

THE SCHEDULE OF THE STRATEGIC GOODS (CONTROL) ORDER 2009

PART II

DUAL-USE GOODS THE EXPORT, TRANSHIPMENT OR BRINGING IN
TRANSIT OF WHICH, AND TECHNOLOGY THE EXPORT OR
TRANSMISSION OF WHICH, REQUIRE A PERMIT

Division 2 – List of Dual-Use Goods

<i>Product Code</i>	<i>Item Description</i>
CATEGORY 5 – TELECOMMUNICATIONS AND “INFORMATION SECURITY”	
	<p>Part 2 — “INFORMATION SECURITY</p> <p><u>Note 1</u></p> <p><i>Category 5, Part 2 concerns “information security” equipment, “software”, systems, application specific “electronic assemblies”, modules, integrated circuits, components or functions whether or not they are components or “electronic assemblies” of other equipment.</i></p> <p><u>Note 2</u></p> <p><i>Category 5 - Part 2 does not include products when accompanying their user for the user’s personal use.</i></p> <p><u>Note 3</u></p> <p><u>Cryptography Note</u></p> <p><i>Category Codes 5A002 and 5D002 do not include goods that meet all of the following:</i></p> <p><i>a. Generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of the following:</i></p> <ol style="list-style-type: none"> <i>1. Over-the-counter transactions;</i> <i>2. Mail order transactions;</i> <i>3. Electronic transactions; <u>or</u></i> <i>4. Telephone call transactions;</i> <p><i>b. The cryptographic functionality cannot easily be changed by the user; <u>and</u></i></p> <p><i>c. Designed for installation by the user without further substantial support by the supplier.</i></p> <p><u>Technical Note</u></p> <p><i>In Category 5 — Part 2, parity bits are not included in the key length.</i></p>
5A2	Systems, Equipment and Components

<i>Product Code</i>	<i>Item Description</i>
DL5A002	<p data-bbox="384 315 1383 387">“Information security” systems, equipment and components therefor, as follows:</p> <p data-bbox="384 423 1383 533">a. Systems, equipment, application specific “electronic assemblies”, modules and integrated circuits for “information security”, as follows, and other specially designed components therefor:</p> <p data-bbox="422 551 488 584"><u>N.B.</u></p> <p data-bbox="422 602 1383 712"><i>For Global Navigation Satellite Systems (GNSS) receiving equipment containing or employing decryption (i.e. GPS or GLONASS), see Category Code 7A005.</i></p> <p data-bbox="422 745 1383 855">1. Designed or modified to use “cryptography” employing digital techniques performing any cryptographic function other than authentication or digital signature and having any of the following:</p> <p data-bbox="461 873 675 907"><u>Technical Notes</u></p> <p data-bbox="461 925 1383 996">1. Authentication and digital signature functions include their associated key management function.</p> <p data-bbox="461 1014 1383 1160">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 unauthorised access.</p> <p data-bbox="461 1178 1383 1249">3. “Cryptography” does not include “fixed” data compression or coding techniques.</p> <p data-bbox="461 1267 528 1301"><u>Note</u></p> <p data-bbox="461 1319 1383 1429"><i>Category Code 5A002.a.1. includes equipment designed or modified to use “cryptography” employing analogue principles when implemented with digital techniques.</i></p> <p data-bbox="461 1447 1383 1518">a. A “symmetric algorithm” employing a key length in excess of 56 bits; <u>or</u></p> <p data-bbox="461 1536 1383 1608">b. An “asymmetric algorithm” where the security of the algorithm is based on any of the following:</p> <p data-bbox="499 1626 1283 1659">1. Factorisation of integers in excess of 512 bits (e.g., RSA);</p> <p data-bbox="499 1677 1383 1787">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); <u>or</u></p> <p data-bbox="499 1805 1383 1915">3. Discrete logarithms in a group other than mentioned in Category Code 5A002.a.1.b.2. in excess of 112 bits (e.g., Diffie- Hellman over an elliptic curve);</p> <p data-bbox="422 1946 1198 1980">2. Designed or modified to perform cryptanalytic functions;</p>

