

In Print

Canadian Export Controls

by Brent Jay

PricewaterhouseCoopers LLP

Presented at the *CICA 2008 Commodity Tax Symposium*

An overview of Canada's export control program with a particular focus on controls which apply to software, electronics and other technology offerings.

For more information, please contact:

Brent Jay

brent.jay@ca.pwc.com

Alastair Moran

alastair.g.moran@ca.pwc.com

Presented September 2008.

Copyright remains with the author.

"PricewaterhouseCoopers" refers to PricewaterhouseCoopers LLP, Canada, an Ontario limited liability partnership. PricewaterhouseCoopers LLP, Canada, is a member firm of PricewaterhouseCoopers International Limited.

Contents

Overview of Paper

Part I: Overview of Canada's Export Controls Program

- A. Basic structure of the *Export and Import Permits Act*
- B. What steps should be taken if your item is on the export or area control lists?
- C. What happens if an exporter does not have a permit?
- D. Statutory Penalties and Offences
- E. Other Forms of Penalties

Part II: The Export Control List

- A. Overview of the List
- B. Groups 2 to 4 and Groups 6 and 7
- C. Group 5: Miscellaneous Goods
- D. Group 1: The Dual-Use List
 - (i) Background
 - (ii) Categories 1 through 9
 - (iii) Overview of Part 2 of Category 5 (information security)
 - (iv) Overview of encryption
 - (v) structure and contents of Part 2 of Category 5

Appendix A: Information to be provided in an application for permit

Overview of Paper

This paper is intended to provide an overview of Canada's export controls program which is a program that applies to certain goods, electronic offerings (including software) and in some cases services or even specific knowledge possessed by a particular individual.

This paper is divided into two distinct parts. Part I discusses the structure and administration of Canada's export controls program. This includes an overview of the *Export and Import Permit Act*, which contains the bulk of Canada's export laws. Part I also canvasses a number of practical issues relating to specific control measures and relating to export control compliance. Finally, Part I canvasses the wide range of penalties and offences associated with breaches of Canada's export control laws. In addition to penalties and offences which are statutory in nature this section also canvasses a number of unusual sanctions which do not have any statutory basis.

Part II of the paper discusses the actual export control list (which is actually a series of 8 lists) including its structure, organization and contents. By discussing patterns in the manner in which the lists are organized the objective is to provide practical guidance for exporters so that they may be in a better position to assess whether their particular exports are controlled. The Part II discussion focuses in particular upon two particularly contentious lists. The group 5 list (which relates to Miscellaneous Goods) is discussed in a higher degree of detail. Similarly, the group 1 (Dual Use List) list and each of its 9 categories will be discussed in a higher degree of detail but with a particular focus on the portions of the group 1 list which relate to information security (i.e., Part 2 of Category 5 of Group1). This special focus has been provided because the control of information security items poses a number of distinct and challenging export control issues.

Part I: Overview of Canadian Export Controls

A. Basic structure of the *Export and Import Permits Act*

The *Export and Import Permits Act* (the “EIPA”) provides the foundation for much of Canada’s export control laws.¹ The EIPA establishes basic mechanisms and procedures to be followed in connection with the export from Canada of goods (including electronic offerings supplied by way of the Internet or by means of some other telecommunications channel) or technology (which may even include knowledge possessed by a particular individual which is to be disseminated through training, consulting or otherwise).

The EIPA does not however specifically designate those goods or technologies which are subject to export control. Rather the EIPA delegates that function to the “Governor in Council” (referred to throughout this paper as the “GIC”) so that export control lists may be established, and updated as required by way of regulation. In fact the EIPA authorizes the GIC to establish the following two discrete control lists:

- (a) an area control list; and
- (b) an export control list.

The area control list² contains the name of countries to which no goods or technology (regardless of their nature) may be exported unless an export permit has previously been granted. At this time the only two countries which are listed on the area control list (see SOR/81-543) are Belarus and Myanmar. However, this list may be updated at any time. As a result exporters are cautioned that they should ensure that they have a mechanism in place to track any such changes as they occur.

The EIPA establishes the authority of the GIC to create an export control list. Unlike the area control list (which is country specific and product neutral) the export control list is, as a general rule, product specific (and for the most part, country neutral).

The broadly worded mandate of the GIC is to list any “goods and technology” which it deems necessary to control for one or more of the legislatively enumerated purposes.³ The EIPA lists several broad categories of enumerated purposes. The first, and arguably most important category of purposes relates to goods which by their very nature could (if they should fall into the wrong hands) be “detrimental to the security of Canada.” The types of goods to be controlled include obviously dangerous items such as “arms, ammunition, implements or munitions of war.” However, any other goods which might “otherwise have a strategic value or nature” and which might be “detrimental to the security of Canada” may also be controlled. This “purpose test” provides the GIC with a very broad authority to list (and control the export of) a broad range of goods.

The GIC is also provided with the authority to list items on the export control list for the purpose of satisfying an agreement or other commitment which Canada has entered into with either a single nation (for example, the United States) or with a number of other countries (for example the *Wassenaar Arrangement on Export Controls on Conventional Arms and Dual Use Goods and Technologies* which Canada has entered into along with 39 other nations). The GIC may also include an item in the export control list in order to ensure that there is an adequate supply of that item in Canada for defence purposes.

1 Other legislation may also apply in respect of the export of goods including for example the *Cultural Property Export Regulations* promulgated under the *Customs Act*.

2 The authority to create an area control list is established by section 4 of the EIPA.

3 Section 3 of the EIPA.

However, there are a number of purposes for which items may be listed which are not in any way connected to matters of defence or national security. For example, in order to give effect to other economic or social policies export control measures may be implemented for any of the following purposes:

- (a) for the purpose of encouraging the further processing within Canada of natural resources;
- (b) for the purpose of limiting or keeping under surveillance the export of raw or processed materials that are produced in Canada; or
- (c) to ensure the orderly export marketing of certain goods that are subject to import limitations in the destination country.

Given the broad range of purposes for which items may be listed it should hardly be surprising that the export control list imposes controls over the export of items as diverse as “pancreas glands of cattle,” “red cedar” products which are suitable for use in the manufacture of shakes or shingles, and certain “roe herring” (see *Export Control List* - Group 5 – Miscellaneous Goods).

It is beyond the scope of this paper to try to canvass all of the items which are contained in the export control list. However, in Part II of this paper every effort will be made to outline the structure of the various export control lists and to hi-lite those control items which are most commonly overlooked by exporters.

