techniques; or

d. Using "lasers" or light-emitting diodes (LEDs) with an output wavelength greater than 400 nm and less than 700 nm, in a "local area network";

2. Being radio equipment operating in the 1,5 MHz to 87,5 MHz band and having all of the following:

a. Automatically predicting and selecting frequencies and "total digital transfer rates" per channel to optimise the transmission; and

b. Incorporating a linear power amplifier configuration having a capability to support multiple signals simultaneously at an output power of 1 kW or more in the frequency range of 1,5 MHz or more but less than 30 MHz, or 250 W or more in the frequency range of 30 MHz or more but not exceeding 87,5 MHz, over an "instantaneous bandwidth" of one octave or more and with an output harmonic and distortion content of better than -80 dB;

5A001.b. continued

3. Being radio equipment employing "spread spectrum" techniques, including "frequency hopping" techniques, other than those specified in 5A001.b.4. and having any of the following:

   a. User programmable spreading codes; or

   b. A total transmitted bandwidth which is 100 or more times the bandwidth of any one information channel and in excess of 50 kHz;

      Note: 5A001.b.3.b. does not control radio equipment specially designed for use with any of the following:
      a. Civil cellular radio-communications systems; or
      b. Fixed or mobile satellite earth stations for commercial civil telecommunications.

   Note: 5A001.b.3 does not control equipment designed to operate at an output power of 1 W or less.

4. Being radio equipment employing ultra-wideband modulation techniques, having user programmable channelising codes, scrambling codes or network identification codes and having any of the following:

   a. A bandwidth exceeding 500 MHz; or

   b. A "fractional bandwidth" of 20% or more;

5. Being digitally controlled radio receivers having all of the following:

   a. More than 1 000 channels;

   b. A 'channel switching time' of less than 1 ms;

   c. Automatic searching or scanning of a part of the electromagnetic spectrum; and

   d. Identification of the received signals or the type of transmitter; or

   Note: 5A001.b.5. does not control radio equipment specially designed for use with civil cellular radio-communications systems.

   Technical Note:
   'Channel switching time' means the time (i.e., delay) to change from one receiving frequency to another, to arrive at or within ±0,05% of the final specified receiving frequency. Items having a specified frequency range of less than ±0,05% around their centre frequency are defined to be incapable of channel frequency switching.

5A001.b. continued

6. Employing functions of digital "signal processing" to provide 'voice coding' output at rates of less than 700 bit/s.

Technical Notes:

1. For variable rate 'voice coding', 5A001.b.6. applies to the 'voice coding' output of continuous speech.

2. For the purposes of 5A001.b.6., 'voice coding' is defined as the technique to take samples of human voice and then convert these samples into a digital signal, taking into account specific characteristics of human speech.

c. Optical fibres of more than 500 m in length and specified by the manufacturer as being capable of withstanding a 'proof test' tensile stress of 2×10^9 N/m^2 or more;

N.B. For underwater *umbilical cables, see 8A002.a.3.*

Technical Note:

'Proof Test': on-line or off-line production screen testing that dynamically applies a prescribed tensile stress over a 0,5 to 3 m length of fibre at a running rate of 2 to 5 m/s while passing between capstans approximately 150 mm in diameter. The ambient temperature is a nominal 293 K (20ºC) and relative humidity 40%. Equivalent national standards may be used for executing the proof test.

d. 'Electronically steerable phased array antennae' as follows:

1. Rated for operation above 31,8 GHz, but not exceeding 57 GHz, and having an Effective Radiated Power (ERP) equal to or greater than +20 dBm (22,15 dBm Effective Isotropic Radiated Power (EIRP));

2. Rated for operation above 57 GHz, but not exceeding 66 GHz, and having an ERP equal to or greater than +24 dBm (26,15 dBm EIRP);

3. Rated for operation above 66 GHz, but not exceeding 90 GHz, and having an ERP equal to or greater than +20 dBm (22,15 dBm EIRP);

4. Rated for operation above 90 GHz;

Note 1: *5A001.d. does not control 'electronically steerable phased array antennae' for landing systems with instruments meeting ICAO standards covering Microwave Landing Systems (MLS).*

Note 2: *5A001.d. does not control antennae specially designed for any of the following:*

a. Civil cellular or WLAN radio-communications systems;

b. IEEE 802.15 or wireless HDMI; or

c. Fixed or mobile satellite earth stations for commercial civil telecommunications.

