Unclassified **DSTI/ICCP/REG(98)4/FINAL**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

OLIS : 28-Jan-1999
Dist. : 01-Feb-1999

Or. Eng.

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

DSTI/ICCP/REG(98)4/FINAL
Unclassified

Working Party on Information Security and Privacy

INVENTORY OF CONTROLS ON CRYPTOGRAPHY TECHNOLOGIES

73900

Document complet disponible sur OLIS dans son format d'origine
Complete document available on OLIS in its original format

Or. Eng.

CONTEXT FOR THE INVENTORY

This report has been prepared by the Working Party on Information Security and Privacy of the OECD ICCP Committee, based on Secretariat research[1] and input supplied by Member countries.

It is important to note that in many Member countries these controls are currently under review in consideration of recent developments at the EU level, as well as ongoing negotiations at the international level. In particular, a substantial number of changes in national policies can be anticipated within a short time as a result of the ongoing negotiations on the revision of certain provisions of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.

Attention is drawn to the fact that this Inventory represents a “snap-shot” view of the controls on the export, import, and domestic use of cryptography technology as reported by Member countries as of September 1998. It should be recognised that the outcome of the ongoing international negotiations in this area could make certain aspects of the information reported in this Inventory out-of-date.

TABLE OF CONTENTS

CONTEXT FOR THE INVENTORY 2

INVENTORY OF CONTROLS ON CRYPTOGRAPHY TECHNOLOGIES 4

OVERVIEW 4
OECD work in the field of cryptography policy 4
Cryptography technologies 5
Controls on cryptography technologies in OECD Member countries 5
INTERNATIONAL INSTRUMENTS 6
The Wassenaar Arrangement 6
European Union 9
Other European Fora 11
OECD MEMBER COUNTRIES 12
Australia 12
Austria 13
Belgium 14
Canada 15
Czech Republic 16
Denmark 17
Finland 18
France 18
Germany 20
Greece 21
Hungary 21
Iceland 22
Ireland 22
Italy 22
Japan 24
Korea 25
Luxembourg 26
Mexico 26
The Netherlands 26
New Zealand 27
Norway 28
Poland 29
Portugal 29
Spain 29
Sweden 30
Switzerland 31
Turkey 32
United Kingdom 32
United States 34
ANNEXES 40
ANNEX I: SUMMARY TABLE OF NATIONAL RESPONSES 41
ANNEX II: THE WASSENAAR ARRANGEMENT (Excerpts only) 46

INVENTORY OF CONTROLS ON CRYPTOGRAPHY TECHNOLOGIES

OVERVIEW

OECD work in the field of cryptography policy

The OECD Information, Computer and Communications Policy (ICCP) Committee has included cryptography technologies and policies in its work on security and privacy since 1989. The current work in this area is handled by the ICCP's Working Party on Information Security and Privacy (WISP). The OECD's experience in addressing policy areas that combine economic, technological and legal aspects, and the Organisation's established body of work related to security of information systems, protection of personal data and privacy, and information, computer and communication technologies, makes it an appropriate forum to discuss cryptography technologies and the economic and social policy issues related to the use of cryptography. Both the 1980 *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* and the 1992 *OECD Guidelines for the Security of Information Systems* identified the need for technological means to assure protection of personal data and privacy and security of information systems. Building upon those instruments, the 1997 *OECD Guidelines on Cryptography Policy*[2] provide a comprehensive approach to international cryptography policy by identifying the basic principles that governments should take into consideration when developing their policies on cryptography.

In recent years OECD Member countries have undertaken to develop and implement policies and laws relating to cryptography, and in many countries these are still in the process of being developed. However, the governments of Member countries have recognised the need for an internationally co-ordinated approach to facilitate the smooth development of an efficient, secure information infrastructure. To that end, the Working Party has committed to ongoing information exchange in the field of cryptography policy to promote a further discussion of related issues. As a part of the continuing work of the OECD in this area, this *Inventory of Controls on the Use of Cryptography Technologies* has been compiled by the Working Party based on the research of the OECD Secretariat and input from Member countries.

This Inventory intends to facilitate international co-operation by surveying international and national instruments relating to controls on the export, import and domestic use of cryptography technologies in OECD Member countries. Specifically, the report addresses:

- to what extent do countries have domestic controls on encryption, and what amendments to domestic laws, if any, are contemplated; and

- to what extent do countries have import or export controls on encryption, and what amendments to such import or export laws, if any, are contemplated.

This Inventory does not include laws on the use of cryptography for authentication and certification, which are covered by a separate report directed specifically at that issue, the *Inventory of Approaches to Authentication and Certification in a Global Networked Society*[3].

Cryptography technologies

Cryptography is an important component of secure information and communications systems and an essential technology for enabling electronic commerce, and a variety of applications have been developed that incorporate cryptographic methods to provide data security. Cryptography is a tool for achieving two related, but distinct, aspects of data security: making it possible to verify the integrity of data and/or the authentication of the sender of a message (using a "digital signature" function), and ensuring the confidentiality of data (using an "encryption" function). Each of these uses for cryptography offers certain benefits and raises different issues.

Governments are challenged by the critical need to encourage the widespread use of cryptography, both to facilitate electronic commerce and to enable users to protect data by keeping communications private during transmission, securing stored data, or providing assurances about who has sent a particular message or signed an electronic contract. At the same time governments are concerned about the implications that the widespread use of cryptography may have for law enforcement in limiting the ability of legal authorities to understand lawfully accessed transmitted or stored data. While the OECD Cryptography Guidelines identify the various interests which must be balanced in the context of international cryptography policy, they do not resolve the fundamental question of how governments can give the benefits of cryptography to legitimate users, without empowering criminals to use it for illegal purposes.

Controls on cryptography technologies in OECD Member countries

A variety of approaches to controlling the use of cryptography technologies have been adopted by OECD countries. In an attempt to separate the issues in terms of the two distinct uses for cryptography, most OECD countries have adopted a dual approach in the process of regulating cryptography: that is, law and policy about cryptography used for encryption is considered separately from "digital signature" laws. One method for controlling the use of cryptography for encryption is to make it illegal to use cryptography to conceal information unless the government has access to the private decryption keys. Another approach is to allow cryptography to be used domestically, but to restrict the export of cryptography products. To address the criminal use of cryptography for concealing information, the court system can be used as a measure to obtain the keys to encrypted data from accused parties.

The main international instrument dealing with export controls on cryptography technologies is the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (July 1996). The Wassenaar Arrangement is a collaboration of countries that defines a set of preliminary guidelines, covering both armaments and sensitive dual-use goods and technologies, which need to be fully implemented at the national level. Participants agree to control through their national laws, regulations and policies those items and technologies contained in a list of Dual-Use Goods and Technologies -- that includes cryptographic goods and technologies -- and a separate Munitions List. All but two OECD Member countries are members of the Wassenaar Arrangement. In addition, the Regulation and Decision of the Council of the European Union concerning the control of the export of dual-use goods (19 December 1994) applies to the 15 Member States of the European Union, all of whom are also OECD Member countries. The list of controlled products in the EU Regulation is based on the Wassenaar Arrangement and other international non-proliferation agreements. In fulfilling their obligations under the Wassenaar Arrangement (and for members of the European Union, the EC Regulation), 27 of the 29 OECD countries place controls on the export of cryptography technologies. Although most of these countries have enacted controlling legislation or regulations, and created licensing authorities, the implementation details vary from country to country.

The Inventory reveals that one way in which the national export controls on cryptography products differ concerns the treatment of cryptography software which is "generally available to the public" or in the "public domain". The Wassenaar Arrangement and the EC Regulation are both subject to a "General Software Note" which exempts such software from export controls. However, according to the Inventory, the General Software Note is not implemented at all in some Member countries and only partially in others. Differences in national approaches to export controls also exist with respect to the treatment of software which is distributed in an intangible form over a data network such as the Internet. Not all Member countries have explicitly addressed this issue, but of those that have, the Inventory shows that some draw a distinction between "tangible" and "intangible" transfers, while others treat both forms of transfer in the same manner.

The Inventory found that the domestic use of cryptography products is unrestricted in the majority of OECD Member countries. However, a small number of Member countries have general laws governing the domestic use of cryptography technologies or minor sector-specific regulations. Controls on the import of cryptography technologies, such as licensing requirements, exist in four OECD Member countries.˙

INTERNATIONAL INSTRUMENTS

The Wassenaar Arrangement

For over four decades, export controls on cryptography were governed by the Coordinating Committee for Multilateral Export Controls (COCOM)[4]. COCOM was created in 1950 to respond to the threat of the Cold War by preventing the sale of arms, and controlling the export of strategic products and technical data from COCOM Member countries to the Warsaw Pact countries. Under the COCOM regime, cryptography was considered a strategic good with military applications, and thus was subject to trade restrictions. In 1991, COCOM decided to allow the export of all mass-market software (including public domain software); most COCOM Member countries reflected these changes in their national regulations.

In response to the diminishing Cold War threat, and in light of emerging new risks to global security, COCOM was dissolved in March 1994 as part of a plan to make a transition to a different kind of arrangement. The focus had shifted from a Western screen for controlling the transfer of military technologies, toward a mechanism to deal with risks to regional and international security and stability related to the spread of conventional weapons and dual-use goods and technologies. Negotiations were initiated by former COCOM countries to develop an arrangement, which would differ significantly in both its goals and procedures, highlighting mechanisms for transparency. During the interim period former members of COCOM agreed to continue the use of the COCOM control lists as a basis for global export controls on a national level until the new arrangement could be established, therefore cryptography remained on export control lists.

Since 1996, the main international instrument dealing with export controls on cryptography technologies has been the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. The Wassenaar Arrangement was formally approved by 33 countries, including 27 of the 29 OECD Member countries, in July 1996.[5] Prior to it's final adoption, the interim agreement was provisionally called the "New Forum". The Wassenaar Arrangement is a collaboration of countries that defines a set of preliminary guidelines covering both armaments and sensitive dual-use goods and technologies which need to be fully implemented at the national level. It focuses on threats to international and regional peace and security by providing for greater openness through information sharing about arms, dual-use goods and technology transfers world-wide.

Basically, the Wassenaar Arrangement provides a global mechanism for controlling legitimate transfers of conventional armaments and sensitive dual-use items, and a venue in which governments can consider collectively the implications of various activities on international and regional security. Agreement is by consensus, and membership is open on a global and non-discriminatory basis to all countries meeting the agreed criteria. When deciding on the eligibility of a state for participation, certain factors, *inter alia*, are taken into consideration, as an index of the country's ability to contribute to the purposes of the Arrangement. These include whether the country is a producer or exporter of arms or dual-use equipment; the country's non-proliferation policies; and its appropriate national policies, including adherence to the major non-proliferation regimes and its adherence to fully effective export controls. The agreement outlines a formal process of transparency, consultation, and where appropriate, multilateral restraint.

Participants agree to control through their national laws, regulations and policies those items and technologies contained in a list of Dual-Use Goods and Technologies and a separate Munitions List. Implementation of the Lists at the national level began in November 1996. The Arrangement established a Secretariat in Vienna where participants meet regularly. The first overall review of the Arrangement will be held in 1999. Aggregate data on transfers, and denials, is exchanged every six months. Denials of sensitive/very sensitive goods and under-cuts[6] have to be notified on an early and timely basis[7].

There are four principal objectives of the Arrangement. It aims to contribute to regional and national security by:

- promoting transparency and greater responsibility with regard to transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations;

- seeking through national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities;

- complementing and reinforcing, without duplication, the existing control regimes for weapons of mass destruction and their delivery systems, as well as other internationally recognised measures designed to promote transparency and greater responsibility, by focusing on the threats to international and regional peace and security which may arise from transfers of armaments and sensitive dual-use goods and technologies where risks are judged greatest; and,

- enhancing co-operation to prevent the acquisition of armaments and sensitive dual-use items for military end-uses, if the situation in a region or the behaviour of a state is, or becomes, a cause for serious concern to the Participating States.