B. What steps should be taken if your item is on the export or area control lists?

Where an item (i.e., goods or technology) which is to be exported is contained within the export control list or the item, by virtue of its proposed destination is contained within the area control list, a permit must be relied upon in order to proceed with the export. This permit is issued by *The Export Controls Division* (“TIE”) of the *Department of Foreign Affairs* (“DFAIT”).

However, even where an item is controlled there may not be any requirement to apply for a permit. The exporter of a controlled item should first consider whether a “general export permit” is already available. General permits are permits which are already in existence and are available generally to “all residents of Canada.” The terms and conditions of the permit will be contained in the order under which the permit was passed.⁴ It is only where a general export permit is not available that an individual export permit (i.e., the type that is specifically applied for) will be required to be obtained.

A typical general export permit is the “*Export of Goods for Special and Personal Use Permit*” (General Export Permit No. 1). GEP 1 allows for a Canadian resident to export to any country (other than those countries listed on the area control list) certain personal and/or settler’s effects or other low value goods. The exact terms and conditions associated with the use of GEP 1 are contained within that general permit.

Notwithstanding that general export permits are already in existence and are available to all Canadians, from a procedural perspective it is important that the exporter properly reference the general export permit on their export declarations (i.e., for example, form B-13A or CAED). This is because a failure to properly reference the general export permit is an offence under the *Customs Act*.

In circumstances where no general export permit is available for a proposed export an individual export permit will be required to be obtained from TIE. In applying for an individual export permit it should be noted that:

- (a) export control permits are not granted as of right. In fact TIE is entitled to (and regularly does exercise its authority to) refuse to issue a permit. The power to refuse to issue a permit is discussed in more detail below;

⁴ The authority to create a general permit to be available for all residents of Canada is contained in subsection 7(1.1) of the EIPA.

(b) even where an export permit is issued it may take a period of weeks (or even months) to be provided with the permit; and

(c) even where an export permit is issued it may contain a number of stringent terms and conditions to be adhered to in connection with the export.⁵

The information which must be provided in an application for an export permit is summarized in Appendix A to this paper.

The powers of the Minister to refuse to issue an export permit are very broad. When considering whether to issue a permit the Minister is specifically directed to consider whether the goods or technology set out in the application “may”⁶ be used for a purpose which is prejudicial to:⁷

“the safety or interests of the state by being used to do anything referred to in paragraphs 3(1)(a) to (n) of the *Security of Information Act*”

As a preliminary matter the cross reference to the *Security of Information Act* (which is extremely powerful anti-terrorism legislation) underscores the significance of the EIPA as being, by implication, central to matters of national security. The cross referenced portions of the *Security of Information Act* establish that a purpose will be considered to be “prejudicial to the safety or interests of the state” (and thus grounds for refusal of a permit) if a person:

- (a) commits, inside or outside Canada, a terrorist activity;
- (b) causes or aggravates an urgent and critical situation in Canada that
 - (i) endangers the lives, health or safety of Canadians, or
 - (ii) threatens the ability of the GIC to preserve the sovereignty, security or territorial integrity of Canada
- (c) interferes with a service, facility, system or computer program, whether public or private, or its operation, in a manner that has significant adverse impact on the health, safety, security or economic or financial well being of the people of Canada or the functioning of any government in Canada; or
- (d) impairs or threatens the capabilities of the Government of Canada in relation to security and intelligence

In addition to the grounds for refusal as set out above, many exporters may be surprised to learn that an export permit may be refused where the export in issue may not be expected to pose any risk within Canada. The EIPA establishes that the Minister may refuse to issue an export permit where the goods or technology in issue may be used for a purpose which is prejudicial to:

“...peace, security or stability in any region of the world or within any country”⁸

It follows from the above that exporters must be prepared to consider the potential impact of their particular product or technology offering both within Canada and in other parts of the world.

Apart from the geographical issues noted above exporters should also note that the threshold test to be considered by the Minister in deciding whether to issue a permit has been set at a fairly low level. For example, the EIPA establishes that if a goods or technology “may” be used for any one of the prejudicial

5 See EIPA ss. 7(1.01).

6 The suggestion seems to be that a mere possibility that an item may be used for an offensive purpose will be sufficient grounds for refusal to issue a permit.

7 See EIPA section 7(1.01).

8 Paragraph 7(1.01)(b) of the EIPA.

purposes then the permit may be refused. The suggestion is that even where the particular threat or risk may be remote the Minister is within its discretion to withhold the permit.

Several other legislative provisions further reinforce that the Minister has considerable discretion to refuse to issue an export permit. For example, subsection 7(1.01) of the EIPA states that the Minister, in determining whether a permit should be issued, may have regard to "...any ... matter that the Minister may consider." Given this broad legislative direction it would be difficult to challenge any Ministerial decision to refuse to issue a permit.

C. What happens if an exporter does not have a permit?

As noted above, where an export permit is not issued (for controlled items) then the EIPA prohibits any person from exporting or transferring, or attempting to export or transfer the controlled goods.⁹

Notwithstanding this seemingly unequivocal language some exporters of controlled products choose to "export first and ask questions (or ask for permission) later." The rationale seems to be that obtaining export clearance is largely an administrative nuisance. Some exporters have even noted that the EIPA seems to contain "built in" curing provisions for situations where permits were not obtained in a timely manner. For example, section 14.1 of the EIPA states that there is no contravention of section 13 of the EIPA if:

"...at the time of exportation...the person would have exported...the goods under the authority of and in accordance with an export permit...issued under this Act had they applied for it and if after, after the exportation....the permit is issued"

At first blush this section seems to be capable of curing a broad range of export control deficiencies. However, any exporter who intends to rely on this provision to export without a permit should consider the following:

- (a) section 14.1 will not provide relief if a permit was applied for and refused; and
- (b) section 14.1 will not provide relief if an application for a permit was filed prior to export even if the permit is ultimately granted (i.e., after the export has occurred).

Accordingly, it would appear that the only circumstance where an exporter *might* be entitled to rely upon section 14.1 for relief purposes would be where the exporter did not apply for an export permit (i.e., where the exporter did not know that the goods were controlled).

In those circumstances the relief will only be available where the Minister subsequently determines (in its sole discretion) that granting the permit would be appropriate. Further, section 14.1 will only apply to provide relief if the export permit which is ultimately granted contains terms and conditions which correspond with the manner in which the export actually transpired. Achieving this level of alignment may be more difficult than exporters might imagine particularly given that the Minister typically does not look favourably upon those who ignore or contravene the EIPA.