Technical Note:

For the purposes of 5A001.d. 'electronically steerable phased array antenna' is an antenna which forms a beam by means of phase coupling, (i.e., the beam direction is controlled by the complex excitation coefficients of the radiating elements) and the direction of that beam can be varied (both in transmission and reception) in azimuth or in elevation, or both, by application of an electrical signal.

e. Radio direction finding equipment operating at frequencies above 30 MHz and having all of the following, and specially designed components therefor:

1. "Instantaneous bandwidth" of 10 MHz or more; and

2. Capable of finding a Line Of Bearing (LOB) to non-cooperating radio transmitters with a signal duration of less than 1 ms;

f Mobile telecommunications interception or jamming equipment, and monitoring equipment therefor, as follows, and specially designed components therefor:

1. Interception equipment designed for the extraction of voice or data, transmitted over the air interface;

2. Interception equipment not specified in 5A001.f.1., designed for the extraction of client device or subscriber identifiers (e.g., IMSI, TIMSI or IMEI), signalling, or other metadata transmitted over the air interface;

3. Jamming equipment specially designed or modified to intentionally and selectively interfere with, deny, inhibit, degrade or seduce mobile telecommunication services and performing any of the following:

a. Simulate the functions of Radio Access Network (RAN) equipment;

b. Detect and exploit specific characteristics of the mobile telecommunications protocol employed (e.g., GSM); or

c. Exploit specific characteristics of the mobile telecommunications protocol employed (e.g. GSM);

4. RF monitoring equipment designed or modified to identify the operation of items specified in 5A001.f.1., 5A001.f.2. or 5A001.f.3.;

Note: 5A001.f.1. and 5A001.f.2. do not control any of the following:

a. Equipment specially designed for the interception of analogue Private Mobile Radio (PMR), IEEE 802.11 WLAN;

b. Equipment designed for mobile telecommunications network operators; or

c. Equipment designed for the "development" or "production" of mobile telecommunications equipment or systems.

N.B.1. SEE ALSO MILITARY GOODS CONTROLS.

N.B.2. For radio receivers see 5A001.b.5.

g. Passive Coherent Location (PCL) systems or equipment, specially designed for detecting and tracking moving objects by measuring reflections of ambient radio frequency emissions, supplied by non-radar transmitters;

Technical Note:
Non-radar transmitters may include commercial radio, television or cellular telecommunications base stations.

Note: 5A001.g. does not control any of the following:
a. Radio-astronomical equipment; or
b. Systems or equipment, that require any radio transmission from the target.

h. Counter Improvised Explosive Device (IED) equipment and related equipment, as follows:

1. Radio Frequency (RF) transmitting equipment, not specified in 5A001.f., designed or modified for prematurely activating or preventing the initiation of Improvised Explosive Devices (IEDs);

2. Equipment using techniques designed to enable radio communications in the same frequency channels on which co-located equipment specified in 5A001.h.1. is transmitting;

N.B. SEE ALSO MILITARY GOODS CONTROLS.

i. Not used;

j. Internet Protocol (IP) network communications surveillance systems or equipment, and specially designed components therefor, having all of the following:

1. Performing all of the following on a carrier class Internet Protocol (IP) network (e.g., national grade IP backbone):

a. Analysis at the application layer (e.g., Layer 7 of Open Systems Interconnection (OSI) model (ISO/IEC 7498-1));

b. Extraction of selected metadata and application content (e.g., voice, video, messages, attachments); and

c. Indexing of extracted data; and

5A001.j. continued

2. Being specially designed to carry out all of the following:

a. Execution of searches on the basis of "hard selectors"; and

b. Mapping of the relational network of an individual or of a group of people.

Note: 5A001.j. does not control systems or equipment, specially designed for any of the following:

a. Marketing purpose;

b. Network Quality of Service (QoS); or

c. Quality of Experience (QoE).

5A101 Telemetry and telecontrol equipment, including ground equipment, designed or modified for 'missiles'.

Technical Note:

In 5A101 'missile' means complete rocket systems and unmanned aerial vehicle systems capable of a range exceeding 300 km.