The "Initial Elements" of the Wassenaar Arrangement include two lists of items and technologies which Member countries have agreed to[8]: (1) a Munitions List which covers military goods and technologies; and (2) a List of Dual-Use Goods and Technologies, i.e. goods that can be used both for a military and for a civil purpose. The latter list is divided into three Tiers: Tier 1 (basic list) and Tier 2 (sensitive list[9]) and Sub-Set of Tier 2 (very sensitive list[10]). The agreement imposes a reporting requirement for the transfer or denial to a non-participant country of listed dual-use goods and technologies. The Tier 1 list requires notification of denials, to be given aggregately on the usual six-monthly basis. However, Tier 2 and Sub-Set of Tier 2 goods and technologies have a higher standard requiring individual notice to be given upon each denial to non-participant states, in no later than 60 days after the date of the occurrence. Transfers of these sensitive goods are also notified on an aggregate basis twice annually.

The Arrangement also requires participating countries to inform one another when a license is approved for an essentially equivalent item to be shipped to an end-user to which another participating country has denied a licence within the preceding three years (“under-cutting”). Although participating countries are encouraged to exercise vigilance in the control of listed items, there is no specific obligation to require individual licenses, this is left to national discretion.

Cryptographic goods and technologies appear on the List of Dual-Use Goods and Technologies under Category 5, Part 2, “Information Security”. Both hardware and software cryptography technologies are listed for control. The exceptions to the provisions covering cryptography technologies are noteworthy:

> *5.A.2. does not control:*
>
> *a. "Personalised smart cards" or specially designed components therefor, with any of the following characteristics:*
>
> > *1. Not capable of message traffic encryption or encryption of user-supplied data or related key management functions therefor; or*
> >
> > *2. When restricted for use in equipment or systems excluded from control under entries 1. to 6. of the Note to 5.A.2.a.3. or under entries b. to h. of this Note;*
> >
> > *b. Equipment containing "fixed" data compression or coding techniques;*
> >
> > *c. Receiving equipment for radio broadcast, pay television or similar restricted audience television of the consumer type, without digital encryption and where digital decryption is limited to the video, audio or management functions;*
> >
> > *d. 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;*
> >
> > *e. Decryption functions specially designed to allow the execution of copy-protected "software", provided the decryption functions are not user-accessible;*
> >
> > *f. Access control equipment, such as automatic teller machines, self-service statement printers or point of sale terminals, which protects password or personal identification numbers (PIN) or similar data to prevent unauthorized access to facilities but does not allow for encryption of files or text, except as directly related to the password or PIN protection;*
> >
> > *g. Data authentication equipment which calculates a Message Authentication Code (MAC) or similar result to ensure no alteration of text has taken place, or to authenticate users, but does not allow for encryption of data, text or other media other than that needed for the authentication;*
> >
> > *h. Cryptographic equipment specially designed and limited for use in machines for banking or money transactions, such as automatic teller machines, self-service statement printers or point of sale terminals.*

According to the “General Technology Note” of the Dual-Use List, controls do not apply to "technology" "in the public domain", to "basic scientific research", or to the minimum necessary information for patent applications. In addition, the “General Software Note” states that:

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*

2. "In the public domain".

A substantial number of changes in national policies can be anticipated within a short time as a result of the ongoing negotiations on the revision of certain provisions of the Wassenaar Arrangement. The outcome of those negotiations is likely to necessitate a revision of this Inventory.

European Union

Export controls

The Regulation and Decision of the Council of the European Union of 19 December 1994 concerning the control of the export of dual-use goods[11] is the basis for the EU regime which governs the export of cryptography technologies. The list of controlled products is based on the Wassenaar Arrangement and other international non-proliferation regimes.

The EC Regulation sets forth a license requirement for the export of certain cryptography products outside of the EU. For a transitional period, the Regulation also requires a licence procedure for intra-Community trade of certain particularly sensitive encryption products, which amounts to EU domestic controls on products shipped between Member States. However, the Regulation does not set out in full the scope, content and implementation practices of national controls. As a result, there is some divergence in national practices among EU Member States.

The Decision which implements the Regulation includes specific exceptions to the export controls that have an effect on the export of cryptography, and which some have interpreted as an indication that the export of cryptography via the Internet does not fall within the scope of the Regulation. In particular, the Decision states that the control of technology is limited to tangible form[12]. Furthermore, the “General Technology Note” of the Decision states that controls on technology do not apply to information “in the public domain”, and the “General Software Note” (which follows the wording of the Wassenaar Arrangement’s General Software Note) indicates that the export control list does not include software which is “in the public domain” or “generally available” to the public by being (1) sold from stock at retail selling points, without restriction by means of over-the-counter transactions, mail order transactions, or telephone order transactions; and (2) designed for installation by the user without further substantial support by the supplier.

Other controls

There are no import controls on cryptography technologies imposed by European Union legislation.

The Treaty of Rome enshrines the principle of the free movement of goods within the Community, which has implications for national cryptography policies of the Member States.

The European Council Resolution of 17 January 1995 on the lawful interception of telecommunications[13] contains a requirement for network operators and service providers, if they use encryption, to provide intercepted communications to law-enforcement agencies *en clair*, that is, to provide the signal as they received it.

General policy developments

In October 1997 the European Commission published a Communication "Ensuring security and trust in electronic Communication - Towards a European Framework for Digital Signatures and Encryption"[14], which describes both the authentication and integrity functions of cryptography, as well as confidentiality functions. The Communication addresses lawful access to encryption keys (key recovery or key escrow schemes) under the latter section, on the basis that such schemes might be interpreted as domestic controls of cryptography. The Communication recognises that there are a number of commercial applications of 'encryption', including pay TV, which uses encryption so that once the subscriber pays a fee, the transmission is decrypted.

The Communication endorses the use of encryption to enable law-abiding citizens and companies to protect themselves against criminal attacks, although noting that criminals cannot totally be prevented from using the technologies for their own ends. It states that "the public needs to have access to technical tools allowing effective protection of the confidentiality of data and communication against arbitrary intrusions. Encryption of data is very often the only effective and cost-efficient way of meeting these requirements." The Communication goes on to indicate that the Commission will be diligent in seeing that Member States' national restrictions in the area of national security and law enforcement are justified and abide by the EU free circulation provisions, and Data Protection Directive. With regard to regulations on the use of encryption, it notes that "divergence between regulatory schemes might result in obstacles to the functioning of the Internal Market."

The Communication also points out that Member States must report to the Commission any proposals to impose technical rules for marketing, use, manufacture or import of cryptographic products[15].

The Communication advises that the dual-use Regulation should be adapted in view of the requirements for the cryptographic products market. It states that Article 19 of the Regulation contains a provision which should be re-examined, in particular to:

- progressively dismantle intra-Community controls on commercial encryption products (although not necessarily for very advanced encryption);

- launch a discussion on the scope and interpretation of certain provisions, such as the "General Software Note" (which stipulates that public-domain software is not subject to controls); and

- deal with problems like intangible means of transmission (such as fax or e-mail).

Finally, the Communication advocates co-operation between police forces on a European and international level, as well as international action to create a framework for electronic commerce which would involve mutual recognition of certificates and common technical standards.

On 15 May 1998, the Commission adopted a Proposal for a Council Regulation (EC) setting up a Community regime for the control of exports of dual-use goods and technology (COM(1998) 257 final, 98/0162 (ACC)), which introduce a notification procedure for intra-Community shipments of cryptographic products instead of an authorisation scheme.

On 13 May 1998, the European Commission adopted a Proposal for a European Parliament and Council Directive on a common framework for electronic signatures (European Commission, COM(1998) 297 final, 13.05.98).[16] The proposed Directive follows the Communication, with a view to harmonising European initiatives on electronic signatures and to promoting the legal recognition of electronic signatures. The proposal also contains provisions for cross-border mechanisms aimed at ensuring interoperability at a global level. It is currently under consideration by the European Parliament and Council.

In 1997 the Commission proposed a European Parliament and Council Directive on the legal protection of services based on, or consisting of conditional access. The proposal is based on a wide-ranging consultation in the context of the Green Paper on “Legal Protection for Encrypted Services In the Internal Market”. The proposed Directive would cover all encoded services where encoding is used to ensure payment of a fee, including information society services provided at a distance by electronic means and at the individual request of a service receiver, as well as broadcasting services[17].

Other European Fora

On 11 September 1995, the Council of Europe adopted a Recommendation[18] concerning problems of criminal procedural law connected with information technology. The document states that, "[m]easures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offences, without affecting its legitimate use more than is strictly necessary." The Recommendation does not however require Member states to implement any specific policy on encryption in their jurisdictions.

A Ministerial level conference on Global Information Networks was held in Bonn on 6-8 July 1997. The Declaration of European Ministers[19] issued following the conference recognises the importance of strong cryptography, and declares that cryptographic products should be available internationally and users should have free choice of cryptographic technologies, subject to applicable law. It urges that measures to safeguard lawful access should be proportionate and effective.

OECD MEMBER COUNTRIES

Australia

Export controls

Australia[20] is a member of the Wassenaar Arrangement.

The export of cryptographic hardware and software from Australia is controlled under Reg 13E of the Customs (Prohibited Exports) Regulations[21] and through the Defence and Strategic Goods List which is administered by the Department of Defence[22].

Written permission from the Department of Defence is required for exporting "systems equipment and components" designed or modified to use cryptography or ensure information security or perform cryptoanalytic functions. Applications for export licences are reviewed by the Defence Signals Directorate of the Department. In practice, export approval is granted on a routine basis for encryption software with key lengths of 56 bits or less.

Within the Australian export controls, the General Software Note does not apply to information security software, including cryptographic software. That is, the export controls apply to cryptographic software even if it is in the public-domain or "generally available". However, public-domain "technology" is excluded[23].

The Australian export restrictions on cryptography technologies include the same exemptions as those outlined in the Dual-Use List of the Wassenaar Arrangement. A personal-use exemption also exists for the temporary export of limited amounts of cryptographic hardware or software by Australian citizens or lawful permanent residents, according to the following limitations:

a) no transfer of hardware, software or technology takes place as a result of the exportation of the cryptographic products;

b) the cryptographic products remain under the control of and in the possession of the exporter;

c) the cryptographic products are not to be reproduced or copied;

d) the cryptographic products must be returned to Australia when the exporter returns to Australia; and

e) the cryptographic products shall not be used for demonstration, marketing or sales of controlled cryptographic products.

The quantity of cryptographic hardware or software products which may be exported under the authority of the permit is limited to one each of any hardware product, and one copy of each software product per exporter, per trip outside of Australia. Records of temporary exports and re-imports under the permit should be maintained by the exporter for a period of 3 years from the date of each temporary export.

The current export control legislation in Australia does not define "tangible" or "intangible" and the application of export restrictions is unclear.

Domestic controls and import regulations

There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies currently in place in Australia.

General policy developments

The Australian Government has no proposals to change the existing policy of not imposing controls on the import or use of cryptography products. The question of export controls will be reviewed following the latest round of Wassenaar discussions.

Austria

Export controls

Austria is a member of the Wassenaar Arrangement and the European Union.

The export of cryptographic products is regulated by Section 8 of the *Außenhandelsgesetz* (BGBl. Nr. 172/1995) which prohibits export if it would breach EU Regulation 3381/94 or other international obligations, or endanger world peace, international security or the security of Austria, or damage Austria's external relations. Export to war zones is also forbidden.

The authority responsible for administering the export controls is the Federal Ministry of Economic Affairs[24].

The General Software Note is incorporated by reference into Austrian law. "Generally available" software and software and technology "in the public domain" do not fall within the scope of the Austrian controls.

Currently the Austrian export control legislation regulates only the export of cryptography products which are in a tangible form.

Domestic controls and import regulations

There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in Austria.

The *Betriebsfunkverordnung* forbids the use of cryptography for in-house (i.e. internal to an organisation) radio transmissions.

General policy developments

Austria follows the developments of the EU, and has no divergent policy developments.

Belgium

Export controls

Belgium is a member of the Wassenaar Arrangement and the European Union.