D. Statutory Penalties and Offences

As a preliminary matter it should be noted that while the EIPA is largely administered by DFAIT (TIE branch) the *Canada Border Services Agency* (or "CBSA") is responsible for enforcing the EIPA. DFAIT and CBSA also rely on a number of other government agencies to support its administration and enforcement of the EIPA including the *Department of National Defence*, the *Royal Canadian Mounted Police* and the *Communications Security Establishment* (the "CSE").

The CBSA's authority even extends to export matters relating to the "export" of electronic offerings (including products exported by way of the Internet) or to controlled information exported as knowledge

⁹ See s. 13 EIPA.

held by individuals. It may come as a surprise to many that the CBSA (undoubtedly with the assistance of the CSE) does in fact monitor emails and other electronic transmissions which exit Canada (in a manner similar to the United States *National Security Agency*).

The wide variety of severe penalties which may apply for breaches of the EIPA or for corresponding export control related breaches of the *Customs Act* underscores the importance of the EIPA. The first category of penalties are those which are levied under AMPS (the *Administrative Monetary Penalty System*). It is quite common for breaches of the EIPA to result in the levying of AMPS penalties. This is because AMPS penalties apply to a wide variety of breaches of the *Customs Act*, including various export control related failures.

Some of the more commonly applied AMPS penalties associated with export control failures include the following:

C315: exporter failed to provide to customs, according to the legislative timeframes, any export permit, license or certificate required.

Penalties: applied per document

First offence: \$1,000
Second offence: \$2,000
Third and subsequent offence: \$3,000

C345: exporter failed to report goods subject to export control prior to export.

Penalties: applied per export

First offence: \$2,000 or 20% of the value of goods (whichever is greater)
Second offence: \$4,000 or 40% of the value of goods (whichever is greater)
Third and subsequent offence: \$6,000 or 60% of the value of the goods (whichever is greater)

In addition to the AMPS penalties above, there may be a seizure of the goods (or an ascertained forfeiture if seizure is impractical) where there is evidence that the exporter willfully avoided compliance with the export requirements

C346: person who has reported goods under subsection 95(1) of the Customs Act that are subject to export control, failed to answer truthfully (verbally or in writing) any question asked by an officer with respect to the goods.

Penalties: applied per occurrence

First offence: \$2,000 or 20% of the value of goods (whichever is greater)
Second offence: \$4,000 or 40% of the value of goods (whichever is greater)
Third and subsequent offence: \$6,000 or 60% of the value of the goods (whichever is greater)

C348: person intentionally provided false information in any permit, certificate, license, document or declaration required to be provided for imported or exported goods under the Customs Act...or under any other Act of Parliament that prohibits, controls or regulates the importation or exportation of goods.

Penalties: applied per occurrence

First offence: \$2,000 or 20% of the value of goods (whichever is greater)
Second offence: \$4,000 or 40% of the value of goods (whichever is greater)
Third and subsequent offence: \$6,000 or 60% of the value of the goods (whichever is greater)

Although the AMPS penalties outlined above are often relied upon by the CBSA to deal with export control infractions there are a number of other penalty tools at the disposal of the CBSA for export related violations. These alternative measures include:

- (a) the right to seize and eventually destroy goods; and
- (b) the right to apply penalties in the nature of ascertained forfeiture: if seizure of the goods would be impractical a monetary penalty may be imposed which is equivalent to the value of the goods.

In addition to the penalties described above the EIPA establishes that any person who contravenes any provision of the EIPA may be subject to either of the following criminal sanctions:¹⁰

- (a) up to 12 months imprisonment and/or a fine up to \$25,000 in a proceeding by way of summary conviction; or
- (b) for more egregious acts or omissions, up to 10 years imprisonment and/or a fine to be established by the Courts, in a proceeding by way of indictment.

Officers and directors of corporations should be particularly concerned with the potential impact of the EIPA. The EIPA establishes that where a corporation commits an offence any officer or director who “directed, authorized, assented to, acquiesced in or participated in” the commission of the offence is a party to and guilty of the offence.¹¹ Where an officer or director is convicted of an offence under the EIPA the sanctions are the same as those set out above. This means that officers and directors could face imprisonment.

The EIPA even provides that officers and directors may be prosecuted in circumstances where the corporation itself is not prosecuted or convicted. This option leaves the Crown the option of proceeding directly against the individual(s) who it considers to be at fault.

Given that the penalties associated with the breach of the EIPA are quite severe, the following exposure management issues should be considered by each and every officer and director of an exporting company:

- (a) what is the offence? (or what specifically is “the commission of an offence?”); and
- (b) when is the officer or director drawn into (or responsible for) the commission of the offence?

With respect to question (a) (i.e., what is the offence) the primary offences under the EIPA are:

- (i) exporting (or attempting to export) controlled goods or technology without a permit; or
- (ii) exporting controlled goods or technology in a manner which does not conform with the terms and conditions of the permit which has been granted.

The suggestion is that offences may be committed in what may appear to be very innocent circumstances. For example, an offence may be committed where the company is merely adhering to normal business practices (i.e., earning revenues by selling its products).

With respect to question (b) (when is the officer or director responsible for the offence) it does not necessarily follow that an officer or director will be responsible for the offence each time that the corporation has committed an offence. Officers or directors may take on personal exposure where they have taken one or more active steps in connection with the offence (for example, a director or officer who directed or authorized the export of the controlled goods or technology). An officer or director may also be considered to have committed an offence where he/she has adopted a passive approach with respect to

10 Section 19 of the EIPA.

11 Section 20 of the EIPA.

exports of controlled items. For example, an officer or director who has “assented to, acquiesced in or participated in” the export of controlled items without a permit, may be guilty of an offence.

From an evidentiary perspective the Crown, in proceeding against an officer or director, may not, strictly speaking, need to show that the officer or director had knowledge that the goods were subject to export control or even that the officer or director was aware of the existence of the export control program. This is because it is a fundamental tenet of Canadian law that ignorance of the law is no excuse.¹²

E. Other forms of Penalties

Apart from the statutory penalties, described above, which are available to encourage compliance with the EIPA compliance discrepancies may also trigger other sanctions. Some of the other forms of sanctions are briefly discussed below.

(i) Substantial export delays resulting in lost sales and lost customer confidence

When businesses learn midstream (i.e., in the middle of a sales cycle) that the goods or technology which they previously were exporting (without permits), are subject to export control the company is certain to encounter a number of difficult timing issues.