Note: 5A101 does not control:

a. Equipment designed or modified for manned aircraft or satellites;

b. Ground based equipment designed or modified for terrestrial or marine applications;

c. Equipment designed for commercial, civil or 'Safety of Life' (e.g., data integrity, flight safety) GNSS services;

5B1 Test, Inspection and Production Equipment

5B001 Telecommunications test, inspection and production equipment, components and accessories, as follows:

a. Equipment and specially designed components or accessories therefor, specially designed for the "development" or "production" of equipment, functions or features, specified in 5A001;

Note: 5B001.a. does not control optical fibre characterization equipment.

b. Equipment and specially designed components or accessories therefor, specially designed for the "development" of any of the following telecommunication transmission or switching equipment:

1. Not used;

2. Equipment employing a "laser" and having any of the following:

a. A transmission wavelength exceeding 1 750 nm; or

b. Not used;

c. Not used;

d. Employing analogue techniques and having a bandwidth exceeding 2,5 GHz; or

Note: 5B001.b.2.d. does not control equipment specially designed for the "development" of commercial TV systems.

5B001.b. continued

3. Not used;

4. Radio equipment employing Quadrature-Amplitude-Modulation (QAM) techniques above level 1 024;

5. Not used.

5C1 Materials

None

5D1 Software

5D001 "Software" as follows:

a. "Software" specially designed or modified for the "development", "production" or "use" of equipment, functions or features, specified in 5A001;

b. Not used;

c. Specific "software" specially designed or modified to provide characteristics, functions or features of equipment, specified in 5A001 or 5B001;

d. "Software" specially designed or modified for the "development" of any of the following telecommunication transmission or switching equipment:

1. Not used;

2. Equipment employing a "laser" and having any of the following:

a. A transmission wavelength exceeding 1 750 nm; or

b. Employing analogue techniques and having a bandwidth exceeding 2,5 GHz; or

Note: 5D001.d.2.b. does not control "software" specially designed or modified for the "development" of commercial TV systems.

3. Not used;

4. Radio equipment employing Quadrature-Amplitude-Modulation (QAM) techniques above level 1 024.

e. "Software", other than that specified in 5D001.a. or 5D001.c., specially designed or modified for monitoring or analysis by law enforcement, providing all of the following:

1. Execution of searches on the basis of "hard selectors" of either the content of communication or metadata acquired from a communications service provider using a 'handover interface'; and

2. Mapping of the relational network or tracking the movement of targeted individuals based on the results of searches on content of communication or metadata or searches as described in 5D001.e.1.

Technical Notes:

1. *For the purposes of 5D001.e., a 'handover interface' is a physical and logical interface, designed for use by an authorised law enforcement authority, across which targeted interception measures are requested from a communications service provider and the results of interception are delivered from a communications service provider to the requesting authority. The 'handover interface' is implemented within systems or equipment (e.g., mediation devices) that receive and validate the interception request, and deliver to the requesting authority only the results of interception that fulfil the validated request.*
2. *'Handover interfaces' may be specified by international standards (including but not limited to ETSI TS 101 331, ETSI TS 101 671, 3GPP TS 33.108) or national equivalents.*

5D001.e. continued

Note: 5D001.e. does not control "software" specially designed or modified for any of the following:

a. Billing purposes;

b. Network Quality of Service (QoS);

c. Quality of Experience (QoE);

d. Mediation devices; or

e. Mobile payment or banking use.

5D101 "Software" specially designed or modified for the "use" of equipment specified in 5A101.

5E1 Technology

5E001 "Technology" as follows:

a. "Technology" according to the General Technology Note for the "development", "production" or "use" (excluding operation) of equipment, functions or features specified in 5A001 or "software" specified in 5D001.a. or 5D001.e.;

b. Specific "technology" as follows:

1. "Technology" "required" for the "development" or "production" of telecommunications equipment specially designed to be used on board satellites;

2. "Technology" for the "development" or "use" of "laser" communication techniques with the capability of automatically acquiring and tracking signals and maintaining communications through exoatmosphere or sub-surface (water) media;

3. "Technology" for the "development" of digital cellular radio base station receiving equipment whose reception capabilities that allow multi-band, multi-channel, multi-mode, multi-coding algorithm or multi-protocol operation can be modified by changes in "software";

4. "Technology" for the "development" of "spread spectrum" techniques, including "frequency hopping" techniques;

Note: 5E001.b.4. does not control "technology" for the "development" of any of the following:

a. Civil cellular radio-communications systems; or

b. Fixed or mobile satellite earth stations for commercial civil telecommunications.

5E001 continued

c. "Technology" according to the General Technology Note for the "development" or "production" of any of the following:

1. Not used;

2. Equipment employing a "laser" and having any of the following:

a. A transmission wavelength exceeding 1 750 nm; or

b. Not used;

c. Not used;

d. Employing wavelength division multiplexing techniques of optical carriers at less than 100 GHz spacing; or

e. Employing analogue techniques and having a bandwidth exceeding 2,5 GHz;

Note: 5E001.c.2.e. does not control "technology" for commercial TV systems.

