1. Integrated circuits designed or rated as radiation hardened to withstand any of the following:

- A dose rate upset of $5 \times 10^6$ Gy (silicon)/s or higher; or
- A dose upset of $5 \times 10^6$ Gy (silicon); or
- A total dose of $5 \times 10^7$ Gy (silicon); or
- A total dose of $5 \times 10^7$ Gy (silicon) at a temperature higher than $218$ K (-55°C); or
- A total dose of $5 \times 10^7$ Gy (silicon) at a temperature lower than $218$ K (-55°C); or
- A total dose of $5 \times 10^7$ Gy (silicon) at a temperature lower than $218$ K (-55°C) with a dose rate of $5 \times 10^6$ Gy (silicon)/s or higher.

2. “Microprocessor microcircuits”, “microcomputer microcircuits”, “microcontroller microcircuits” containing an arithmetic logic unit (ALU) or “multichip integrated circuit” containing an arithmetic logic unit (ALU) and external storage.

3. A resolution of 12 bit or more, but less than 14 bit, with a "sample rate" greater than 250 MSPS; or
4. A resolution of 14 bit or more, but less than 16 bit, with a "sample rate" greater than 400 MSPS; or
5. A resolution of 16 bit or more, with a "sample rate" greater than 800 MSPS; or
6. "Digital-to-Analogue Converters (DAC) having any of the following:

- A dose rate upset of $5 \times 10^6$ Gy (silicon)/s or higher; or
- A dose upset of $5 \times 10^6$ Gy (silicon); or
- A total dose of $5 \times 10^7$ Gy (silicon); or
- A total dose of $5 \times 10^7$ Gy (silicon) at a temperature higher than $218$ K (-55°C); or
- A total dose of $5 \times 10^7$ Gy (silicon) at a temperature lower than $218$ K (-55°C); or
- A total dose of $5 \times 10^7$ Gy (silicon) at a temperature lower than $218$ K (-55°C) with a dose rate of $5 \times 10^6$ Gy (silicon)/s or higher.

*Note 1*: The “microprocessor microcircuit” normally does not contain external storage.

*Note 2*: This includes chip sets which are designed to operate together to provide the function of a “microprocessor microcircuit”.

*Note 3*: “Microprocessor microcircuit” (3) means a “monolithic integrated circuit” or a “multichip integrated circuit” containing an arithmetic logic unit (ALU) and capable of providing a general purpose instruction set from an external storage.

*Technical Note*: Non-volatile memories are memories with data retention over a period of time after a power shutdown.

*Note*: 3A001.a.2. does not control integrated circuits designed for civil automobiles or railway train applications.
(二)

(一)

(三)

b. A typical "basic gate propagation delay time" of less than 0.02 ns;

5. Digital-to-Analogue Converter (DAC) clock frequency of 3.5 GHz or more and a DAC resolution of 12 bit or more; or

b. A toggle frequency exceeding 1.2 GHz;

6. Electro-optical and "optical integrated circuits", designed for...
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4.1</td>
<td>1. General purpose integrated circuits, as follows:</td>
</tr>
<tr>
<td></td>
<td>a. Analogue-to-digital conversions meeting any of the following:</td>
</tr>
<tr>
<td></td>
<td>b. Any of the following:</td>
</tr>
<tr>
<td>2.5.1</td>
<td>a. Storage of digitised data; or</td>
</tr>
<tr>
<td></td>
<td>b. Processing of digitised data;</td>
</tr>
<tr>
<td>2.6.1</td>
<td>a. Solid-state pulsed power switching thyristor devices and 'thyristor modules', using either electrically, optically, or electron radiation controlled switch methods and having any of the following:</td>
</tr>
<tr>
<td></td>
<td>b. Solid-state power semiconductor switches, diodes, or 'modules', having all of the following:</td>
</tr>
</tbody>
</table>
"Information security" items or functions should be considered against the provisions in Category 5 - Part 2, even if they are components, "software" or features of other items.

"Information security" (GISN GISN 5) is all the means and functions ensuring the accessibility, confidentiality or integrity of information or communications, excluding the means and functions intended to safeguard against malfunctions. This includes "cryptography", "cryptographic activation", "cryptanalysis", protection against compromising emanations and computer security.

Technical Note: Cryptanalysis: analysis of a cryptographic system or its inputs and outputs to derive confidential or sensitive data, including clear text.