If exports without permits are made subsequent to the date when the exporter specifically became aware of the export permit requirement then it should be expected that the CBSA would likely respond by levying its most substantial penalties (i.e., the criminal sanctions). This is because any non-compliant exportation subsequent to the “knowledge” date would undoubtedly constitute an open and express breach of Canada’s laws.

Accordingly, the exporter will typically find that it has no choice but to halt all exportations until such time as export permits are granted. Exporters will normally find that they are unable to meet their contractual obligations to ship (either physically or electronically) to their customers for a period of weeks or perhaps even months. This may trigger penalty provisions which are contained in the supply agreements.

Apart from potentially substantial delays in shipping products non-compliant exporters will also frequently encounter another difficult problem: they may have no choice but to explain to their customers (and other supply chain partners) that they have encountered export control compliance issues. Even if the supplier is able to “explain away” shipping related delays the compliance issues will come to light where DFAIT demands that the exporter obtain end user certification from the customers or from government officials in the destination country.

The timing concerns described above may also be exacerbated by government officials who will not “fast track” applications for permits to compensate for exporter deficiencies. In fact, quite the opposite should be expected: where companies have shown a poor export control track record DFAIT will typically perform even more due diligence prior to agreeing to provide export permits. This will translate into more detailed demands for information, more required assurances from supply chain parties and more background work to determine if granting permits would be appropriate. Significant shipping delays should be expected in those circumstances.

In short, apart from penalty clauses and other delay related costs, many businesses which have run afoul of the export control program will find that the breach is extremely damaging to the goodwill which the company has worked so hard to achieve.

(iii) Administrative burdens may increase

The Minister has substantial discretion in the manner in which it administers the export control program. Exporters who have satisfied the Minister that they have created a reliable and transparent corporate export control program will typically find that the permit process will proceed relatively smoothly. Export

12 This doctrine is derived from ancient roman law and is known as the principle of *Ignorantia juris non excusat*.

permits, when issued will typically be fairly broad in scope (i.e., permits will not need to be applied for as frequently) and contain more liberal terms and conditions. Once DFAIT has established a positive ongoing relationship with a particular exporter DFAIT may be more comfortable in “turning around” permit applications more quickly and with fewer questions asked.

Exporters who are new to the export control program because they are introducing new products (i.e., controlled products) or because they are entering new markets will need to “earn” these same privileges by gaining the trust of DFAIT. New exporters will typically find that there will be more terms and conditions (and other checks and balances) put in place by DFAIT to ensure that the exporter is fully complying with the program.

Exporters who are new to the export control program because they have previously failed to achieve compliance should expect very special treatment. Among other things they should expect that the terms and conditions attached to any export permits would be extremely stringent and permits, when issued will be relatively narrow in scope (i.e., the exporter will be kept on a “tight leash”). As may be expected some exporters will find that these comprehensive requirements will pose a substantial administrative burden (both for the exporter and for the customer), will slow the sales process and may not sit well with any person in the supply chain.

Exporters may also find that their competitors who have established a better working relationship with DFAIT will have a strategic advantage in getting products to market more quickly and efficiently.

(iii) Public relations disasters

Apart from the administrative difficulties outlined above exporters who are not in compliance with Canada’s export control laws may find that a failure to obtain export permits could be devastating from a public relations and branding perspective.

Should a link ever be established between a product offering of a particular company and a terrorist group, terrorist activity (such as a bombing) or other extremely undesirable activity, person or group then it should be expected that this link would be extremely damaging to the company.

However, the damage associate with any such linkage would be far more acute if it were to become public knowledge that the company had exported the product in breach of the export control program (i.e., the exporter was in breach of the very laws which were intended to prevent such an occurrence).

For example, consider the public (and business) reaction if it were to be revealed that a terrorist group relied upon Canadian software containing encryption algorithms to communicate secretly with a terrorist cell to plan a terrorist attack?

Although this particular risk may be considered by some companies to be fairly remote the damage associated with any such connection coupled with an overt breach of Canadian laws may be sufficient to destroy the business. On the other hand a company which has received formal “sign off” from DFAIT may be in a better position to demonstrate to the public that it conducted business in a legitimate and responsible manner.

Part II: The Export Control List

A. Overview of the List

As a preliminary matter, it may be a misnomer to describe the export control list as a single list. Rather, the export control list is a series of seven discrete lists (referred to as “groups”) and with each group having its own unique definitions and special rules of interpretation. The seven groups are as follows:

- Group 1: Dual Use List
- Group 2: Munitions List
- Group 3: Nuclear Non-Proliferation List
- Group 4: Nuclear-Related Dual Use List
- Group 5: Miscellaneous Goods and Technology
- Group 6: Missile Technology Control Regime List
- Group 7: Chemical and Biological Weapons Non-Proliferation List

Each of these lists (or Groups) was drafted independently and in response to a particular international obligation (or series of obligations) and/or policy concerns. For example, Groups 3 and 4 relate to Canada’s participation as a party to the *Treaty on the Non-Proliferation of Nuclear Weapons*. Group 2 and Group 7 contain items the export of which Canada has agreed to control under the *Chemical Weapons Convention*. Group 7 also contains items which Canada has agreed to control by virtue of its participation in the *Australia Group*, a group formed to monitor and control the proliferation of chemical and biological weapons.

Given that so many divergent underlying sources and policy considerations have contributed to the creation of the various group lists it should hardly be surprising that the groups may not always dovetail together in a seamless manner (for example like the various chapters of the *Customs Tariff*).

Further, as a matter of interpretation it is not uncommon for a particular item to be listed as controlled in two different groups or for a particular item to be carved out from control in a particular group but at the same time remaining subject to control by a second group. By way of example, a particular item may be carved out of the Group 4 Nuclear-Related Dual Use List only to be captured by the Group 1: Dual Use List or by the Group 5: Miscellaneous Goods and Technology List.

As a result, in order to determine whether a particular good or technology is subject to export control each of the seven groups should be considered.