N.B. For "technology" for the "development" or "production" of non-telecommunications equipment employing a laser, see 6E.

5E001.c. continued

3. Equipment employing "optical switching" and having a switching time less than 1 ms;

4. Radio equipment having any of the following:

a. Quadrature-Amplitude-Modulation (QAM) techniques above level 1 024;

b. Operating at input or output frequencies exceeding 31,8 GHz; or

Note: 5E001.c.4.b. does not control "technology" for equipment designed or modified for operation in any frequency band which is "allocated by the ITU" for radio-communications services, but not for radio-determination.

c. Operating in the 1,5 MHz to 87,5 MHz band and incorporating adaptive techniques providing more than 15 dB suppression of an interfering signal; or

5. Not used;

6. Mobile equipment having all of the following:

a. Operating at an optical wavelength greater than or equal to 200 nm and less than or equal to 400 nm; and

b. Operating as a "local area network";

d. "Technology" according to the General Technology Note for the "development" or "production" of "Monolithic Microwave Integrated Circuit" ("MMIC") amplifiers specially designed for telecommunications and that are any of the following:

Technical Note:
For purposes of 5E001.d., the parameter peak saturated power output may also be referred to on product data sheets as output power, saturated power output, maximum power output, peak power output, or peak envelope power output.

1. Rated for operation at frequencies exceeding 2,7 GHz up to and including 6,8 GHz with a "fractional bandwidth" greater than 15%, and having any of the following:

a. A peak saturated power output greater than 75 W (48,75 dBm) at any frequency exceeding 2,7 GHz up to and including 2,9 GHz;

b. A peak saturated power output greater than 55 W (47,4 dBm) at any frequency exceeding 2,9 GHz up to and including 3,2 GHz;

5E001.d.1. continued

c. A peak saturated power output greater than 40 W (46 dBm) at any frequency exceeding 3,2 GHz up to and including 3,7 GHz; or

d. A peak saturated power output greater than 20 W (43 dBm) at any frequency exceeding 3,7 GHz up to and including 6,8 GHz;

2. Rated for operation at frequencies exceeding 6,8 GHz up to and including 16 GHz with a "fractional bandwidth" greater than 10%, and having any of the following:

a. A peak saturated power output greater than 10W (40 dBm) at any frequency exceeding 6,8 GHz up to and including 8,5 GHz; or

b. A peak saturated power output greater than 5W (37 dBm) at any frequency exceeding 8,5 GHz up to and including 16 GHz;

3. Rated for operation with a peak saturated power output greater than 3 W (34,77 dBm) at any frequency exceeding 16 GHz up to and including 31,8 GHz, and with a "fractional bandwidth" of greater than 10%;

4. Rated for operation with a peak saturated power output greater than 0,1 nW (-70 dBm) at any frequency exceeding 31,8 GHz up to and including 37 GHz;

5. Rated for operation with a peak saturated power output greater than 1 W (30 dBm) at any frequency exceeding 37 GHz up to and including 43,5 GHz, and with a "fractional bandwidth" of greater than 10%;

6. Rated for operation with a peak saturated power output greater than 31,62 mW (15 dBm) at any frequency exceeding 43,5 GHz up to and including 75 GHz, and with a "fractional bandwidth" of greater than 10%;

7. Rated for operation with a peak saturated power output greater than 10 mW (10 dBm) at any frequency exceeding 75 GHz up to and including 90 GHz, and with a "fractional bandwidth" of greater than 5%; or

8. Rated for operation with a peak saturated power output greater than 0,1 nW (-70 dBm) at any frequency exceeding 90 GHz;

5E001 continued

e. "Technology" according to the General Technology Note for the "development" or "production" of electronic devices and circuits, specially designed for telecommunications and containing components manufactured from "superconductive" materials, specially designed for operation at temperatures below the "critical temperature" of at least one of the "superconductive" constituents and having any of the following:

1. Current switching for digital circuits using "superconductive" gates with a product of delay time per gate (in seconds) and power dissipation per gate (in watts) of less than 10^{-14} J; or

2. Frequency selection at all frequencies using resonant circuits with Q-values exceeding 10 000.

5E101 "Technology" according to the General Technology Note for the "development", "production" or "use" of equipment specified in 5A101.