Export rules in Belgium are contained in the Law of 5 August 1991, the Ministerial decree of 19 May 1995 (implementing the EC Regulation) and the Royal Decree of 8 March 1993 regarding the import, export and transmission of arms, munitions and materials for military use and of related technology. The controls follow the EU Regulations on the export of cryptographic products. An export license for exporting cryptography hardware or software outside of the Benelux countries is required.

The A.R.E., 4th Division, is the agency in charge of issuing licences for export and transmission of cryptographic materials. Applications for licences, with accompanying technical documentation, are assessed by the Division's engineers who determine the legislation which applies to the product. Where the product does not come under the export controls it can be freely exported and an attestation is provided to this effect.

The General Software Notes is implemented in Belgium; "generally available" software and software and technology "in the public domain" do not fall within the scope of the Belgian controls.

Belgian export controls concern only the export of tangible goods. At present, intangible goods are not controlled, although Belgium is involved in the discussions of this issue at the European level.

Domestic controls and import regulations

There are no import restrictions on cryptography technologies currently in place in Belgium.

Belgian law specifically declares that the domestic use of cryptography will be unrestricted. The Law of 19 December 1997 created a new Article 109 in the Law of 21 March 1991 which provides that "the use of cryptography shall be free from restrictions". The aim of this new Article is to provide the legal framework needed for increasingly common applications of cryptography. It allows cryptographic techniques to be freely used within the private domain, private enterprises and private networks. Encrypted messages can be freely transmitted. The Law also provides that:

> *In order to supply to the public the cryptographic services determined by the Crown, prior notification must be given to the Belgian Institute for Postal services and Telecommunications (BIPT). Such notification must be sent by registered letter no later than four weeks before the activity begins.*

The procedures for meeting this obligation, and the natural or legal persons to whom the obligation would apply, were to be specified in an Implementing Order. However, this Order was never issued and cryptography therefore remains free from any administrative restrictions in Belgium. The problems relating to cryptography will to a large extent be settled in Belgium in the context of recent developments regarding digital signatures[25] and computer crime (see below).

General policy developments

As part of the effort to combat crime and amend the Penal Code to take account of new computer-related offences, a Draft Law on Computer Crime is currently before the Belgian Parliament.

This draft Law authorises the Public Prosecutor, in the event of an offender being caught in the act, or the examining magistrate, as part of his enquiry, to have a message decrypted and to read that message. The Public Prosecutor or Examining Magistrate may seek assistance from any person who may have particular knowledge about the computer system, other than the suspect himself or members of his family, in order to gain access, in an understandable format, to encrypted data that have been stored in, or transmitted by, that system.

Canada

Export controls

Canada is a member of the Wassenaar Arrangement.

Canada’s export controls are based on the Export and Import Permits Act which is administered by the Department of Foreign Affairs and International Trade. The Canadian Export Control List, a regulation under the Act, comprises a wide range of military and strategic goods which includes hardware and software products designed or modified to use cryptography. However, there are a number of exceptions, coinciding with the exclusions contained in the Wassenaar Dual-use List.

Canada exempts from export licenses mass market software or software “in the public domain” in accordance with Wassenaar’s General Software Note (GSN). A one-time review and clarification of the status of individual products is strongly encouraged, including a detailed assessment of distribution mechanisms that might qualify a product to be considered as mass market software or public domain software.

For controlled cryptographic products, individual export permits are required, except in instances where Canadian residents may be travelling temporarily away from Canada and may wish to take with them a portable personal computer with its resident encryption software; in these cases a General Export Permit is in place.

All US-origin goods are also controlled under Canadian rules, and require either an individual or general export permit. All types of cryptography can be exported from Canada to the US permit-free; however, US-origin cryptography which is not included in the Canadian Export Control List (e.g. mass market or public domain software) cannot be exported from Canada without a Canadian general or individual export permit.

Inasmuch as cryptography exports are highly sensitive, Canada encourages equal compliance for software exports, regardless of whether the product is in tangible (i.e. a physical diskette) or intangible form (i.e. an electronic file distributed via the Internet).

Export permits for controlled products are issued by the Export Controls Division of the Department of Foreign Affairs and International Trade, following consultations with other pertinent branches of the Canadian Government. In practice, export approval is now assessed on a routine basis, for multiple destination countries or end-users, for encryption products with key lengths of 56-bit DES equivalent or less, subject to a one-time review. Permits are also facilitated where trusted end-users, such as Canadian corporations or bona fide financial institutions, are involved.

Domestic controls and import regulations

There are no domestic controls on the use of cryptography, or import restrictions, currently in place in Canada.

General policy developments

The Canadian Government believes that, while the benefits of cryptography for electronic commerce, privacy protection and crime prevention are clear, it is equally true that cryptographic technologies can be used to hide criminal activity and threaten national security. Investigations and prosecutions and the enforcement of laws and regulations will be hampered if there is no lawful access to plain text.

Canadian cryptography policy is under review in order to ensure that it contributes to the realisation of Canada's goal to be a leader in the use of electronic commerce, and reflects an appropriate balance between business, human rights and privacy interests, public safety and law enforcement and national security interests. One of the components of this review was a public consultation process involving a discussion paper entitled "A Cryptography Policy Framework for Electronic Commerce: Building Canada's Information Economy and Society"[26] (February 1998). A new cryptography policy for Canada will be released in the Fall of 1998.

A description of the Government of Canada public key infrastructure, and the electronic authentication and confidentiality services that it will support for the electronic conduct of government business, both internally and with its clients, can be found at the Communications Security Establishment Website: "Government of Canada Public Key Infrastructure - White Paper"[27] (February 1998).

Czech Republic

Export controls

The Czech Republic is a member of the Wassenaar Arrangement.

The Czech Republic recently enacted the "Control of Exports and Imports of Goods and Technologies Subject to International Control Regimes"[28]. This Act is implemented by decree, incorporating the EU and Wassenaar lists of controlled dual-use goods.

Export permits for controlled products are reviewed by the Czech Ministry of Industry and Trade. There are two kinds of licenses for export of cryptography products: an "individual license" or an "individual open license". Exporters typically receive an individual license with a written statement about the transaction. An individual open license is used for expected recurring exports of specific controlled goods within a particular territorial scope and a certain time period.

The Czech Republic's export restrictions only apply to tangible technology. "Generally available" software and public domain software and technology are exempted.

Domestic controls and import regulations

The Czech Republic's export control regime described above also applies generally to the import of these controlled goods[29]. However, the Ministry has granted a general license for the import of cryptographic products[30]. Thus, while the government retains authority to control imports of encryption, an importer of products incorporating cryptography does not currently need any special authorisation for such imports.

No domestic controls on the use of cryptography are currently in place in the Czech Republic.

Denmark

Export controls

Denmark is a member of the Wassenaar Arrangement and the European Union.

Export controls in Denmark are implemented in the Executive Order on Exports of Dual-Use Goods, Technologies and Know-how[31]. The licensing authority is the Danish Agency for Trade and Industry.

The General Software Note is implemented in Denmark according to the Wassenaar text and is applied to cryptography products. An exporter may contact the export control authority to clarify whether a cryptographic product is exempt from the normal licensing requirements.

The Danish export control legislation covers both tangible and intangible software transfers. While no real advance control is applied to prevent unauthorised intangible transfers, penal sanctions can be applied for unlicensed transfers of products which are subject to the export controls.

Domestic controls and import regulations

No domestic controls on the use of cryptography, or import restrictions on cryptography technologies, are currently in place in Denmark.

General policy developments

In general, Denmark will aim to balance the needs of law enforcement authorities for lawful access to transmitted or stored data, with the needs of business enterprises and citizens for strong encryption.

An Expert Committee on Cryptography under the auspices of the Ministry of Research and Information Technology, including representatives from other Danish Ministries, released a Report in April 1997[32]. The Committee studied the advantages and disadvantages of introducing regulations covering the use and sale of cryptography. The Committee recommended against introducing such regulations, but suggested that Danish cryptography policy should be viewed in light of international developments. An analysis of the effects of introducing incentive schemes for the use of key recovery systems was finished in May 1998, which concluded that the introduction of such schemes could not be recommended in light of the present international situation.

Against this background, the Expert Committee made its final recommendations in June 1998. The Committee concluded that neither regulation nor incentive schemes should be implemented at this time, but that Denmark should not renounce the possibility of being able to regulate the field of cryptography at a later date if the general international approach moves in this direction. The Danish government now expects to formulate a Danish cryptography policy on the background of the recommendation from the expert committee.

Finland

Export controls

Finland is a member of the Wassenaar Arrangement and the European Union.

Export controls in Finland have been implemented by the Act on the Control of Exports of Dual-Use Goods (562/96), the Decree on Export of Dual-Use Goods (645/96) and the Decision of the Ministry of Trade and Industry on the export licensing of dual-use products (9 January 1997, 54/1997). These laws implement the EC regulation and decision on the export of dual-use goods.

The export of cryptographic products requires a license under the 1996 Law. The licensing authority is the Ministry of Trade and Industry.

The EU decision and regulation are incorporated by reference into Finnish law. Finland applies the General Software Note; an export license is not needed for "generally available" software or "public domain" software and technology. However, Finland restricts the export of "technical assistance" and other "services".

Finnish export controls apply to both tangible and intangible software transfers.

Domestic controls and import regulations

There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in Finland.

General policy developments

National policy on encryption issues is still in preparation in Finland. The level of export control for dual-use goods has been, and will continue to be, as agreed together with other participating countries in international export control regimes such as the Wassenaar Arrangement.

France

Export controls, domestic controls and import regulations[33]

France is a member of the Wassenaar Arrangement and the European Union.

The French government agency in charge of implementing laws related to cryptography is the "Service Central de la Sécurité des Systèmes d'Information"[34] (SCSSI), which comes under the authority of the Secretary General for National Defence.

The controls on encryption in France are governed by:

- law 90-1170 of 29 December 1990 (Official Journal of 30 December 1990), article 28; modified by law 91-648 of 11 July 1991 (Official Journal of 13 July 1991); and further modified by law 96-659 of 26 July 1996, notably article 17 on penalties (Official Journal of 27 July 1996);

- decree 95-613 of 5 May 1995 on the control of the export of goods with a double use (Official Journal of 7 May 1995, page 7547);

- order of 5 May 1995 on the control of export to third party countries and the transfer to member states of the European Community of goods with a double use (Official Journal of 7 May 1995, page 7561);

- order of 5 May 1995 defining the general G.502 licence for the export of encryption methods and setting out the means for establishing and using this licence (Official Journal of 7 May 1995, page 7578);

- decree 96-67 of 29 January 1996 relating to the powers of the Secretary General for National Defence (SGDN) on security in information technology (Official Journal of 30 January 1996);

- decree 98-101 of 24 February 1998 defining the conditions in which declarations are submitted and licences granted for the import, export, use and supply of encryption products (Official Journal of 25 February 1998, page 2911); and

- decree 98-102 of 24 February 1998 defining the conditions in which trusted third parties are licensed pursuant to article 28 of Law 90-1170 of 29 December 1990 on telecommunications regulations (Official Journal of 25 February 1998, page 2915).

In summary, Article 28 of the “Telecommunications Law”, the Law of 29 December 1990 states that for use, supply and export of cryptography with no other object than authentication of data or assuring data integrity, a prior declaration must be submitted. A copy of the acknowledgement of declaration must be presented to customs at each export. For temporary export, a user declaration will serve as an export declaration in the case of cryptography exclusively for personal use by an individual. For any other kind of cryptography, a prior authorisation is needed.

France updated its Telecommunications Law[35] in 1996 (the “26 July Law”). Article 17 deals with cryptography. The supply, import from countries outside the European Union, or export of an encryption device or service is subject to authorisation if it performs functions of confidentiality.

The French law does not apply the General Software Note exemption with respect to the export of cryptography products from France.

The French export controls do not distinguish between software which is physically exported in a tangible form or distributed in intangible form, for instance via a data network such as the Internet.

