APPENDIX 1

RELEVANT PORTIONS OF THE WA-LIST

GENERAL TECHNOLOGY NOTE AND GENERAL SOFTWARE NOTE

DUAL-USE LIST – CATEGORY 5 PART 2 – ”INFORMATION SECURITY”

STATEMENTS OF UNDERSTANDING AND VALIDITY NOTES

DUAL-USE LIST

Note *Terms in "quotations" are defined terms. Refer to 'Definitions of Terms used in these Lists' annexed to this List.*

GENERAL TECHNOLOGY NOTE

The export of "technology" which is "required" for the "development", "production" or "use" of items controlled in the Dual-Use List is controlled according to the provisions in each Category. This "technology" remains under control even when applicable to any uncontrolled item.

Controls do not apply to that "technology" which is the minimum necessary for the installation, operation, maintenance (checking) and repair of those items which are not controlled or whose export has been authorised.

N.B. *This does not release such "technology" controlled in entries 1.E.2.e. & 1.E.2.f. and 8.E.2.a. & 8.E.2.b.*

Controls do not apply to "technology" "in the public domain", to "basic scientific research" or to the minimum necessary information for patent applications.

GENERAL SOFTWARE NOTE

The Lists do not control "software" which is either:

1. Generally available to the public by being:

    a. Sold from stock at retail selling points without restriction, by means of:
        1. Over-the-counter transactions;
        2. Mail order transactions; or
        3. Telephone call transactions; and

    b. Designed for installation by the user without further substantial support by the supplier; or

    N.B. *Entry 1 of the General Software Note does not release "software" controlled by Category 5 - Part 2.*

2. "In the public domain".

Part 2 - "INFORMATION SECURITY"

Note 1 *The control status of "information security" equipment, "software", systems, application specific "electronic assemblies", modules, integrated circuits, components or functions is determined in Category 5, Part 2 even if they are components or "electronic assemblies" of other equipment.*

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

Note 3 *Cryptography Note*

5.A.2. and 5.D.2. do not control items that meet all of the following:

a. Generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of the following:
   1. Over-the-counter transactions;
   2. Mail order transactions;
   3. Electronic transactions; or
   4. Telephone call transactions;

b. The cryptographic functionality cannot easily be changed by the user;

c. Designed for installation by the user without further substantial support by the supplier;

d. Does not contain a "symmetric algorithm" employing a key length exceeding 64 bits; and

e. 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. to d. above.

Technical Note

In Category 5 - Part 2, parity bits are not included in the key length.

5. A. 2. SYSTEMS, EQUIPMENT AND COMPONENTS

a. Systems, equipment, application specific "electronic assemblies", modules and integrated circuits for "information security", as follows, and other specially designed components therefor:

N.B. *For the control of global navigation satellite systems receiving equipment containing or employing decryption (i.e. GPS or GLONASS), see 7.A.5.*

5. A. 2. a. 1. Designed or modified to use "cryptography" employing digital techniques performing any cryptographic function other than authentication or digital signature having any of the following:
Technical Notes
1. Authentication and digital signature functions include their associated key management function.
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.
3. "Cryptography" does not include "fixed" data compression or coding techniques.

Note *5.A.2.a.1. includes equipment designed or modified to use "cryptography" employing analogue principles when implemented with digital techniques.*

5. A. 2. a. 1. a. A "symmetric algorithm" employing a key length in excess of 56 bits; or
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 5.A.2.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;

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, including the hopping code for "frequency hopping" systems;

6. Designed or modified to provide certified or certifiable "multilevel security" or user isolation at a level exceeding Class B2 of the Trusted Computer System Evaluation Criteria (TCSEC) or equivalent;

7. Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion.

Note *5.A.2. does not control:*

a. "Personalised smart cards" where the cryptographic capability is restricted for use in equipment or systems excluded from control under entries b. to f. of this Note. If a "personalised smart card" has multiple functions, the control status of each function is assessed individually.

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;

c. Equipment where the cryptographic capability is not user-accessible and which is specially designed and limited to allow any of the following:
1. Execution of copy-protected software;
2. Access to any of the following:
a. Copy-protected read-only media; or
b. 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; or
3. One-time copying of copyright protected audio/video data.

d. Cryptographic equipment specially designed and limited for banking use or money transactions;
Technical Note
'Money transactions' in 5.A.2. 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 end-to-end encryption;

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.