"Cryptography" (5) means the discipline which embodies principles, means and methods for the transformation of data to hide its information content, prevent its undetected modification or prevent its unauthorized use. "Cryptography" is limited to the transformation of information using one or more "secret parameters" (e.g., crypto variables) as associated key management.

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 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.

Technical Note: For the purpose of the "satellite navigation system" receiving equipment containing or employing decryption, see 7A005 and for related decryption "software" and "technology" see 7D005 and 7E001.
c. An "asymmetric algorithm" where the security of the algorithm is based on

2. Computation of discrete logarithms in a multiplicative group of a finite

a. The cryptographic capability meets all of the following:

2. Digital communication or networking systems, equipment or components, not

a. It is restricted for use in any of the following:

b. It is non-reprogrammable for any other use; or:

c. It supports a non-primary function of the item; and

b. It is specially designed and limited to allow protection of 'personal

3. Computers, other items having information storage or processing as a

2. 'Readers/writers' specially designed or modified, and limited, for items

b. A "symmetric algorithm" employing a key length in excess of 56 bits, and

1. It is specially designed and intended for use as an "asymmetric security

b. It is specially designed and intended for use in any of the following: the

b. It is specially designed and intended for use in any of the following:

2. Digital communication or networking systems, equipment or components, not

b. It supports a non-primary function of the item; and

b. It is specially designed for use in any of the following: the

1. It is specially designed and intended for use in any of the following:

3. Computers, other items having information storage or processing as a

b. It is specially designed and intended for use in any of the following: a.

3. Computers, other items having information storage or processing as a

2. Digital communication or networking systems, equipment or components, not

2. 'Readers/writers' specially designed or modified, and limited, for items

b. It is specially designed for use in any of the following: a.

1. It is specially designed and intended for use in any of the following:

b. It is specially designed for use in any of the following: a.

b. It supports a non-primary function of the item; and

b. It is specially designed and intended for use in any of the following:

b. It is specially designed and intended for use in any of the following:

b. It supports a non-primary function of the item; and
a. A network-capable endpoint device meeting any of the following:

b. Hardware components or ‘executable software’, of existing items described in paragraph a. of this Note, that have been designed for these existing items,

1. Uses only published or commercial cryptographic standards; and

2. The cryptographic functionality cannot easily be changed by the user.

b. Networking equipment meeting all of the following:

1. A bandwidth exceeding 500 MHz; or

2. The component or ‘executable software’ does not change any aspect of the endpoint device functionality to the existing items.

1. “Information security” is not the primary function or set of functions of the device.

2. The device is limited to a specific ‘connected civil industry application’;

3. The device is limited to 0,1W (20 dBm) or less, and supporting 16 or fewer concurrent users.

4. The device is limited to personal ‘connected civil industry application’ or the tasks of “Operations, Administration or Maintenance” (“OAM”)

5. The device is limited to “OAM” of the equipment.

6. Items specially designed for a ‘connected civil industry application’;

7. 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:

- spreading code for “spread spectrum” systems, other than those specified in 5A002.a. of an item already specified in Category 5 – Part 2;
- hopping code for “frequency hopping” systems.

8. Telephone call transactions;

9. Mail order transactions;

10. Limited to “OAM” of the equipment.

11. Designed or modified to use cryptographic techniques to generate channelising codes, scrambling codes or network identification codes, for systems using “personal area network” functionality, implementing only published or commercial cryptographic standards.

12. Telephone call transactions;

13. Mail order transactions;

14. Limited to “OAM” of the equipment.

15. Mobile telecommunications Radio Access Network (RAN) equipment or devices designed or modified to use cryptographic techniques to generate the hopping code for “frequency hopping” systems.

16. Technical Note: “Quantum cryptography” is also known as Quantum Key Distribution (QKD).
(1) 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.

(2) 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.

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

(3) Items limited to logical data extraction;

(4) Items specially designed and limited to jail-breaking or rooting.

As of 14/April, 2021
| 5.D.1 | Program: required for the "use" of equipment, functions or features specified by 5.A.1.
|       | A.55 | 9(1) |

5.D.2 | Program: having the performance of or emulating the functions of, any of the following:
|       | A.55 | 9(1) |

5.E.1 | "Program" required for the "development", "production", "use" of equipment, functions or features specified by 5.A.1.
|       | A.55 | 9(1) |

5.E.2 | "Program" required for the "development", "production", "use" of equipment, functions or features specified by 5.B.1.
|       | A.55 | 9(1) |

5.E.3 | "Program" that has the function specified by 5.A.2, activates the encryption function of the program and the product.
|       | A.55 | 9(1) |