Regarding the use of cryptography products in France, Article 17 of the 26 July Law relaxes restrictions on the use of authentication devices, stating that no prior declaration will be required for “encryption devices or services which do not provide confidentiality but are used to authenticate or guarantee the integrity of messages; where the device provides for confidentiality functions based solely on secret conventions managed under approved procedures and by an organisation approved under the conditions defined in Part II of the Article i.e. a licensed trusted third party.”

Under French law a trusted third party will be a government licensed organisation which manages encoding keys for users. The licenses will be conditional upon the trusted third party submitting encoding keys to the appropriate authorities according to the law so that the State can, if necessary, access the information. Supply of cryptographic products remain subject to authorisation even if they are used in conjunction with a trusted third party.

The French Government describes a trusted third party's function as follows:

> *The trustworthy third party is a recognised organisation which manages encoding keys on the user's behalf. The user signs a contract with the trustworthy third party which regularly transmits the keys to use to encode information to the user. A clause is written into the licensing agreement with the trustworthy third party which stipulates that it must submit the encoding keys to the proper authorities according to the law. Thus, users can use an encryption professional who guarantees a high quality service to them, while the State can, if need be, have access to the information.*

General policy developments

The 26 July Law is currently being implemented and it is expected that the first trusted third parties will be licensed by the end of September 1998. A forum to discuss the implementation of the Law and to consider amendments to the regulations will be organised by the Ministry of Industry in early 1999.

Germany

Export controls

Germany is a member of the Wassenaar Arrangement and the European Union.

Export of cryptographic products from Germany is regulated by implementation of the EU Dual-Use Regulation. The administrating authority is the Federal Ministry of Economics (BMWi).

"Generally available" software and software and technology 'in the public domain' do not fall within the scope of the German controls.

Domestic controls and import regulations

There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in Germany.

General policy developments

The German approach is generally reflected in the Electronic Commerce Initiative of the Federal Government[36] of 29 October 1997. The statement declares that "[t]he German government does not presently intend to regulate by statute the marketing and use of encryption products. In Germany, encryption systems may thus be freely chosen and used."

The government's progress report to the German action plan "Info 2000 -- Germany's Way to Information Society" (Autumn 1997) states the following goals to be pursued concerning encryption products:

- ensuring availability of reliable and strong systems in Germany on a sustainable basis;
- guarding the interests of the German security and criminal prosecution authorities; and
- promoting the strength of the market position of German producers of encryption systems.

The German Federal Government agreed to do without legal regulation of the free circulation and use of encryption products and processes in the current legislative period, which means that German users will retain their unrestricted freedom to choose and use the encryption systems they prefer. The Federal Government will continue to closely monitor developments in the field of cryptography technology, mainly within the context of European and international co-operation, and it will take further measures, where necessary, for implementing its objectives.

Greece

Export controls

Greece is a member of the Wassenaar Arrangement and the European Union.

Domestic controls and import regulations

There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in Greece.

Hungary

Export controls

Hungary is a member of the Wassenaar Arrangement.

Hungary has implemented export controls on cryptography technologies according to the Wassenaar dual-use list. The licensing authority is the Ministry of Economic Affairs.

Export of "generally available" software and public domain software and technology is exempted in Hungary.

Domestic controls and import regulations

Hungarian import controls require an import license in the same situations that export licenses are required. There are no domestic laws regulating the use of cryptography in Hungary.

Iceland

Export controls, domestic controls and import regulations

There are no domestic controls on the use of cryptography, nor are there export or import restrictions on cryptography technologies, currently in place in Iceland.

Ireland

Export controls

Ireland is a member of the Wassenaar Arrangement and the European Union.

The Irish export controls are implemented through the Control of Exports Act 1983 (No. 35 of 1983), the Control of Exports Order 1996 (SI No. 363 of 1996) which lists the military and paramilitary items subject to export licensing requirements, the European Communities (Control of Exports of Dual-Use Goods) Regulations 1996 (SI No. 362 of 1996) which provides penalties for breach of the EU Regulation and the Customs Act 1956 (No. 7 of 1956).

The authority responsible for licensing the export of cryptographic products in Ireland is the Export Licensing Unit of the Department of Enterprise, Trade and Employment.

The General Software Note has been implemented in Ireland following the wording of the Wassenaar Arrangement.

Domestic controls and import regulations

There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in Ireland.

Italy

Export controls

Italy is a member of the Wassenaar Arrangement and the European Union.

Italy has implemented the EU Dual-Use Regulations with regard to export of cryptography technologies. The authority responsible for licensing the export of cryptographic products (products listed in annex I of the 96/613/CUSP Decision of the EU Council) from Italy is the *Ministerio del commercio con l'estero* (Ministry of Foreign Trade). Authorisations are made pursuant to Article 2 of the Italian Law No. 89, 24 February, 1997.

The General Software Note is applied in Italy; software generally available to the public, or in the public domain, is not subject to authorisation and can be exported freely.

It is currently unclear whether Italy's export controls apply to both tangible and intangible exports of software.

Domestic controls and import regulations

Prior to Law No. 59 of 15 March 1997 and to Decree of the President of the Republic No. 513 of 10 November 1997, Italy did not enforce any special domestic controls on cryptography, except the legal provisions of Articles 12 and 24 of Law No. 801 of 24 October 1977 on the specific themes of the protection of state secrets and diffusion of information, the diffusion of which is prohibited. Some other provisions are contained in the various laws on the control, export, import and transit of armaments and on the export and transit of materials of particular strategic importance[37].

Cryptography technologies in the Public Administration were only briefly mentioned in some of the deliberations of the Authority for Information Technology in the Public Administration (AIPA)[38], such as the Deliberation of 28 July 1994 under Article 1, No. 9. This Deliberation states that issues related to the use of encryption, of the protection and conservation of the relevant keys and the use of electronic signature systems will be regulated by subsequent legal provisions.[39] It also sets out that every file stored in an optical disc should contain information about cryptography according to rules which would be subsequently defined.

As concerns security issues with respect to the specific techniques for the use of optical storage devices, the explanatory notes of the above Deliberation state that "for confidential reasons cryptography must be allowed for storage of information on disk, but in such a case the cryptography algorithm must be normalised and also the formation and conservation procedures of the single keywords and the relevant responsibilities must be governed by specific regulations."

Cryptography is also mentioned in the feasibility study on the Public Administration's Unitary Network (PAUN)[40]. This wide-ranging study also states that the security of the PAUN will be made through domains. In order to guarantee the origin, content, privacy and non-refusal of the messages exchanged by the domains there will be applications software based on the use of symmetric and/or public key cryptography. The management of the cryptography keys will be handled through a body which will be set up by and placed under the direct control of the Presidency of the Council of Ministers, composed of three distinct sections dealing with: (1) creation and distribution of the keys, located at the service centre; (2) management of notarial documents, located at the operation centre; and (3) certification of the keys, located at the Authority for Information Technology.

The general report also contains specific studies which make reference to the use of electronic signatures (as a guarantee of the integrity of the data and of the security of the message's origin) and to public key cryptography (ensuring the privacy of the data).

At the end of 1995 AIPA examined draft provisions on electronic legal and other documents in conformity with Article 3 of the Decree Law No. 39 of 3 February 1993. Since this text was the result of a study group, AIPA published it on the Internet to obtain public comments. This study also examines issues relating to the management and storage of cryptography keys.

In November 1996 AIPA presented the document, "Network of the automated information processing systems' Cabinets and Responsible Authorities", which also deals with the issues of network security and the use of cryptography.

Law No. 52 of 15 March 1997 also acknowledges the legal validity of computer documents. It delegates the government to legislate on the attribution of functions and tasks to the regions and local authorities with the reformation of the Public Administration and a simplification of administrative procedures. Specifically, it provides that "acts, data and documents made by the Public Administration and private parties through the use of computer and information-telecommunications systems, are legally valid and produce effects for all legal purposes."[41]

Pursuant to the above provision, the Decree of the President of the Republic No. 513 of 10 November 1997 was issued outlining Rules on the criteria for and ways of formulating, storing and transmitting document through computer and information-telecommunications systems. This Decree provides specific provisions for computer documents and their probative validity, and for digital signature and validation systems with reference to the use of cryptography (asymmetric key encryption systems), both in the private and in the public sectors.

Article 15 of Law No. 675 of 31 December 1996 on the Protection of individuals and other subjects with reference to personal data processing, deals with the problem of the security of data. It provides that the minimum standards of security to be adopted in a preventive way (including cryptography) will be defined in a set of rules to be issued in a Decree of the President of the Republic, upon proposal of the Minister of Justice, after consulting the AIPA and the Authority for the Protection of Data.

Japan

Export controls

Japan is a member of the Wassenaar Arrangement.

Japan has implemented export restrictions on cryptography products according to the Wassenaar Dual-Use List. The export of cryptographic products from Japan is regulated under the Foreign Exchange and Foreign Trade Law (Law No.228, 1949), the Foreign Exchange Order (Cabinet Order No.260, 1980), the Export Trade Control Order (Cabinet Order No.63, 1949) and the International Trade Administration Bureau Notification (No.492, 1992).

An export licence is required for all cryptographic products, and decisions on applications are, in principle, made on an individual basis by the licensing authority, the Ministry of International Trade and Industry (MITI). Streamlined procedures were introduced in February 1998 regarding products which are perceived as less sensitive, such as DVD devices, receivers of digital pay TV, etc.

Japanese export controls follow the text of the General Software Note; software that is generally available or in the public domain is excluded from the controls.

The Japanese export controls apply to both tangible and intangible exports of software.

Domestic controls and import regulations

There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in Japan.

General policy developments

The development of cryptography policy in Japan is generally focused in two Japanese Ministries: the Ministry of Posts and Telecommunications (MPT)[42] and the Ministry for International

Trade and Industry (MITI)[43]. Recently, the National Police Agency (NPA) and the Ministry of Justice have also taken a role in this area.

MITI published a paper in May 1997 "Towards the Age of the Digital Economy - For Rapid Progress in the Japanese Economy and World Economic Growth in the 21st Century"[44] presenting MITI's approach to electronic commerce issues generally. Cryptography is seen as an important tool for establishing information security in electronic commerce. Development of cryptography and investigative projects should be promoted, and network users should be provided with much more information about the various initiatives underway.

Since cryptography, which is important to prevent crimes related to computer networks, can also be misused to further various crimes, the NPA is considering a policy to promote cryptography and to prevent misuse of cryptography. The NPA has considered cryptography policy in co-operation with an extra-departmental body, and the extra-departmental body published a paper in February 1998.

The policy report "Vision 21 for Info-Communications", which was submitted by the Telecommunications Council to MPT in June 1997, pointed out that establishing security measures, such as encryption, is indispensable in order to create an environment for electronic commerce and electronic settlement over networks, and the development of cryptography technologies and cryptography policy needs to be promoted, along with international co-operation.

Korea

Export controls

Korea is a member of the Wassenaar Arrangement.

Korea has implemented controls on the export of cryptographic hardware and software in accordance with the Wassenaar provisions. Regulations on the export of cryptographic products are contained in the Public Notice on Export and Import of Strategic Goods which was issued pursuant to the Foreign Trade Act and its Decree. The licensing authority is the Ministry of Commerce, Industry and Energy.

The General Software Note is implemented in Korea in the Public Notice following the wording of the Wassenaar Arrangement; Korean export controls do not apply to software that is "in the public domain" or "generally available to the public".

Domestic controls and import regulations

There are no import restrictions on cryptography technologies into Korea. There are no domestic regulations specifically governing the use of cryptography by the private sector.

General policy developments

In 1998, the Ministry of Commerce, Industry and Energy and the Ministry of Justice jointly proposed a draft Act on Electronic Transactions which defines the use of cryptography technologies for electronic commerce in order to secure user and consumer confidence. The draft Act also states that the government might consider measures regarding lawful access when it is deemed necessary for national security.