<i>Product Code</i>	<i>Item Description</i>
	3. Not used;
	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, other than those specified in Category Code 5A002.a.6., including the hopping code for “frequency hopping” systems;
	6. 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: a. A bandwidth exceeding 500 MHz; <u>or</u> b. A “fractional bandwidth” of 20% or more;
	8. Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion;
	9. Designed or modified to use “quantum cryptography”. <u>Technical Note</u> “Quantum cryptography” is also known as Quantum Key Distribution (QKD).
	<p><u>Note</u></p> <p>Category Code 5A002 does not include any of the following:</p> <p>a. “Personalised smart cards” having any of the following:</p> <ol style="list-style-type: none"> 1. Where the cryptographic capability is restricted for use in equipment or systems excluded from control under entries b. to g. of this Note; <u>or</u> 2. For general public-use applications where the cryptographic capability is not user-accessible and it is specially designed and limited to allow protection of personal data stored within; <p><u>N.B.</u></p> <p>If a “personalised smart card” has multiple functions, the control status of each function is assessed individually.</p> <p>b. Receiving equipment for radio broadcast, pay television or similar restricted audience broadcast of the consumer type, without digital encryption except that exclusively used for sending the billing or programme-related information back to the broadcast providers;</p>

<i>Product Code</i>	<i>Item Description</i>
	<p>c. <i>Equipment where the cryptographic capability is not user-accessible and which is specially designed and limited to allow any of the following:</i></p> <ol style="list-style-type: none"> 1. <i>Execution of copy-protected “software”;</i> 2. <i>Access to any of the following:</i> <ol style="list-style-type: none"> a. <i>Copy-protected contents stored on read-only media; <u>or</u></i> b. <i>Information stored in encrypted form on media (e.g., in connection with the protection of intellectual property rights) when the media is offered for sale in identical sets to the public;</i> 3. <i>Copying control of copyright protected audio or video data; <u>or</u></i> 4. <i>Encryption and decryption (or either of them) for protection of libraries, design attributes, or associated data for the design of semiconductor devices or integrated circuits;</i> <p>d. <i>Cryptographic equipment specially designed and limited for banking use or ‘money transactions’;</i></p> <p><u>Technical Note</u></p> <p><i>‘Money transactions’ in Category Code 5A002 Note d. includes the collection and settlement of fares or credit functions.</i></p> <p>e. <i>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));</i></p> <p>f. <i>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; <u>or</u></i></p> <p>g. <i>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 d. 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.</i></p>
5B2	Test, Inspection and Production Equipment
DL5B002	<p>“Information security” test, inspection and “production” equipment, as follows:</p> <ol style="list-style-type: none"> a. Equipment specially designed for “development” or “production”, as follows:

<i>Product Code</i>	<i>Item Description</i>
	<p>1. “Development” of equipment or functions specified in Category Code 5A002, 5B002, 5D002 or 5E002 including measuring or test equipment;</p> <p>2. “Production” of equipment or functions specified in Category Code 5A002, 5B002, 5D002 or 5E002, including measuring, test, repair or “production” equipment;</p> <p>b. Measuring equipment specially designed to evaluate and validate the “information security” functions specified in Category Code 5A002 or 5D002.</p>
5C2	Materials
	None.
5D2	Software
DL5D002	<p>“Software”, as follows:</p> <p>a. “Software” specially designed or modified for the “development”, “production” or “use” of equipment or “software” specified in Category Code 5A002, 5B002 or 5D002;</p> <p>b. “Software” specially designed or modified to support “technology” specified in Category Code 5E002;</p> <p>c. Specific “software”, as follows:</p> <p>1. “Software” having the characteristics, or performing or simulating the functions of the equipment specified in Category Code 5A002 or 5B002;</p> <p>2. “Software” to certify “software” specified in Category Code 5D002.c.1.</p> <p><u>Note</u> Category Code 5D002 does not include “software” as follows:</p> <p>a. “Software” required for the “use” of equipment excluded from control under the Note to Category Code 5A002;</p> <p>b. “Software” providing any of the functions of equipment excluded from control under the Note to Category Code 5A002.</p>
5E2	Technology
DL5E002	“Technology” (according to the General Technology Note) for the “development”, “production” or “use” of equipment or “software”

<i>Product Code</i>	<i>Item Description</i>
	specified in Category Code 5A002, 5B002 or 5D002.