Part 2 - "INFORMATION SECURITY"

Note 1: *Not used.*

Note 2: *Category 5 – Part 2 does not control products when accompanying their user for the user's personal use.*

Note 3: *Cryptography Note*

5A002, 5D002.a.1., 5D002.b. and 5D002.c.1. do not control items as follows:

a. Items that meet 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; or

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; and

4. When necessary, details of the goods are accessible and will be provided, upon request, to the competent authorities of the EU Member State in which the exporter is established in order to ascertain compliance with conditions described in paragraphs 1. to 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:

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; and

4. When necessary as determined by the competent authorities of the EU Member State in which the exporter is established, details of the component or 'executable software' and details of relevant end-items are accessible and will be provided to the competent authority upon request, in order to ascertain compliance with conditions described above.

Technical Note:
For the purpose of the Cryptography Note, 'executable software' means "software" in executable form, from an existing hardware component excluded from 5A002 by the Cryptography Note.

Note: 'Executable software' does not include complete binary images of the "software" running on an end-item.

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; and

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.

2. In determining eligibility of paragraph a. of Note 3, competent 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.

5A2 Systems, Equipment and Components

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

N.B. For the control of "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 any means other than secure "cryptographic activation", 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 therefor, 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. to 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; and

b. It is performed by incorporated equipment or "software" that would, as a standalone item, be specified in Category 5 – Part 2.

5A002.a. continued

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; or

g. Key management in support of any function described in paragraph a. to f. above.

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. Factorisation 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); or

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

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); or

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.

5A002.a. continued

Note 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 upon request, in order to establish any of the following:*

a. Whether the item meets the criteria of 5A002.a.1. to 5A002.a.4.; or

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

Note 2: *5A002.a. does not control any of the following items, or specially designed "information security" components therefor:*

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'; or

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

2. It cannot be reprogrammed for any other use; or:

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, personalised for public or commercial transactions or individual identification; and

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 a.4. of the Cryptography Note (Note 3 in Category 5, Part 2), that have been customised for a specific civil industry application with features that do not affect the cryptographic functionality of these original non-customised devices;

f. Items, where the "information security" functionality is limited to wireless "personal area network" functionality, implementing only published or commercial cryptographic standards;

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

h. Routers, switches, gateways 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

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; 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 in 5D002; or
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 endpoint 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"); or

2. The device is limited to a specific 'connected civil industry application'; or

b. Networking equipment meeting all of the following:

1. Being specially designed to communicate with the devices specified in paragraph j.1.a. above; and

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

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.

5A002 continued

b. Being a 'cryptographic activation token';

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

1. 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); or

2. 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 channelising 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; or

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.

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 purpose 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.

5A004 Systems, equipment and components for defeating, weakening or bypassing "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.

b. Items, not specified in 4A005 or 5A004.a., designed to perform all of the following:

1. 'Extract raw data' from a computing or communications device; and

2. Circumvent "authentication" or authorisation controls of the device, in order to perform the function described in 5A004.b.1.

Technical Note:
'Extract raw data' from a computing or communications device means to retrieve binary data from a storage medium (e.g., RAM, flash or hard disk) of the device without interpretation by the device's operating system or filesystem.

Note1: 5A004.b. does not control systems or equipment specially designed for the "development" or "production" of a computing or communications device.

Note: 5A004.b. does not include:
a. Debuggers, hypervisors;
b. Items limited to logical data extraction;
c. Data extraction items using chip-off or JTAG; or
d. Items specially designed and limited to jail-breaking or rooting.

5B2 Test, Inspection and Production Equipment

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.

5C2 Materials

None.

5D2 Software

5D002 "Software" as follows:

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.; or

3. Equipment or "software", as follows:

a. Equipment specified in 5A004.a. or "software" specified in 5D002.c.3.a.;

b. Equipment specified in 5A004.b. or "software" specified in 5D002.c.3.b.

b. "Software" having the characteristics of a 'cryptographic activation token' specified in 5A002.b.;

5D002 continued

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; or

3. Equipment, as follows:

a. Equipment specified in 5A004.a.;

b. Equipment specified in 5A004.b.

Note: 5D002.c.3.b. does not control "intrusion software".

d. Not used.

5E2 Technology

5E002 "Technology" as follows:

a. "Technology" according to the General Technology Note for the "development", "production" or "use" of equipment specified in 5A002, 5A003, 5A004 or 5B002, or of "software" specified in 5D002.a. or 5D002.c.

Note: 5E002.a. does not control "technology" for items specified in 5A004.b., 5D002.a.3.b. or 5D002.c.3.b.

b. "Technology" having the characteristics of a 'cryptographic activation token' specified in 5A002.b.

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.