In May 1998, the Ministry of Information and Communication (MIC) organised a working group composed of experts from industry, academia, and research institutes to study the domestic use of cryptography with a view to implementing the OECD Cryptography Policy Guidelines. The MIC is also working on measures to protect important information stored by public and private authorities by applying cryptography technologies and enhancing international co-operation for public key management.

Luxembourg

Export controls

Luxembourg is a member of the Wassenaar Arrangement and the European Union.

Luxembourg has implemented export controls on cryptographic hardware and software in accordance with the EU Dual-Use Regulations.

Domestic controls and import regulations

There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in Luxembourg.

Mexico

Export controls, domestic controls and import regulations

There are no domestic controls on the use of cryptography, nor are there export or import restrictions on cryptography technologies, currently in place in Mexico.

The Netherlands

Export controls

The Netherlands is a member of the Wassenaar Arrangement and the European Union.

Regulations in the Netherlands apply to the export of cryptographic software and hardware in compliance with the 1962 Law on Import and Export (Dutch statute-book 1962, 295) and its ensuing ministerial decision on export of strategic goods (Dutch statute-book 1963, 128).

The export of all cryptographic software and hardware from the Netherlands (except for specific banking applications) requires an export license. The administering authority is the Central Agency of Import and Export, under the authority of the Ministry of Economic Affairs. Once an application has been received, an evaluation and decision process (whether or not to issue an export license) is set in process. In practice, the products are evaluated on a case-by-case basis.

The Netherlands applies the General Software Note (GSN); the export of mass market and public domain software from the Netherlands does not require a licence. The language of the GSN is included in the text of the legal instruments for export control in the Netherlands and is applied by the export control authorities. The terms “substantial support” and “public domain” are given a strict interpretation by the export control authorities. In some cases exporters who themselves interpreted the GSN in a less strict manner have been corrected.

Currently the Dutch export control legislation concerns itself with tangible goods only. This includes software embedded in products or stored on disks, but it does not include intangible transmissions as a formal export.

Domestic controls and import regulations

There are no import restrictions on cryptography technologies in place in the Netherlands.

Regarding domestic regulations in the present Telecommunications Act, the use of cryptography on closed-terrestrial radio systems (not public mobile systems) is restricted and requires a license from the telecommunication regulator. In the proposed Telecommunications Act (approved in the first term of Parliament on 7 April 1998) this restriction is not mentioned.

As a result of the European Council Resolution on international requirements for the Lawful Interception of Telecommunications, the Dutch Telecommunications Act includes an obligation on network operators and service providers. They must provide the signal *en clair* when a legal warrant for interception is given.

Under the Dutch Computer Crime Act, in the case of stored data in encrypted form and a lawful authorisation, any applicable entity (excluding a suspect) is obligated to co-operate with the law enforcement authorities. This is to obtain lawful access to *en clair* data.

New Zealand

Export controls

New Zealand is a member of the Wassenaar Arrangement.

New Zealand implements the Wassenaar provisions through its national export controls: the Customs and Excise Act 1996 and the Customs Prohibition Order 1996. Exports of cryptography require a strategic export permit from the International Security & Arms Control division of the Ministry of Foreign Affairs and Trade (MFAT). All applications are considered on a case-by-case basis.

New Zealand export controls do not exclude cryptography “in the public domain” or “generally available to the public”.

At present the Customs & Excise Act applies only to exports of cryptography in a tangible form, such as a book, CD ROM or disk. There are, technically, no controls on the export of cryptography in an intangible (electronic) form. (But export would be specifically prohibited if it would contribute to a weapon of mass destruction programme.) This aspect of the Customs and Excise Act is currently being reviewed.

Domestic controls and import regulations

There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in New Zealand.

General policy developments

While no amendments to New Zealand’s domestic laws are currently being contemplated, they remain under continuous review to ensure that they take adequate account of technological and other developments.

A National Cryptography Policy Committee, chaired by the Department of the Prime Minister and Cabinet and comprised of agencies including Ministry of Commerce, MFAT, the Ministry of Justice, New Zealand Police and NZ Customs Service, has been formed to co-ordinate agency responsibilities such as strategic export controls and electronic signatures. The Ministry of Commerce is the lead NZ Government agency on matters of electronic commerce.

Norway

Export controls

Norway is a member of the Wassenaar Arrangement.

The export of cryptographic products from Norway is regulated under the Act of 18 December 1987, No 93, relating to the Export Control of Strategic Goods, Services, Technologies etc., Regulations of 10 January 1989 for the Implementation of the Export Control of Strategic Goods, Services, Technologies etc. and the List of Dual-Use Goods and Technologies. Export controls are administered by the Ministry of Foreign Affairs.

Norwegian law follows the exemption contained in the General Software Note of the Wassenaar Arrangement. In addition, Internet distribution is also considered a sufficient basis to apply the General Software Note.

Domestic controls and import regulations

There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in Norway.

General policy developments

The Norwegian Parliament passed an Act on Preventive National Security (*Lov om forebyggende sikkerhetstjenester mm* (*Sikkerhetsloven*), St.prp No 12 (1997-98)). The Act will be effective as soon as sub-regulations are ready, which is expected to be in Spring 1999. The Data Inspectorate (*Datatilsynet*) is expected to require encryption of sensitive personal data in external transmissions.

A report from the Norwegian IT Security Council recommends that cryptography policies be amended or established in the following prioritised areas: Public Administration, National Security, Justice sector, Health Care, Private interaction with Public Administration, Privacy and Trusted Third Party Services.

Poland

Export controls

Poland is a member of the Wassenaar Arrangement and intends to become a Member of the European Union.

An export license is required in Poland for exporting cryptographic software or hardware, in accordance with the EU Dual-Use Goods Regulation.

Domestic controls and import regulations

There are no domestic controls on the use of cryptography currently in place in Poland.

The import of cryptographic technology in Poland requires either a general authorisation or an import certificate.

Portugal

Export controls

Portugal is a member of the Wassenaar Arrangement and the European Union.

Portugal has implemented controls according to the EU Dual-Use Regulations. The licensing authority is the Directorate General for Commerce.

Domestic controls and import regulations

There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in Portugal.

Spain

Export controls

Spain is a member of the Wassenaar Arrangement and the European Union.

The export of cryptographic products is regulated in Spain by the *Real Decreto 491/1998 de 27 de marzo, por el que se aprueba el Reglamento del Comercio Exterior de Material de Defensa y de Doble Uso* (Official Journal of April 8th, 1998). This Decree implements the Wassenaar Arrangement and the EC Regulation. Cryptographic products are specifically quoted in Annex I.1 (11) and Annex II (12). They are also implicit in Annex I.1 (18), which includes the means (equipment and technology) to build them. The application and control of the Decree belongs to an Interministerial Committee (*Junta Interministerial Reguladora del Comercio Exterior de Material de Defensa y de Doble Uso),* chaired by the Secretary of State for Trade.

The Decree includes both a General Note on Technology (Annex I.1 *Nota general de tecnología*) and a General Software Note which translates the wording of the Wassenaar Arrangement (Annex I.2 (1)(d) *Nota general para el equipo lógico*).

Spanish export controls apply to both tangible and intangible exports of software.

Domestic controls and import regulations

There are no domestic controls on the use of cryptography in Spain. Article 52)(1) of the Telecommunications General Law [45] establishes the freedom to use any cryptographic programme or product to protect the interchange of data through telecommunication networks.

There are currently no restrictions on the import of cryptography technologies into Spain for use by private businesses. Controls apply only if the imported product or system, whether stand alone or integrated, is to be used in the national security domain. These controls are implemented by the *Centro Criptológico Nacional*, CESID, Ministry of Defence.

General policy developments

Although Article 52(2) of the Telecommunications General Law allows administrative control measures to be created through further specific regulations, there are no current developments in this area.

Sweden

Export controls

Sweden is a member of the Wassenaar Arrangement and the European Union.

The EU regulations and decisions have been implemented in Sweden by the Strategic Products Act (1991:341) and the Ordinance relating to Strategic Products (1994:2060). The licensing authority is the Inspectorate for Strategic Products (ISP).

The General Software Note has been implemented in Sweden following the wording of the Wassenaar Arrangement.

Domestic controls and import regulations

There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in Sweden.

General policy developments

The Swedish Cabinet Office is currently studying issues related to cryptography policy, and guidelines are being prepared.

In October 1997 a report was issued by the Swedish Cabinet Office on “Cryptography Policy: Possible Courses of Action for Sweden”. Although the report does not issue any formal suggestions on how to deal with the use and regulation of cryptography in society, it provides a synopsis of where and why the cryptography debate should begin. These starting points are listed below:

- Everybody has the right to use cryptography in order to secure communication and stored data.

- Import of cryptographic products to Sweden will continue to be unrestricted.

- Export controls of cryptography will remain.

- In order to facilitate the development of electronic commerce an initial set of rules should be developed for both the usage of digital signatures and the regulations of those institutions that are responsible for the issue of digital signature key certificates.

- A number of countries will introduce requirements for key deposition and court authorised access to plain text or confidential keys when criminal activities are suspected as a condition for export licenses for cryptographic products.

- Conditions must be created to enabline Swedish IT users to use Swedish key deposition facilities. Other countries are expected to require key deposition with international traffic, or as conditions when procuring products that are regulated by export controls.

- To enable Swedish law enforcement authorities to fight, for instance, terrorism and drug-traffic, certain legal provisions need to be established for lawful access to plain text and confidential keys.

- Necessary Swedish regulations in the area of cryptography will be introduced in co-operation with and in pace with international development.

Switzerland

Export controls

Switzerland is a member of the Wassenaar Arrangement.

The export of cryptographic hardware and software is regulated in Switzerland under the Federal Law on the Control of Goods Usable for Civilian and Military Purposes and Specific Military Goods (13 December 1996) and the Ordinance concerning the Export, Import and Transit of Dual Use Goods and Specific Military Goods (25 June 1997), both of which came into force on 1 October 1997. The licensing authority is the Federal Office of Foreign Economic Affairs.

The General Software Note (GSN) has been implemented in Switzerland in the Ordinance and follows the wording of the Wassenaar Arrangement. Switzerland takes a strict approach to paragraph (1)(b) of the GSN which requires that software be "designed for installation by the user without further substantial support by the supplier" before it can be considered "generally available to the public". In particular, if cryptography software is exported to a company which intends to make the software available to its customers without any substantial support, then the first part of this transaction requires an export licence even though the second step may fall within the GSN.

Swiss export controls apply to both tangible and intangible exports of software.

General licenses may be granted for export to designated destinations.

Domestic controls and import regulations

There are no import restrictions on cryptography technologies currently in place in Switzerland. There are no domestic regulations specifically governing the use of cryptography.

Turkey

Export controls

Turkey is a member of the Wassenaar Arrangement.

The export of dual-use goods is controlled in Turkey by the Undersecretariat for Foreign Trade (UFT) through the registration procedure contained in Article 3.a of the Export Regime Decree No. 95/7623 of 22 December 1995. Sensitive goods, technology and dual-use materials, including all cryptographic products (regardless of whether used for military purposes or not), must be registered with the Istanbul Metals and Minerals Exporters' Association (IMMIB) which notes this registration on the customs declaration. The registration procedures for goods covered by the international non-proliferation arrangements are carried out by the IMMIB under the auspices of the UFT. In addition, the export of cryptographic products used for military purposes are subject to the grant of a permit by the Ministry of National Defence (MND) under Law Number 3763 of 1940 regarding "The Control of Private Industrial Enterprises Producing War Weapons, Vehicles, Equipment and Ammunition".

The General Software Note has been implemented in Turkey following the wording of the Wassenaar Arrangement.

Turkish export laws apply only to software exported in a tangible form (for example, recorded on discs or similar media), and not to intangible goods, such as transfers over the Internet or other data networks.

Domestic controls and import regulations

There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in Turkey.

United Kingdom

Export controls

The United Kingdom is a member of the Wassenaar Arrangement and the European Union.

The export of cryptography technologies is controlled in the UK in accordance with the EU Dual-Use Regulation, implemented through the Export of Goods (Control) Order 1994 as amended by the Dual-Use and Related Goods (Export Control) Regulations 1996. The licensing authority is the Export Control Department of the Department of Trade and Industry (DTI)[46].