B. Groups 2 to 4 and Groups 6 and 7

The core items contained in groups 2 to 4 and groups 6 and 7 are items which are inherently and very obviously dangerous. For example, the following are some of the typical items which are listed within each of those groups:

Group 2: Munitions List

“Bombs, torpedoes, rockets, missiles, other explosive devices and charges, and related equipment accessories, as follows, specifically designed for military use, and specially designed components therefore” (Item 2-4)

Group 3: Nuclear Non-Proliferation List

“Nuclear reactors and especially designed or prepared equipment and components therefore” (Item 3-2.1)

Group 4: Nuclear-Related Dual Use List

“Uranium isotope separation equipment and components...” (Item 4-3)

Group 6: Missile Technology Control Regime List Item

“Complete rocket systems (including ballistic missile systems, space launch vehicles, and sounding rockets)...capable of a range equal to or greater than 300 km” (6-19.A.1)

Group 7: Chemical and Biological Weapons Non-Proliferation List

“Fermenters, capable of cultivation of pathogenic micro-organisms, viruses or for toxin production, without the propagation of aerosols, and having a capacity equal to or greater than 20 litres” (Item 7-12.2)

Due to the obviously dangerous nature of many of these items it would be very difficult for any exporter not to be aware that the items are controlled.¹³ For example, under Group 7 (chemical and biological weapons non-proliferation) the following are listed as controlled items: certain human pathogens, including the Ebola virus and the Hantaan virus as well as deadly toxins such as Ricin or Saxitoxin.

However, exporters will not be able to rely entirely on intuition to navigate these groups. This is because each one of these groups also contain a number of less obvious or tangential items. For example, Group 7 (which among other things references deadly viruses) also lists as a controlled item, (under item 7-12.6) “protective full or half suits, or hoods dependent upon a tethered air supply and operating under positive pressure.” Obviously, unlike the pathogens or toxins which are listed in Group 7, the protective suit is not in and of itself dangerous. However, from a practical perspective, knowledge of the location where such suits are ultimately used should be expected to be extremely relevant in tracking activities related to chemical and biological weapons.¹⁴

C. Group 5: Miscellaneous Goods

Group 5, as its name suggests contains a myriad of miscellaneous goods. Included in this list are a number of seemingly obscure and unrelated items such as: pancreas glands, human serum albumin, sugar containing products, roe herring, peanut butter, blinding lasers and anti-personnel mines.

Although many of the items contained in Group 5 are not connected to each other from a subject matter perspective, for each item there is a specific underlying reason why it has been listed as controlled. For example, with respect to anti-personnel mines (item 5503), Canada has since 1997 been a signatory to the *Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction*. On the other hand peanut butter exports are controlled because the United States has imposed country specific import quotas (where peanut butter is being exported to countries other than the United States the goods are still subject to export controls, but the exporter may rely upon GEP 31 instead of obtaining a specific export permit).

Because of the wide variety of disjointed items contained within Group 5 exporters should always consider whether their intended exports fall within this list. The following two items contained within Category 5 also deserve special mention because of their extremely broad scope:

Item 5400: United States Origin Goods

All goods which originate in the United States and which are to be exported from Canada are controlled under item 5400 unless:

- (a) the goods are listed elsewhere in the export control list;

13 In fact most companies which export overtly dangerous goods will have a very sophisticated internal export control compliance system in place.

14 Tracking the suits may also be relevant for the reason that the suits could facilitate the “use” or handling of the good.

(b) the goods are further processed or manufactured outside of the United States so as to result in a substantial change in value, form or use of the goods or in the production of new goods; or

(c) the goods are destined for the United States.

This item is not at all product specific and as a result applies to every conceivable type of good (from rubber boots to staplers). In many cases the exporter of goods which are controlled under item 5400 will not be required to obtain a specific export permit. This is because goods which are controlled under item 5400 may be exported under the authority of General Export Permit 12 except if the goods are destined for any of Cuba, the Democratic People's Republic of Korea, Iran or Syria.

Item 5505: Goods for Certain Uses (Catch-all)

Goods which are not elsewhere listed but:

(a) which are intended for use in; or

(b) in respect of which there are reasonable grounds to suspect that the goods are for use in

i. the development, production, handling, operation, maintenance, storage, detection, identification or dissemination of chemical, biological or nuclear weapons, or of materials or equipment that could be used in such weapons

ii. the development, production, handling, operation, maintenance, or storage of missiles capable of delivering chemical, biological or nuclear weapons or of materials or equipment that could be used in such missiles, or

iii. any chemical, biological or nuclear weapons facility or missile facility.

This item (which is frequently referred to simply as the "catch-all clause") places a heightened obligation upon exporters to be vigilant in connection with sales of any items (including seemingly innocuous items) which could potentially be used in one of the listed applications. The *Guide to Canada's Export Controls* underscores the importance of this item with the following comment:

This item covers non-listed, commercial/civilian items, which could make a serious or major contribution to the proliferation of chemical, biological or nuclear weapons, or their missile delivery systems, if those items were to fall into the hands of questionable end users or destined to dubious end-uses.¹⁵

Exporters should be aware that the threshold test which will result in the triggering of this item is relatively low. In fact the exporter's obligations will be triggered any time that there are "reasonable grounds to suspect" that the goods may be used inappropriately. Exporters who are in doubt as to whether a particular export may or may not be caught by Item 5505 might want to consider erring on the side of caution.

15 See "A Guide to Canada's Export Controls", page xxix

D. Group 1: the Dual-Use List

(i) Background

The dual use list contains a wide range of relatively innocuous items which may be manufactured or created for ordinary commercial uses but which could be used (or easily converted to use) for military, terrorist or other strategic purposes. Because the items contained in the dual use list will not typically appear to be dangerous exporters often encounter compliance issues in connection with Group 1. Exporters of any virtually any type of goods (but particularly those goods which have been manufactured to exacting specifications or for specialized functions) would be well served to consider the potential application of this list.

The dual use list was created in order to fulfill Canada's obligations under the *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual Use Goods and Technology* (the "Wassenaar Arrangement") and comprises those dual use items which could have both civilian and military application. A *Guide to Canada's Export Controls* describes the purpose of the Wassenaar Arrangement in the following terms:

The *Wassenaar Arrangement (WA) on Export Controls for Conventional Arms and Dual Use Goods and Technology* was 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 technology, thus preventing destabilizing accumulations...The WA complements and reinforces...the existing control regimes for weapons of mass destruction and their delivery systems. 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.

As a preliminary matter it should be noted that there is a geographical carve out associated with the Group 1 dual use list. The list does not apply to goods or technology which are destined for the United States.¹⁶ However, this does not mean that goods may be trans-shipped by way of the United States in order to avoid the control measures. In order to rely on the U.S. destination exclusion the goods should be intended to remain within the U.S. or at the very least be subject to further processing within the U.S. It should also be noted that when the goods are subsequently exported from the U.S. they may be subject to U.S. export control measures.