5. B. 2. TEST, INSPECTION AND PRODUCTION EQUIPMENT

a. Equipment specially designed for:

1. The "development" of equipment or functions controlled by Category 5 - Part 2, including measuring or test equipment;
2. The "production" of equipment or functions controlled by Category 5 - Part 2, including measuring, test, repair or production equipment.

b. Measuring equipment specially designed to evaluate and validate the "information security" functions controlled by 5.A.2. or 5.D.2.

5. C. 2. MATERIALS - None

5. D. 2. SOFTWARE

a. "Software" specially designed or modified for the "development", "production" or "use" of equipment or "software" controlled by Category 5 - Part 2;
b. "Software" specially designed or modified to support "technology" controlled by 5.E.2.;
c. Specific "software", as follows:
   1. "Software" having the characteristics, or performing or simulating the functions of the equipment controlled by 5.A.2. or 5.B.2.;
   2. "Software" to certify "software" controlled by 5.D.2.c.1.

Note *5.D.2. does not control:*
a. "Software" required for the "use" of equipment excluded from control under the Note to 5.A.2.;
b. "Software" providing any of the functions of equipment excluded from control under the Note to 5.A.2.

5. E. 2. TECHNOLOGY

a. "Technology" according to the General Technology Note for the "development", "production" or "use" of equipment or "software" controlled by Category 5 - Part 2.

STATEMENTS OF UNDERSTANDING AND VALIDITY NOTES

MUNITIONS LIST

ML 10 (NF (95) WG2/2)

Absence of items from the Munitions List and absence of configuration for military use would mean that an aircraft would not be considered military.

DUAL-USE LIST OF GOODS AND TECHNOLOGIES

General Technology Note (NF (95) CA WP 1)

Governments agree that the transfer of "technology" according to the General Technology Note, for "production" or "development" of items on this list shall be treated with vigilance in accordance with national policies and the aims of this regime.

General Technology Note (WG2 GTN TWG/WP1 Revised 2)

It is understood that Member Governments are expected to exercise controls on intangible "technology" as far as the scope of their legislation will allow.

General Software Note (NF (95) CA WP 1)

Governments agree that the transfer of "software", for "production" or "development" of items on this list shall be treated with vigilance in accordance with national policies and the aims of this regime.

Statement of Understanding - medical equipment (NF (96) DG PL/WP1)

Participating countries agree that equipment specially designed for medical end-use that incorporates an item controlled in the Dual-Use List is not controlled.

Category 2

2.B.1.

Validity Note 2.B.1. is valid until 5 December 2000 and renewal of the agreed parameters will require unanimous consent.

2.E.3.f.

Validity Note The control of diamond-like carbon technology in 2.E.3.f. is valid until 1 December 2000 and its renewal for an additional one-year period will require unanimous consent.

Category 4

4.A.3.b.

Statement of Understanding

Governments agree to review 4.A.3.b. six months after the date of entry into force of the amendments to the List of Dual-Use Goods and Technologies, taking into account, inter alia, relevant acquisition patterns and transfer data.

4.D.3.b.

Validity Note 4.D.3.b. is valid until 1 November 2000 and its renewal for each successive two-year period will require unanimous consent.

Category 5, Part 2

Validity Note Cryptography Note, paragraph d., as it applies to "software", is valid until 3 December 2000, and renewal for a successive period will require the unanimous consent of participating countries.

Statement of Understanding

Governments agree to review the parameters of 5.A.2.a.1.a. and 5.A.2.a.1.b., in conjunction with the review of the parameter of paragraph d. of the Cryptography Note, not later than 3 December 2000.

Category 9

9.E.2.

Statement of Understanding

"Development" or "production" "technology" controlled by 9.E. for gas turbine engines remains controlled when used as "use" "technology" for repair, rebuild and overhaul. Excluded from control are: technical data, drawings or documentation for maintenance activities directly associated with calibration, removal or replacement of damaged or unserviceable line replaceable units, including replacement of whole engines or engine modules.

ANNEX 1

4.A.3.b.
Statement of Understanding

Governments agree to review 4.A.3.b. six months after the date of entry into force of the amendments to the List of Dual-Use Goods and Technologies, taking into account, inter alia, relevant acquisition patterns and transfer data.

DEFINITION OF TERMS USED IN THESE LISTS

Statement of Understanding

Participating States note that, in these Lists, words and terms appearing under 'Definitions of Terms used in these Lists', if used in their undefined forms, take their common or dictionary meanings. Governments are expected to preserve these distinctions, as far as national languages and legislation allow, when the Lists are translated into national legislation.
(See also Note 2 to 'Definitions of Terms used in these Lists').

N.B. *The references in this section refer to the List of Dual-Use Goods and Technologies and the Munitions List approved by the Plenary Meeting in Vienna on 1st to 3rd December 1999.*