UK export controls follow the wording of the General Software Note; the controls do not apply to "generally available" software or software and technology in the "public domain". Exporters have access to an interpretative note providing "Guidance on the Interpretation of the General Software Note", and can make their own decisions on whether the exemption applies in a specific case, or they have the option of seeking advice from the DTI Export Control Department.

The export controls in the United Kingdom are applied to the export of tangible goods only, and exports of intangibles (for example, the supply of software by downloading from the Internet) are not covered.

Exporters must apply for a two year export license for any products using cryptography. In some circumstances the DTI will issue a more general Open Individual Export License, good for three years, which may contain specific conditions. All exporters must keep detailed records on the exports authorised by a license.

Applications for "Open Individual Export Licences" (OIELs) from exporters for encryption products which contain the 56-bit DES algorithm (or algorithms of an equivalent strength) are considered. Such OIELs will, depending on the individual circumstances, be limited in terms of the applicable country destinations, the type of end user, the specified use of the products and, inter-alia on any international discussions taking place on exports of cryptographic products. In addition, in line with the Government policy regarding Trusted Third Parties (TTPs), it may be appropriate, in certain circumstances, for the exporter to demonstrate that their products have (or will have) the capability to inter-work with licensed TTPs.

From 28 January 1998 the DTI has made available an "Open General Export Licence". The new licences permit, without further authority but subject to certain conditions, the export of goods which are not capable of on-line voice encryption or decryption which are designed to be used in conjunction with digital computers for personal use when accompanying their user.

Domestic controls and import regulations

There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in the United Kingdom.

General policy developments

A June 1996 DTI policy paper on provision of encryption services on public telecommunications networks states that export controls on encryption products (hardware or software) including digital encryption algorithms will remain in place in the UK, but that the Government, along with its EU partners, would try to simplify export controls for encryption products used by licensed TTP's. The Government would introduce legislation for licensing and regulating Trusted Third Parties (TTPs), with aims to preserve law-enforcement access to encrypted data. Prior to legislation, a consultation process with all interested parties would be held.

The consultation process was launched with a "Consultation Paper on Licensing of Trusted Third Parties for the Provision of Encryption Services"[47] issued by the Department of Trade and Industry (DTI) on 19 March 1997. The Consultation paper covered aspects of cryptography related to the licensing of TTPs, their use for confidentiality purposes, lawful access for confidentiality, legal recognition of digital signatures and international issues.

Following upon the results of the consultation, on 27 April 1998 DTI announced proposals for a Secure Electronic Commerce Bill. The Government aims to introduce legislation which will include: measures to promote the legal recognition of electronic signatures in electronic commerce; the introduction of a voluntary licensing regime for Trusted Third Parties (the generic term for bodies that provide one, or a variety of cryptography services to their clients), Certification Authorities (bodies which mainly issue certificates for electronic signatures), and Key Recovery Agents (responsible for facilitating the “recovery” of encrypted data); and measures to enable law enforcement agencies to obtain a warrant for lawful access to information necessary to decrypt the content of communications or stored data (this would not include cryptographic keys used solely for digital signatures purposes).

United States

Export controls

The United States (US) is a member of the Wassenaar Arrangement.

The export of non-military cryptographic hardware and software is administered in the US by the Bureau of Export Administration (BXA)[48] under the authority of the Department of Commerce. Cryptography technologies are covered by the Commerce Control List (CCL) under the Export Administration Regulations (EAR).

The current US export controls cover export licensing policies for different categories of encryption items, key escrow or key recovery products. (Recently announced changes to the US policy are discussed below). Under the current rules, certain mass-market encryption software may be made eligible for license exception treatment after a one-time BXA review. In addition, licence exceptions are available for export of key escrow and key recovery products to non-embargoed countries. Manufacturers which submit a key recovery commitment plan can also export non-recoverable 56-bit DES products under license exception. Other encryption items may be covered by licensing arrangements, or may be considered on a case-by-case basis. The licensing of “encryption technology” is considered on a case-by-case basis.

The US only implements Part 1 of the General Software Note of the Wassenaar Arrangement relating to "generally available" (i.e. mass market) software where the software uses specified algorithms having a key length of 40 bits or less (or equivalent proprietary algorithms) which have been approved after a one-time review. The US does not implement Part 2 relating to encryption software that is "in the public domain”. Part 734 of the EAR controls the export of encryption source code and object code software even if it is in the public domain. This is contrary to the practice of some other Wassenaar members.

Regarding the implementation of Part 1 of the General Software Note, an exporter submits a classification request for a one-time review per the instructions of Supplement No. 6 to Part 742 of the EAR. This request is reviewed for the technical parameters of the product as well as for determining whether the definition of the General Software Note is met, subject to the 40-bit cap. The wording of Part 1 of the GSN is included in the EAR.

In addition to the export of software in a tangible form, the US controls the export of encryption software in an intangible form (for example, distribution through the Internet).

The temporary export of cryptography products which are for personal use are exempt from export controls where certain EAR requirements are met[49].

Domestic controls and import regulations

There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in the United States.

General policy developments

Following several months of dialogue between the US Government, industry, the law enforcement community and privacy groups, on 16 September 1998 the US Administration announced a series of steps which will be taken to update its encryption policy[50]. As part of this initiative, the US Administration intends to support the establishment of a technical support center to help build the technical capacity of Federal, State and local law enforcement authorities to stay abreast of advancing communications technologies. The Administration will also strengthen its support for electronic commerce through the following steps:

- exports of 56-bit DES and equivalent products will be streamlined (under license exception, except for seven specified countries), and requirements for key recovery plans are eliminated;

- exports of unlimited strength encryption products (with or without key recovery) will be streamlined (under license exemption) to certain industries, including subsidiaries of US firms worldwide (except in seven specified countries), as well as insurance companies, civilian health and medical organisations, and online merchants / electronic commerce users in the 45 countries recently approved for exports of cryptography to banks and financial institutions;

- key recovery products will continue to be exportable under license exception worldwide (except to seven specified countries) and the review of foreign key recovery agents is eliminated; and

- exports of “recoverable” products will be approved to most commercial firms in the 45 countries recently approved for exports of cryptography to banks and financial institutions under encryption licensing arrangements.

Exports to end users or destinations which are not covered by this policy will continue to be reviewed on a case-by-case basis. Prior to export, all products are subject to a one-time technical review. The US Administration welcomes a continued dialogue with US industry and intends to review its policy in one year to determine if additional updates may be necessary to continue a balanced approach that protects the public safety and national security, ensures privacy, enables continued technology leadership by US industry and promotes electronic commerce.

The US Administration’s “Framework for Global Electronic Commerce” of July 1997[51] stated that “governments should encourage self-regulation ... and support the efforts of the private sector organisations to develop mechanisms to facilitate the successful operation of the Internet”. The government’s Framework for Global Electronic Commerce restates the (voluntary) key recovery approach. Administration officials have stated that the United States does not advocate any single product, technology, or even technical approach, but remains flexible -- provided that the resulting solutions and arrangements preserve the US’s ability to protect public safety and national security[52].

Other recent US initiatives related to cryptography policy include:

- in May 1997 National Institute of Standards and Technology began development of a Federal Information Processing Standard (FIPS) for public-key based cryptographic key agreement and exchange;[53]

- the National Research Council (NRC) published a study on “Cryptography’s Role in Securing the Information Society” (June 1996);

- the Office of Management and Budget (OMB) published a white paper on “Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure” (May 1996); and

- on 2 October 1996 a law was adopted which requires the US Sentencing Commission to report annually on the use of computer encryption in concealing criminal activity.

There are several pieces of proposed legislation currently at various stages of the law-making process, some seeking to impose domestic restrictions on the use of encryption technologies, others requiring mandatory or voluntary government key-recovery or key escrow provisions, and others seeking to permit free use and export of cryptography and cryptographic products:

- Computer Security Enhancement Act of 1997 (H.R.1903);

- Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act of 1997 (S.377);

- Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace (E-Privacy) Act (S.2067);

- Communications Privacy and Consumer Empowerment Act (H.R.1964);

- Encrypted Communications Privacy Act of 1997 (S.376);

- Secure Public Networks Act (S.909); and

- Security and Freedom Through Encryption (SAFE) Act (H.R.695).

There have been three separate court challenges to the US export regulations, claiming that the regulations violate the First Amendment of the US Constitution which protects free speech[54].

NOTES

[1] The Secretariat has consulted a variety of sources in preparing the preliminary draft of the Inventory which was provided to form a basis for further input from Member governments, including the *Crypto Law Survey* compiled by Bert-Jaap Koops (see *http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm*) and John Young's Cryptome Website (see *http://jya.com/crypto.htm*), and the Websites operated by the Global Internet Liberty Campaign (see *http://www.gilc.org/*), the Electronic Privacy Information Center (see *http://www.epic.org/*), and the Center For Democracy and Technology (see *http://www.cdt.org/*).

[2] OECD Recommendation of the Council concerning Guidelines for Cryptography Policy, 27 March 1997.

[3] DSTI/ICCP/REG(98)3/REV2.

[4] The 17 COCOM members were Australia, Belgium, Canada, Denmark, France, Germany, Greece, Italy, Japan, Luxembourg, The Netherlands, Norway, Portugal, Spain, Turkey, United Kingdom, and the United States. Co-operating members included Austria, Finland, Hungary, Ireland, New Zealand, Poland, Singapore, Slovakia, South Korea, Sweden, Switzerland, and Taiwan.

[5] Wassenaar Arrangement Members are: Argentina, Australia, Austria, Belgium, Bulgaria, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Poland, Portugal, Korea, Romania, the Russian Federation, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, Ukraine, the United Kingdom and the United States.

[6] Under-cuts should be notified preferably within 30 days, but not later than within 60 days: Wassenaar Arrangement, Initial Elements, Section II, paragraph 4.

[7] Denials of sensitive/very sensitive goods should be notified preferably within 30 days but not later than 60 days: Wassenaar Arrangement, Initial Elements, Section V, paragraph 3.

[8] See Appendix 5 of the “Initial Elements”, Wassenaar Arrangement.

[9] Listed in Annex 1 to the Dual-Use List.

[10] Listed in Annex 2 to the Dual-Use List.

[11] Regulation (EC) 3381/94 (OLJ 367/1, 31.12.94) and Decision 94/942/CFSP (OLJ 367/8, 31.12.94) of the Council of the European Union of 19 December 1994 set forth controls on the export of dual-use goods and established the list of dual-use goods which fall under the Regulation.

[12] See the notes to Annex 1 of Decision 96/613/CFSP (a completely new version of the Regulation is currently under consideration).

[13] European Council Resolution 96/C329/01.

[14] COM(97)503, see *http://www.ispo.cec.be/eif/policy/*.

[15.] See Council Directive 83/189/EEC (OJL 109, 26.4.83*)*.

[16.] See http://www.ispo.cec.be/policy.

[17.] (97/C 314/07) (Text with EEA relevance) COM(97)356 final.

[18.] Recommendation [R(95)13] of the Council of Europe, see *http://www.privacy.org/pi/intl_orgs/coe/info_tech_1995.htm.*

[19.] See the Bonn Declaration at *http://www.2.echo.lu/bonn/final.html.*

[20] The email contact point for the Australian Government with respect to cryptography issues is *crypto@ag.gov.au.*

[21.] See the Regulations at *http://www.austlii.edu.au/au/legis/cth/consol_reg/cer439/s13e.html.*

[22.] Cryptography is addressed under Part 3 Category 5 “Telecommunications & Information Security” of the Defence and Strategic Goods List. See the Australian Export Controls Website at http://www.defence.gov.au/dao/exportcontrols/.

[23.] For more practical information on export of cryptography technologies refer to the Guide “Australian Controls on the Export of Defence and Strategic Goods”. Document available at http://www.defence.gov.au/dao/exportcontrols/greenbk/guidelin.htm.