The Group 1 list is broken down into a series of nine lists (each of which is described as a "Category") as follows:

- Category 1: Advanced Materials
- Category 2: Materials Processing
- Category 3: Electronics
- Category 4: Computers
- Category 5: Part 1: Telecommunications
- Category 5: Part 2: Information Security
- Category 6: Sensors and "Lasers"
- Category 7: Navigation and Avionics
- Category 8: Marine
- Category 9: Propulsion

Each of the 9 categories within Group 1 are further broken down into the following sub-categories:

- A. Systems, equipment and components
- B. Test, Inspection and Production Equipment

¹⁶ See section 2 of the *Export Control List* (SOR/89-202)

- C. Materials
- D. Software
- E. Technology

As a result of this structure a reference, for example, to “1-9.D” is a reference to software which relates to the propulsion category.

(ii) Categories 1 through 9

The following is a brief description of some of the more typical items contained within each of the 9 categories of Group 1:

Category 1 (advanced materials) references a wide variety of commercial goods which do not have any commonalities other than the fact that they are sophisticated or specialized in design and/or function. Typical items include:

- protective suits designed or modified for defence against biological agents, radioactive materials or chemical warfare agents (1-1.A.4)
- body armour which is not manufactured to military specifications (1-1.A.5)
- materials specially designed for use as absorbers of electromagnetic waves (1-1.C.1)
- technology for the production or development of certain of the other items listed in Category 1 (1-1.E.1)

Category 2 (materials processing) references a wide range of specialized tools and other manufacturing or production equipment. Items range from anti-friction bearing systems to highly sophisticated milling tools and chemical vapour deposition equipment. A typical example of a controlled good is as follows:

Machine tools, as follows, and any combination thereof, for removing (or cutting) metals, ceramics or “composites,” which, according to the manufacturer’s technical specification, can be equipped with electronic devices for “numerical control”...(1-2.B.1)

Category 3 (electronics) references a wide variety of electronic components (including circuits, microwave components, acoustic wave devices and devices made from superconductive materials) as well as other more general purpose electronic equipment such as recording equipment, frequency synthesizers, signal analyzers and microwave test receivers. A typical example of a controlled good is as follows:

Storage integrated circuits manufactured from a compound semiconductor. (1-3.A.4)

Category 4 (computers) focuses in particular upon computers which have been designed and developed with unique, and extreme performance characteristics. Controlled computers include those which may operate in hostile environments (such as in extreme temperatures or in the presence of radiation). A typical example of a controlled good is as follows:

Computers, as follows, and specially designed related equipment, “electronic assemblies” and components therefore: (1-4.A.4)

- a. “systolic array computers”
- b. “neural computers”
- c. “optical computers”

Category 5 (Part 1) (telecommunications equipment) relates to telecommunications equipment which is designed to withstand or to continue to operate in severe environments (including for example subsequent to a nuclear explosion, in the presence of gamma radiation or at temperatures below -55 degrees Celsius). Controlled items also include telecommunications equipment which is designed to be particularly secure or which is designed to interfere with the operation of other equipment. A typical example of a controlled good is as follows:

Jamming equipment specially designed or modified to intentionally and selectively interfere with, deny, inhibit, degrade or seduce cellular mobile telecommunication services...(1-5.A.1.f)

Category 5 (Part 2) (information security) is discussed in more detail below.

Category 6 (sensors and lasers) contains a very broad range of items. In addition to a wide array of lasers, Category 6 lists acoustics systems (both for transmitting and receiving a wide range of signals in a variety of environments) including for example hydrophone or sonar equipment, optical and imaging sensors, high speed or other specialized cameras, optical mirrors, magnetometers, gravimeters and radar equipment. A typical example of a controlled good is as follows:

High speed cinema recording cameras using any film format from 8 mm to 16 mm inclusive, in which the film is continuously advanced throughout the recording period, and that are capable of recording at framing rates, exceeding 13,150 frames/second (1-6.A.3.1)

Category 7: (navigation and avionics) relates to highly specialized aircraft related equipment and other navigation equipment. Items in this category range from accelerometers (for use in guidance systems), gyros and certain altimeters. A typical example of a controlled good is as follows:

Gyro-astro compasses, and other devices which derive position or orientation by means of automatically tracking celestial bodies or satellites, with an azimuth accuracy of equal to or less (better) than 5 seconds of arc (1-7.A.4)

Category 8 (marine) includes a wide range of specialized marine vessels (both surface and submersible vessels) and associated vessel parts. This category also contains specialized equipment which may be used in a marine environment such as underwater cameras, underwater robots or fibre-optic hull penetrators. A typical example of a controlled good is as follows:

Surface effect vehicles (rigid sidewalls) with a maximum design speed, fully loaded, exceeding 40 knots in a significant wave height of 3.25 m (Sea State 5) or more (1-8.A.1.g)

Category 9 (Propulsion) relates to engines (or parts of engines) which could be used for aircraft or rocket propulsion and any associated software or technology. A typical example of a controlled good is as follows:

Ramjet, scramjet or combined cycle engines and specially designed components therefore (1-9.A.11)

(iii) Overview of Part 2 of Category 5 (Information Security)

Part 2 of Category 5 is particularly important because it applies to a very broad range of product offerings which may be either physical or electronic in nature and in some cases may even apply to transfers of knowledge.

Encryption technologies are central to Part 2 of Category 5. As may be expected Part 2 has grown exponentially in importance in recent years due to the proliferation of software, hardware and other products (including in many cases ordinary consumer products such as cell phones) which rely in part upon encryption for the protection of sensitive information. It should be anticipated that far more product offerings will be developed in the coming years which will be even more encryption reliant.

(iv) Overview of Encryption

Encryption is the process whereby ordinary information is converted by way of an algorithm (i.e. typically a very complex algorithm) into a format which is unintelligible to any person other than the key holder. Decryption is the process whereby the keyholder converts that same information back into the original, intelligible format.

To protect both domestic and international flows of information a wide variety of incredibly sophisticated encryption technologies have been developed in the past half century. Encryption is widely used in a variety of products including everyday consumer products such as cell phones, ATM cards, portable home telephones or even cable television converters. Encryption (or cryptography) is very widely relied upon in connection with the Internet (including e-commerce transactions) because any information shared over or transmitted by way of the Internet would not otherwise be secure. For example, it is quite common for emails or remote login access to be protected by encryption.

The following is a brief summary of the development of modern encryption techniques and technology. In the 1970s symmetric key cryptography (i.e., cryptography whereby the sender and receiver of information share the same distinctive key) proliferated and was relied upon in a wide variety of applications. In terms of encryption standards during the 1970s the Data Encryption Standard (also known as “DES,” “single DES” or “56 Bit” encryption) was recognized by the United States Government (*National Institute of Standards and Technology or NIST*) as an official cryptography standard. DES remains to this day a very high encryption standard notwithstanding that it relies upon what is now considered to be a relatively short (56 Bit) key length.