[24.] *Bundesministerium für wirtschaftliche Angelegenheiten*, Gruppe II/A, Stubenring 1, 1011 Wien, Austria.

[25.] Belgium has a Draft Law on Electronic Signatures. This is discussed in the OECD Inventory of Approaches to Authentication and Certification in a Global Networked Society.

[26.] Document available from the Industry Canada web site at *http://strategis.ic.gc.ca/crypto.*

[27.] Document available at *http://www.cse-cst.gc.ca/cse.*

[28.] Act No. 21/1997, Decree Number 43/1997.

[29.] See Act No. 21/1997.

[30.] Pursuant to Decree No. 44/1997 and § 16 of Act No. 21/1997.

[31] Executive Order No 468 of 13 June 1995.

[32.] See *http://www.fsk.dk/fsk/publ/1997/crypt/.*

[33.] This section of the inventory does not separate the discussion of export controls from the discussion of domestic controls and important regulations as the French laws deal with these issues together.

[34.] Central service for the security of information systems.

[35.] No. 96-659 of 26 July 1996. For a transcript of the law (in French) see the French Government site: *http://www.telecom.gouv.fr/francais/activ/telecom/nloi.htm.* For further information on the law from the French Government *http://www.telecom.gouv.fr/english/activ/telecom/.*

[36.] See *http://www.bmwi.de.*

[37.] Law no.185 of 8 July 1990, Law no. 222 of 27 February 1992 and the relevant ministerial decrees of 28 October 1993, 18 November 1993, 5 May 1994 and 1 September 1995.

[38.] The AIPA was created by Legislative Decree No. 39 of 12 February 1993.

[39.] Set out in Article 9, inter alia.

[40.] Provided for in the 5 September 1995 Directive of the President of the Council of Ministers, published in the Official Gazette [G.U.] no. 272 of 21 November 1995.

[41.] Article 15, paragraph 2.

[42.] See *http://www.mpt.go.jp.*

[43.] See *http://www.miti.go.jp.*

[44.] See *http://www.miti.go.jp/intro-e/a228101e.html.*

[45.] Law 11/98 of 24-04-1998, Official Journal of April 25th, 1998.

[46.] See the DTI web site at *http://www.dti.gov.uk.*

[47.] See *http://www.dtiinfo1.dti.gov.uk/pub.*

[48] See *http://www.bxa.doc.gov/.*

[49.] See EAR 15 CFR Part 740, License Exceptions 740.9 TMP (temporary imports, exports and re-exports) and 740.14 - BAG (baggage).

[50.] See *http://207.96.11.93/press/98/WHPress1.htm.*

[51.] See *http://www.whitehouse.gov.*

[52.] Testimony of Robert S. Litt, Principal Associate Deputy Attorney General, before the Subcommittee on the Constitution, Federalism, and Property Rights Committee on the Judiciary, United States, 17 March 1998.

[53.] See *http://csrc.nist.gov/.*

[54.] See Karn at *http://people.qualcomm.com/karn*, Bernstein at *www.eff.org*, and Junger at *http://jya.pdj.com.*

ANNEXES

ANNEX I: SUMMARY TABLE OF NATIONAL RESPONSES

Key:

Symbol	Meaning
*	Yes
?	Information has not been supplied by Member country

COUNTRY	WASSENAAR MEMBER	EU MEMBER	EXPORT CONTROLS	APPLICABLE LAWS	SUPERVISING AUTHORITY	APPLICATION OF THE GENERAL SOFTWARE NOTE	DIFFERENT TREATMENT FOR "TANGIBLE" AND "INTANGIBLE" SOFTWARE TRANSFERS?	DOMESTIC CONTROLS	IMPORT CONTROLS
Australia	*	No	*	Reg 13E of Customs (Prohibited Exports) Regulations; and the Defence and Strategic Goods List	Defence Signals Directorate of the Department of Defence	No	Undetermined	No	No
Austria	*	*	*	Section 8 of the *Außenhandelsgesetz* (BGBl. Nr. 172/1995)	Federal Ministry of Economic Affairs (*Bundesministerium für wirtschaftliche Angelegenheiten*)	* (incorporated by reference)	* (exports of intangibles not controlled)	* (in-house radio transmission)	No
Belgium	*	*	*	Law of 5 August 1991; Ministerial Decree of 19 May 1995; and Royal Decree of 8 March 1993	A.R.E., 4th Division	?	* (exports of intangibles not controlled)	No	No
Canada	*	No	*	Export and Import Permits Act; and the Export Control List	Department of Foreign Affairs and International Trade	*	No	No	No
Czech Republic	*	No	*	Control of Exports and Imports of Goods and Technologies Subject to International Control Regimes Act	Department of Industry and Trade	?	?	No	No

COUNTRY	WASSENAAR MEMBER	EU MEMBER	EXPORT CONTROLS	APPLICABLE LAWS	SUPERVISING AUTHORITY	APPLICATION OF THE GENERAL SOFTWARE NOTE	DIFFERENT TREATMENT FOR "TANGIBLE" AND "INTANGIBLE" SOFTWARE TRANSFERS?	DOMESTIC CONTROLS	IMPORT CONTROLS
Denmark	*	*	*	Executive Order on Exports of Dual-Use Goods Technologies and Know-how	Danish Agency for Trade and Industry	*	No	No	No
Finland	*	*	*	Control of Exports of Dual-Use Goods Act; Decree on Export of Dual-Use Goods; and Decision of the Ministry of Trade and Industry on export licensing of dual-use products (January 1997)	Ministry of Trade and Industry	*	No	No	No
France	*	*	*	Various laws, decrees and orders (see main text)	*Service Central de la Sécurité des Systèmes d'Information (SCSSI)*	No	No	*	*
Germany	*	*	*	?	Federal Ministry of Economics (BMWi)	?	?	No	No
Greece	*	*	*	?	?	?	?	No	No
Hungary	*	No	*	?	Ministry of Economic Affairs	?	?	No	*
Iceland	No	No	No	Not applicable	Not applicable	Not applicable	Not applicable	No	No
Ireland	*	*	*	Control of Exports Act 1983; Control of Exports Order (1996); European Communities (Control of Exports of Dual-Use Goods) Regulations (1996); and Customs Act (1956)	Export Licensing Unit of Department of Enterprise, Trade & Employment	*	?	No	No
Italy	*	*	*	Law no. 89, February 24, 1997	Ministry of Foreign Trade (Ministerio del commercio con l'estero)	*	Undetermined	*	No

COUNTRY	WASSENAAR MEMBER	EU MEMBER	EXPORT CONTROLS	APPLICABLE LAWS	SUPERVISING AUTHORITY	APPLICATION OF THE GENERAL SOFTWARE NOTE	DIFFERENT TREATMENT FOR "TANGIBLE" AND "INTANGIBLE" SOFTWARE TRANSFERS?	DOMESTIC CONTROLS	IMPORT CONTROLS
Japan	*	No	*	Foreign Exchange and Foreign Trade Law (No.228, 1949); Foreign Exchange Cabinet Order (No.260, 1980); Export Trade Control Cabinet Order (No.63, 1949); and International Trade Administration Bureau Notification (No.492, 1992)	Ministry of International Trade and Industry (MITI)	*	No	No	No
Korea	*	No	*	Public Notice on Export and Import of Strategic Goods	Ministry of Commerce, Industry and Energy	*	?	No	No
Luxembourg	*	*	*	?	?	?	?	No	No
Mexico	No	No	No	Not applicable	Not applicable	Not applicable	Not applicable	No	No
Netherlands	*	*	*	Law on Import and Export (Dutch statute-book 1962, 295); and the Ministerial Decision on Export of Strategic Goods (Dutch statute-book 1963, 128)	Central Agency of Import and Export under the Ministry of Economic Affairs	*	* (exports of intangibles not controlled)	* (related telecomms laws)	No
New Zealand	*	No	*	Customs and Excise Act 1996; and Customs Prohibition Order 1996	International Security & Arms Control Division under the Ministry of Foreign Affairs and Trade	No	* (exports of intangibles not controlled)	No	No

COUNTRY	WASSENAAR MEMBER	EU MEMBER	EXPORT CONTROLS	APPLICABLE LAWS	SUPERVISING AUTHORITY	APPLICATION OF THE GENERAL SOFTWARE NOTE	DIFFERENT TREATMENT FOR "TANGIBLE" AND "INTANGIBLE" SOFTWARE TRANSFERS?	DOMESTIC CONTROLS	IMPORT CONTROLS
Norway	*	No	*	Act relating to the Export Control of Strategic Goods, Services, Technologies etc; Regulations for the Implementation of the Export Control of Strategic Goods, Services, Technologies etc; and List of Dual-Use Goods & Technologies	Ministry of Foreign Affairs	*	?	No	No
Poland	*	No	*	?	?	?	?	No	* (authorisation required)
Portugal	*	*	*	?	Directorate General for Commerce	?	?	No	No
Spain	*	*	*	*Real Decreto por el que se aprueba el Reglamento del Comercio Exterior de Material de Defensa y de Doble Uso*	*Junta Interministerial Reguladora del Comercio Exterior de Material de Defensa y de Doble Uso*	*	*	No	* (controls on technologies to be used in the national security domain)
Sweden	*	*	*	Strategic Products Act; and the Ordinance relating to Strategic Products	Inspectorate for Strategic Products	*	?	No	No
Switzerland	*	No	*	Federal Law on the Control of Goods Unable for Civilian & Military Purposes & Specific Military Goods; and Ordinance on the Export, Import & Transit of Dual Use Goods & Specific Military Goods	Federal Office of Foreign Economic Affairs	*	No	No	No

COUNTRY	WASSENAAR MEMBER	EU MEMBER	EXPORT CONTROLS	APPLICABLE LAWS	SUPERVISING AUTHORITY	APPLICATION OF THE GENERAL SOFTWARE NOTE	DIFFERENT TREATMENT FOR "TANGIBLE" AND "INTANGIBLE" SOFTWARE TRANSFERS?	DOMESTIC CONTROLS	IMPORT CONTROLS
Turkey	*	No	*	Law regarding the Control of Private Industrial Enterprises Producing War Weapons, Vehicles, Equipment & Ammunition; and Article 3.a of the Export Regime Decree	Ministry of National Defence; and Undersecretariat for Foreign Trade	*	*	No	No
UK	*	*	*	Export of Goods (Control) Order as amended by the Dual-Use and Related Goods (Export Control) Regulations	Export Control Department under the Department of Trade and Industry	*	* (exports of intangibles not controlled)	No	No
United States	*	No	*	Export Administration Regulations; and the Commerce Control List	Bureau of Export Administration under the Department of Commerce	* (the US partially applies the GSN by imposing a 40-bit cap)	No	No	No

ANNEX II: THE WASSENAAR ARRANGEMENT (Excerpts only)

The Wassenaar Arrangement

on

Export Controls for Conventional Arms and

Dual-Use Goods and Technologies

Final Declaration

1. Representatives of Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Poland, Portugal, the Russian Federation, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States met in Wassenaar, the Netherlands, on 18 and 19 December 1995.

2. The representatives agreed to establish The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.

3. The representatives established initial elements of the new arrangement, to be submitted to their respective Governments for approval.

4. They also established a Preparatory Committee of the Whole to start work in January 1996.

5. The representatives agreed to locate the Secretariat of The Wassenaar Arrangement in Vienna, Austria. The first plenary meeting will take place in Vienna on 2 and 3 April 1996.

The Peace Palace in The Hague, the Netherlands, on 19 December 1995.

Initial Elements

(Excerpts Only)

As adopted by the Plenary of 11 - 12 July 1996

I. **Purposes**

1. The *Wassenaar Arrangement* has been established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations. Participating States will seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities.

2. It will complement and reinforce, without duplication, the existing control regimes for weapons of mass destruction and their delivery systems, as well as other internationally recognised measures designed to promote transparency and greater responsibility, by focusing on the threats to international and regional peace and security which may arise from transfers of armaments and sensitive dual-use goods and technologies where the risks are judged greatest.

3. This arrangement is also intended to enhance co-operation to prevent the acquisition of armaments and sensitive dual-use items for military end-uses, if the situation in a region or the behaviour of a state is, or becomes, a cause for serious concern to the Participating States.

4. This arrangement will not be directed against any state or group of states and will not impede bona fide civil transactions. Nor will it interfere with the rights of states to acquire legitimate means with which to defend themselves pursuant to Article 51 of the Charter of the United Nations.

II. **Scope**

1. Participating States will meet on a regular basis to ensure that transfers of conventional arms and transfers in dual-use goods and technologies are carried out responsibly and in furtherance of international and regional peace and security.

2. To this end, Participating States will exchange, on a voluntary basis, information that will enhance transparency, will lead to discussions among all Participating States on arms transfers, as well as on sensitive dual-use goods and technologies, and will assist in developing common understandings of the risks associated with the transfer of these items. On the basis of this information they will assess the scope for co-ordinating national control policies to combat these risks. The information to be exchanged will include any matters which individual Participating States wish to bring to the attention of others, including, for those wishing to do so, notifications which go beyond those agreed upon.

3. The decision to transfer or deny transfer of any item will be the sole responsibility of each Participating State. All measures undertaken with respect to the arrangement will be in accordance with national legislation and policies and will be implemented on the basis of national discretion.

4. In accordance with the provisions of this arrangement, Participating States agree to notify transfers and denials. These notifications will apply to all non-participating states. However, in the light of the general and specific information exchange, the scope of these notifications, as well as their relevance for the purposes of the arrangement, will be reviewed. Notification of a denial will not impose an obligation on other Participating States to deny similar transfers. However, a Participating State will notify, preferably within 30 days, but no later than within 60 days, all other Participating States of an approval of a licence which has been denied by another Participating State for an essentially identical transaction during the last three years.

5. Upon the commencement of this arrangement, Participating States agree that work on further guidelines and procedures will continue expeditiously and taking into account experience acquired. This will include, in particular, a review of the scope of conventional arms to be covered with a view to extending information and notifications beyond the categories described in Appendix 3. Participating States agree to discuss further how to deal with any areas of overlap between the various lists.

6. Participating States agree to assess the overall functioning of this arrangement regularly, for the first time in 1999.

III. **Control Lists**

1. Participating States will control all items set forth in the List of Dual-Use Goods and Technologies and in the Munitions List (see Appendix 5), with the objective of preventing unauthorised transfers or re-transfers of those items.

2. The List of Dual-Use Goods and Technologies (tier 1) has two annexes of sensitive (tier 2) and a limited number of very sensitive items (sub-set tier 2).

3. The lists will be reviewed regularly to reflect technological developments and experience gained by Participating States, including in the field of dual-use goods and technologies which are critical for indigenous military capabilities. In this respect, studies shall be completed to coincide with the first revision to the lists to establish an appropriate level of transparency for pertinent items.

IV. **Procedures for the General Information Exchange**

1. Participating States agree to exchange general information on risks associated with transfers of conventional arms and dual-use goods and technologies in order to consider, where necessary, the scope for co-ordinating national control policies to combat these risks.

2. A list of possible elements of the general information exchange on non-participating states is contained in Appendix 1.

V. **Procedures for the Exchange of Information on Dual-Use Goods and Technology**

1. Participating States will notify licences denied to non-participants with respect to items on the List of Dual-Use Goods and Technologies, where the reasons for denial are relevant to the purposes of the arrangement.

2. For tier 1, Participating States will notify all licences denied relevant to the purposes of the arrangement to non-participating states, on an aggregate basis, twice per year. The indicative content of these denial notifications is described in Appendix 2.

3. For items in the second tier and its sub-set of very sensitive items, Participating States will notify, on an individual basis, all licences denied pursuant to the purposes of the arrangement to non-participating states. Participating States agree that notification shall be made on an early and timely basis, that is preferably within 30 days but no later than within 60 days, of the date of the denial. The indicative content of these denial notifications is described in Appendix 2.

4. For items in the second tier, Participating States will notify licences issued or transfers made relevant to the purposes of the arrangement to non-participants, on an aggregate basis, twice per year. The indicative content of these licence/transfer notifications is described in Appendix 2.

5. Participating States will exert extreme vigilance for items included in the sub-set of tier 2 by applying to those exports national conditions and criteria. They will discuss and compare national practices at a later stage.

6. Participating States agree that any information on specific transfers, in addition to that specified above, may be requested *inter alia* through normal diplomatic channels.

VI. **Procedures for the Exchange of Information on Arms**

...

VII. **Meetings and Administration**

1. Participating States will meet periodically to take decisions regarding this arrangement, its purposes and its further elaboration, to review the lists of controlled items, to consider ways of co-ordinating efforts to promote the development of effective export control systems, and to discuss other relevant matters of mutual interest, including information to be made public.

2. Plenary meetings will be held at least once a year and chaired by a Participating State on the basis of annual rotation. Financial needs of the arrangement will be covered under annual budgets, to be adopted by Plenary Meetings.

3. Working Groups may be established, if the Plenary meeting so decides.

4. There will be a secretariat with a staff necessary to undertake the tasks entrusted to it.

5. All decisions in the framework of this arrangement will be reached by consensus of the Participating States.

VIII. **Participation**

The new arrangement will be open, on a global and non-discriminatory basis, to prospective adherents that comply with the agreed criteria in Appendix 4. Admission of new participants will be based on consensus.

IX. **Confidentiality**

Information exchanged will remain confidential and be treated as privileged diplomatic communications. This confidentiality will extend to any use made of the information and any discussion among Participating States.

Appendix 5

List of Dual-Use Goods and Technologies and Munitions List

(Excerpts Only)

SUBMITTED TO THE PLENARY MEETING IN VIENNA

11th and 12th July, 1996

These lists reflect the agreements recorded in Appendix 5 to the Initial Elements dated 19th December, 1995, and appropriate drafting changes agreed by the Drafting Group on the 16th March, 1996.

Category 2 of Annex 1 reflects the amendments of the Plenary Meeting dated 2nd and 3rd April, 1996.

DUAL-USE LIST

Note Terms in "quotations" are defined terms. Refer to 'Definition 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

2. "In the public domain".

CATEGORY 5 - PART 2 - "INFORMATION SECURITY"

Part 2 - "INFORMATION SECURITY"

Note *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.*

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.

1. Designed or modified to use "cryptography" employing digital techniques to ensure "information security";

2. Designed or modified to perform cryptanalytic functions;

3. Designed or modified to use "cryptography" employing analogue techniques to ensure "information security";

Note 5.A.2.a.3. does not control the following:

1. Equipment using "fixed" band scrambling not exceeding 8 bands and in which the transpositions change not more frequently than once every second;

2. Equipment using "fixed" band scrambling exceeding 8 bands and in which the transpositions change not more frequently than once every ten seconds;

3. Equipment using "fixed" frequency inversion and in which the transpositions change not more frequently than once every second;

4. Facsimile equipment;

5. Restricted audience broadcast equipment;

6. Civil television equipment.

4. Designed or modified to suppress the compromising emanations of information-bearing signals;

Note 5.A.2.a.4. does not control equipment specially designed to suppress emanations for reasons of health and safety.

5. Designed or modified to use cryptographic techniques to generate the spreading code for "spread spectrum" or the hopping code for "frequency agility" 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. "Personalized smart cards" or specially designed components therefor, with any of the following characteristics:

1. Not capable of message traffic encryption or encryption of user-supplied data or related key management functions therefor; or

2. When restricted for use in equipment or systems excluded from control under entries 1. to 6. of the Note to 5.A.2.a.3. or under entries b. to h. of this Note;

b. Equipment containing "fixed" data compression or coding techniques;

c. Receiving equipment for radio broadcast, pay television or similar restricted audience television of the consumer type, without digital encryption and where digital decryption is limited to the video, audio or management functions;

d. 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;

e. Decryption functions specially designed to allow the execution of copy-protected "software", provided the decryption functions are not user-accessible;

f. Access control equipment, such as automatic teller machines, self-service statement printers or point of sale terminals, which protects password or personal identification numbers (PIN) or similar data to prevent unauthorized access to facilities but does not allow for encryption of files or text, except as directly related to the password or PIN protection;

g. Data authentication equipment which calculates a Message Authentication Code (MAC) or similar result to ensure no alteration of text has taken place, or to authenticate users, but does not allow for encryption of data, text or other media other than that needed for the authentication;

h. Cryptographic equipment specially designed and limited for use in machines for banking or money transactions, such as automatic teller machines, self-service statement printers or point of sale terminals.

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 specified in 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" specified in 5.E.2.;

c. Specific "software", as follows:

1. "Software" having the characteristics, or performing or simulating the functions of the equipment specified in 5.A.2. or 5.B.2.;

2. "Software" to certify "software" specified in 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.

DEFINITIONS OF TERMS USED IN THESE LISTS

(Excerpts only)

This document contains the definitions of the terms used in these Lists, in alphabetical order.

Note *Definitions apply throughout the Lists and their Annexes. The references are purely advisory and have no effect on the universal application of defined terms throughout these Lists and their Annexes.*

Category references are given in brackets after the defined term.

"Cryptography" (5)

The discipline which embodies principles, means and methods for the transformation of data in order 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) or associated key management.

N.B. *'Secret parameter': a constant or key kept from the knowledge of others or shared only within a group.*

"Digital computer" (4, 5)

Equipment which can, in the form of one or more discrete variables, perform all of the following:

a. Accept data;

b. Store data or instructions in fixed or alterable (writable) storage devices;

c. Process data by means of a stored sequence of instructions which is modifiable; *and*

d. Provide output of data.

N.B. *Modifications of a stored sequence of instructions include replacement of fixed storage devices, but not a physical change in wiring or interconnections.*

"Fixed" (5)

The coding or compression algorithm cannot accept externally supplied parameters (e.g. cryptographic or key variables) and cannot be modified by the user.

"Information security" (5)

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", 'cryptanalysis', protection against compromising emanations and computer security.

N.B. *'Cryptanalysis': analysis of a cryptographic system or its inputs and outputs to derive confidential variables or sensitive data, including clear text.*

"In the public domain" (GTN, GSN)

This means "technology" or "software" which has been made available without restrictions upon its further dissemination.

N.B. *Copyright restrictions do not remove "technology" or "software" from being "in the public domain".*

"Personalized smart card" (5)

A smart card containing a microcircuit, in accordance with ISO/IEC 7816, which has been programmed by the issuer and cannot be changed by the user.

"Programme" (2, 4, 5, 6)

A sequence of instructions to carry out a process in, or convertible into, a form executable by an electronic computer.

"Required" (5, 6, 9, GTN)

As applied to "technology" or "software", refers to only that portion of "technology" or "software" which is peculiarly responsible for achieving or extending the controlled performance levels, characteristics or functions. Such "required" "technology" or "software" may be shared by different goods.

"Software" (Both Lists)

A collection of one or more "programmes" or "microprogrammes" fixed in any tangible medium of expression.

"Source code" (or source language) (4, 5, 6, 7, 9)

> *A convenient expression of one or more processes which may be turned by a programming system into equipment executable form ("object code" (or object language)).*

"Technology" (GTN & Both Lists)

Specific information necessary for the "development", "production" or "use" of a product. This information takes the form of technical data or technical assistance. Controlled "technology" is defined in the General Technology Note and in the Dual-Use List.

N.B. 1 "Technical data" may take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read-only memories.

N.B. 2 "Technical assistance" may take forms such as instructions, skills, training, working knowledge and consulting services and may involve the transfer of 'technical data'.

STATEMENTS OF UNDERSTANDING AND VALIDITY NOTES

(Excerpts Only)

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.

Category 5, Part 2

Validity Note

> *The control in 5.A.2.a.1. will remain in effect for a period of 2 years after the date of entry into force of the List of Dual-Use Goods and Technologies, and its renewal in its present form will require unanimous consent.*

N.B. In the event of a normal List Review of Category 5 - Part 2 occurring prior to the expiration of this Validity Note, any result of the List Review will override this Validity Note.