In the late 1970’s a second type of far more advanced (and more flexible) encryption technique was developed. This new technology was known as the “asymmetric key” or “public key” system. Unlike the symmetric key system (which required that the same key be issued both to the sender and receiver) the asymmetric key system relied upon distinctive, but mathematically related keys being issued to the two parties. To employ this system the public key (which is used for encrypting the information) would be distributed freely while the private key would be closely controlled. The use of asymmetric keys has proliferated along with the explosive growth of the Internet.

Today both symmetric key and asymmetric key systems are widely used internationally. Part 2 of Category 5 specifically references the single DES standard in connection with symmetric algorithms (item 1-5.A.2.1.a). The dual use list also specifically references asymmetric algorithms (item 1-5.A.2.1.b)

Throughout the 1970s, 1980s and 1990s the DES standard was the encryption methodology which was most extensively relied upon worldwide to encrypt both commercial and military or other government information. However, by the late 1990s, largely as a result of significant advances in computing power, a new standard for information security was formally approved by NIST – the Triple DES (or “TDES”) standard. This standard, which is based upon a much longer, 168 bit key length, is considered to be highly secure from attack and remains in use in a wide variety of commercial and government applications.

However, even though Triple DES remains (and will for years remain) as an incredibly high standard of encryption, in the early 2000s an even more advanced encryption standard was developed. This new standard, known as the “Advanced Encryption Standard” (or by its trade name “Rijndael”) was also formally approved by NIST and deemed to be suitable for a wide variety of secure applications.

Throughout the periods referenced above a broad range of other competing encryption techniques have also been developed. Although most of these other techniques have not received formal NIST approval the more advanced techniques are virtually impervious to attack even with the use of the most sophisticated computing power.

The ability of persons anywhere in the world to rely upon encryption technology to transmit or receive information which is essentially impervious to (government) scrutiny is a very significant concern for the Government Canada and for the governments of other countries.

In many cases this concern manifests in connection with the control (or monitoring) of ordinary commercial goods which were not created for any malicious purpose. In many cases the commercial items which are subject to export control will incorporate or rely upon encryption technology strictly as a means to protect the intended user's information. Further, there will not typically be any specific reason to believe that the user's information might relate to terrorism or to any other strategic function.

For example, among the items which are commonly subject to export control under Part 2 of Category 5 are data recovery and backup systems (i.e. disaster recovery systems). These systems will normally rely on encryption to ensure that the data to be backed up is transmitted and stored in a secure manner.

(v) Structure and Contents of Part 2 of Category 5 (Information Security)

At the core of Part 2 is item 1-5.A.2.a which controls the following in connection with cryptography:

Systems, equipment, application specific "electronic assemblies,"¹⁷ modules and integrated circuits for "information security,"¹⁸ and other specially designed components¹⁹ which meet any of the following specifications:

1. Designed or modified to use "cryptography" employing digital techniques performing any cryptographic function other than authentication or digital signature having any of the following:

- a. a "symmetric algorithm" employing a key length of in excess of 56 bits; or
- b. an "asymmetric algorithm" where the security of the algorithm is based on any of the following:

- 1. Factorisation of integers in excess of 512 bits (eg. RSA):
- 2. Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (eg, Diffie-Hellman over Z/pZ); or
- 3. Discrete logarithms in a group other than mentioned in 1-5.A.2.a.1.b.2 in excess of 112 bits (eg, Diffie-Hellman over an elliptic curve)

"Cryptography" is defined²⁰ as "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

17 An "electronic assembly" is defined as "a number of electronic components (i.e., "circuit elements", "discrete components", integrated circuits, etc.) connected together to perform (a) specific function(s) replaceable as an entity and normally capable of being disassembled.

18 "Information security" is defined as "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".

19 The following items are included in the 1-5.A.2 list but are not specifically cryptography related: Item 4: Specially designed or modified to reduce the compromising emanations of information bearing signals beyond what is necessary for health, safety or electromagnetic interference standards; Item 8: Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion.

20 All definitions are contained in Group 2 of "A Guide to Canada's Export Controls"

information using one or more “secret parameters”²¹ (e.g. crypto variables) or associated key management.

A “symmetric algorithm” is defined as “a cryptographic algorithm using an identical key for both encryption and decryption.”

An “asymmetric algorithm” is defined as “a cryptographic algorithm using different, mathematically-related keys for encryption and decryption.”

2. Designed or modified to perform cryptanalytic functions;

This item relates to goods which have been designed or modified to perform the function of seeking out weaknesses or insecurities in a cryptographic scheme (i.e., in order to subvert the scheme).

5. Designed or modified to use cryptographic techniques to generate the spreading code for “spread spectrum” systems...

A “spread spectrum” is defined as “the technique whereby energy in a relatively narrow band communication channel is spread over a much wider energy spectrum”

6. Designed or modified to use cryptographic techniques to generate channelizing codes, for systems using ultra-wideband modulation techniques, having any of the following characteristics:

- a. a bandwidth exceeding 500 MHz; or
- b. a “fractional bandwidth” of 20% or more

9. Designed or modified to use “quantum cryptography.”

Quantum cryptography is defined as “a family of techniques for the establishment of a shared key for cryptography” by measuring the quantum-mechanical properties of a physical system (including those physical properties explicitly governed by quantum optics, quantum field theory or quantum electrodynamics).

In addition to the above the following are also controlled under Part 2 of Category 5:

- equipment which has been designed to develop or produce items which are listed as controlled above (see item 1-5.B.2)

- software which is designed or modified for the production, development, use or support of the equipment or the software which is listed as controlled above (see item 1-5.D.2)

“Technology” is also subject to control when it is for the “development,”²² “production”²³ or “use”²⁴ of equipment or “software”²⁵ which is controlled by part 2 of Category 5 (see item 1-5.E.2). The term “technology” in turn is defined very broadly as:

21 A “secret parameter” is a constant or key kept from the knowledge of others or shared only within a group.

22 “Development” is related to all stages prior to serial production, such as: design, design research, design analyses, design concepts, assembly and testing of prototypes, pilot production schemes, design data, process of transforming design data into a product, configuration design, integration design, layouts.

23 “Production” is defined to include “all production stages, such as: product engineering, manufacture, integration, assembly (mounting), testing, inspection, quality assurance”

24 “Use” is defined as “operation, installation (including on site installation) maintenance (checking), repair, overhaul and refurbishing”.

25 “Software” is defined as “a collection of one or more “programmes” or “micro-programmes” fixed in any tangible medium of expression”.

...specific information necessary for the “development” “production” or “use” of a product. The information takes the form of technical data or technical assistance. Controlled “technology” for the dual use list is defined in the General Technology Note and in the Dual Use List.

The definition of “technology” specifically includes a reference to “technical assistance.” As a result services (whether a charge is levied or not) or the sharing of information are equally capable of being subject to export control, regardless of whether the information accompanies a physical good or an electronic offering. The technical notes which accompany this definition also confirm the broad scope of the term “technical assistance.” The notes provide that “technical assistance” may take forms such as instruction, skills, training, working knowledge or consulting services.

The term “technical data” is also intended to be quite broad in scope. The technical notes elaborate that 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 or read only memories.

It follows from the broad definitions above that something as innocuous as providing training or consulting in connection with certain encryption technologies may be considered to be a controlled export. This will be the case regardless of whether the person providing the service is offering any corresponding written materials or other documentation.

Although item 1-5.A. 2 is intended to be extremely broad in scope, there are a number of important carve outs which have been made from this list. Some of the excluded items are as follows:

- certain personalized smart cards (i.e., a smart card which has been programmed for a specific application and which cannot be reprogrammed by the user)
- receiving equipment for certain broadcasts (i.e. for cable television, pay per view or radio broadcasts)
- cryptographic equipment designed for banking or money transactions
- portable or mobile radiotelephones for civil use
- cordless telephone equipment which is not capable of end to end encryption

Other important exclusions should also be considered when determining if an item is controlled under Part 2 of Category 5. For example, items which otherwise would be controlled are excluded if they are products which are accompanying the user for the user’s personal use (see General Note 2 to Part 2).

More importantly, items are excluded from export control under 1-5.A.2 (i.e., the systems, equipment and component list) and under 1-5.D.2 (the software list) if they meet all of the following conditions:²⁶

The items are:

- a. generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of the following:
 1. over the counter transactions;
 2. mail order transactions;
 3. electronic transactions; or
 4. telephone call transactions
- b. the cryptographic functionality cannot easily be changed by the user

26 This exclusion is provided by the Cryptography Note (Note 3 to Part 2 of Category 5)

- c. designed for installation by the user without further substantial support by the supplier; and
- e. when necessary, details of the items are accessible and will be provided, upon request, to the appropriate authority in the exporter's country in order to ascertain compliance with conditions described in paragraphs a. to c. above.

Similarly, the General Software Note (to Group 1) establishes that software which meets conditions 'a' (generally available to the public) and 'c' (designed for installation by the user) above will not be controlled under Group 1. The general software note also establishes that software which is "in the public domain" will not be subject to control under Group 1. The term "in the public domain" is defined as follows:

This means technology or software which has been made available without restriction upon its further dissemination. [Note: copyright restrictions do not remove technology or software from being "in the public domain"]

Many exporters have been quick to assume that their otherwise controlled products will qualify for at least one of these three carve outs. However, from a practical perspective, it is worth noting that the three exclusions are in fact quite similar in their wording, application and scope. As a result if a particular offering fails to meet one of these exclusions then there is a heightened risk that it may fail to meet any of the three exclusions. Further, and more importantly, it has been our experience that DFAIT interprets these three exclusions in a fairly restrictive manner.

Appendix A

Information to be provided in an application for export permit

Subsection 3(1) of the *Export Permits Regulations* provides that the following information shall be provided in any application for an export permit:

- (a) the date on which the application form is completed
- (b) the applicant's name, address and telephone number...
- (c) if the applicant is applying for a permit on behalf of or for the use of another person who will export the goods, the name address and telephone number of the other person
- (d) the customs office at which the goods will be reported...
- (e) the name and address of each consignee
- (f) the country in which the goods are to be consumed or the country of final destination
- (g) for each type of separately identifiable goods,
 - (i) the country of origin of the goods and if any portion of the goods is of United States origin and is included in item 5400 of group 5 of the Schedule to the List, the percentage that the portion is of the total cost of the goods,
 - (ii) if the goods are included in the schedule to the List, the corresponding item number of those items in the Guide,
 - (iii) the Harmonized Commodity Description and Coding System commodity code, if available
 - (iv) a description of the goods, including technical specifications, with sufficient detail to disclose their true identity and in terms that avoid the use of trade names, technical names or general terms that do not adequately describe the goods
 - (v) the quantity, unit value and total market value of the goods, free on board factory or first shipping point in Canada
- (h) the total value of all types of separately identifiable goods intended to be exported
- (i) an indication of whether the permit is to be sent by mail or courier service...
- (j) information that may be required by the Minister in respect of the purpose for which the applicant proposed to export the goods, in order to establish that the export of the goods is consistent with the purpose for which the export of the goods is controlled, including
 - (i) an International Import Certificate
 - (ii) an End Use Certificate
 - (iii) an End Use Statement
 - (iv) a copy of the contract of sale between the applicant and the person from whom the applicant purchased the goods
 - (v) a copy of the contract of sale between the applicant and the person to whom the applicant sold the goods for export

- (vi) a summary report on prior exports of like goods by the applicant
- (vii) the name and address of the person from whom the applicant acquired the goods
- (viii) the intended end use of the goods by the consignee
- (ix) the intended end use location of the goods if different from the location of the consignee
- (x) the export permit numbers of any previous export permits issued to the same applicant
- (xi) an import permit issued by the government of the country for which the goods are destined
- (xii) an in-transit authorization

In addition to the requirement to file an export permit application form (containing information as described above) the applicant shall also submit to the Minister (as per subsection 3(2) of the *Export Permits Regulations*):

- (a) a declaration that, to the best of the applicant's knowledge, the goods will enter into the economy of the country referred to in paragraph 1(f) and will not be transhipped or diverted from that country
- (b) in the case of controlled goods, proof of registration or exemption from registration under the *Controlled Goods Regulations* or proof that the person occupies a position referred to in paragraph 36(a) of the *Defence Production Act*,
- (c) a United States export authorization in respect of the following goods
 - (i) any controlled goods that are goods of United States origin,
 - (ii) any goods incorporating any goods of United States origin that are controlled goods, or
 - (iii) any goods manufactured in Canada using any goods of United States origin that are controlled goods; and
 - (iv) a declaration that the information provided under this section is true, complete and correct.
- (d) a declaration that the information provided under this section is true, complete and correct.