

Commission of Inquiry into the
Actions of Canadian Officials
in Relation to Maher Arar



Commission d'enquête sur les
actions des responsables canadiens
relativement à Maher Arar

**THE LEGISLATIVE AND ORGANIZATIONAL
FRAMEWORK FOR THE NATIONAL
SECURITY ENVIRONMENT IN CANADA**

EXHIBIT P-2
(REVISED VERSION)

MAY 2005

TABLE OF CONTENTS

I.	THE LEGISLATIVE FRAMEWORK	1
A.	Federal Law.....	1
1.	<i>Bill C-36, Anti-Terrorism Act, (2001, c.41)</i>	1
2.	<i>Criminal Code, 1985, c. C-46</i>	3
a.	Part II.1 – Terrorism.....	3
(i)	Definitions of “Terrorist Activity”, “Terrorist Group”, and “Terrorism Offences”	3
(ii)	Financing of Terrorism.....	5
(iii)	List of Entities	6
(iv)	Freezing of Property	7
(v)	Seizure and Restraint of Property	7
(vi)	Forfeiture of Property.....	8
(vii)	Participating, Facilitating, Instructing and Harboring	9
(viii)	Proceedings and Aggravated Punishment	10
(ix)	Investigative Hearing	10
(x)	Recognizance with Conditions	12
(xi)	Annual Reports and Sunset Clause	13
(xii)	Parliamentary Review of the <i>Anti-Terrorism Act</i>	13
b.	Part VI – Invasion of Privacy	14
(i)	Wiretapping Provision Prior to Bill C-36	14
(ii)	Wiretapping Amendments Relating to Terrorism Offences and Groups..	14
c.	Part VIII – Offences Against the Person and Reputation	15
d.	Part XI – Wilful and Forbidden Acts in Respect of Certain Property	15
e.	Part XII.2 – Proceeds of Crime	15
f.	Part XV – Special Procedure and Powers.....	15
g.	Part XXIII – Sentencing	16
h.	Part XXVII – Summary Convictions.....	16
3.	<i>Bill C-24, An Act to Amend the Criminal Code (organized crime and law enforcement) and to Make Consequential Amendments to Other Acts S.C. 2001 c.32</i>	16
4.	<i>Canada Evidence Act, R.S.C. 1985, c. C-5</i>	17
a.	<i>Specified Public Interest</i>	17
b.	<i>International Relations, National Defence and National Security</i>	17
5.	<i>Access to Information Act, R.S. 1985 c. A-1, Personal Information Protection and Electronic Documents Act, 2000, c-5, Privacy Act, R.S. 1985 c. P-21</i> ...	19
6.	<i>Security of Information Act, R.S. 1985, c. O-5</i>	19
7.	<i>Canadian Security Intelligence Service Act, R.S. 1985, c. C-23</i>	25
8.	<i>Royal Canadian Mounted Police Act, R.S.C. 1985, c. R-10</i>	29
9.	<i>Security Offences Act, R.S. 1985, c. S-7</i>	32
10.	<i>Department of Foreign Affairs and International Trade Act, R.S. 1985, c. E-22</i>	33
11.	<i>National Defence Act, R.S. 1985, c. N-5</i>	34
a.	Defence Intelligence	34
b.	Communications Security Establishment (CSE)	35
12.	<i>Charities Registration (Security Information) Act, 2001 c-41</i>	36
13.	<i>Proceeds of Crime (Money Laundering) and Terrorist Financing Act, 2000 c.17 and the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)</i>	38

14.	<i>United Nations Suppression of Terrorism Regulations, SOR/2001-360</i>	41
15.	<i>United Nations Afghanistan Regulations, SOR/99-444</i>	42
16.	<i>An Act to Amend the Aeronautics Act, S.C. 2001, c. A-2 (Bill C-44)</i>	43
17.	<i>Immigration and Refugee Protection Act, S.C. 2001, c. 27</i>	43
18.	<i>Canadian Human Rights Act, R.S. 1985 c. H-6</i>	46
19.	<i>Public Safety Act, S.C. 2004 c. 15</i>	46
B.	International Law	50
1.	<i>United Nations Anti-Terrorism Conventions</i>	50
2.	<i>U.N. Security Council Resolution 1373</i>	51
3.	<i>U.N. Security Council Resolution 1269</i>	52
4.	<i>International Convention for the Suppression of the Financing of Terrorism, Adopted by the General Assembly of the United Nations on December 9, 1999</i>	53
5.	<i>Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc. A/810 at 71 (1948)</i>	54
6.	<i>International Covenant on Civil and Political Rights. Concluded at New York, Dec. 16, 1966. Entered Into Force March 23, 1976. 999 U.N.T.S. 171</i>	55
7.	<i>Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment. Concluded at New York, Dec. 10, 1984. Entered Into Force June 26, 1987. 1465 U.N.T.S. 85</i>	56
8.	<i>American Declaration of the Rights and Duties of Man. Adopted at Bogota by the Ninth International Conference of American States, Mar. 30-May 2, 1948. O.A.S. Res. XXX. O.A.S. Off. Rec. OEA/Ser. L/V/I.4 Rev. (1965)</i>	58
9.	<i>Vienna Convention on Consular Relations and Optional Protocols, 596 U.N.T.S. 261, Entered Into Force March 19, 1967</i>	58
II.	THE ORGANIZATIONAL FRAMEWORK FOR THE NATIONAL SECURITY ENVIRONMENT APPLICABLE IN CANADA PRIOR TO DECEMBER 2003	59
III.	THE ORGANIZATIONAL FRAMEWORK FOR THE NATIONAL SECURITY ENVIRONMENT APPLICABLE IN CANADA IN JUNE 2004	59
A.	Public Safety and Emergency Preparedness Portfolio	59
B.	The Canada-US Smart Border Agreement	60
C.	Canada/US Integrated Border Enforcement Teams (IBETs)	61
D.	Integrated National Security Enforcement Teams (INSET)	62
E.	Integrated National Security Assessment Centre (INSAC) and Integrated Threat Assessment Centre (ITAC)	62
F.	Canadian Air Transport Security Authority (CATSA)	63
G.	National Security Advisor to the Prime Minister	63
H.	Cabinet Committee on Security, Public Health and Emergencies	63
I.	National Security Standing Committee	63
J.	Privy Council Office (PCO)	64
K.	Other Parliamentary Committees on National Security	64
L.	New National Security Policy	65

THE LEGAL FRAMEWORK OF CANADA'S NATIONAL SECURITY ENVIRONMENT

I. THE LEGISLATIVE FRAMEWORK

A. Federal Law

1. Bill C-36, *Anti-Terrorism Act*, (2001, c.41)

Under this Act, the Government of Canada has taken steps to combat terrorism and terrorist activities at home and abroad through new anti-terrorism measures. It was introduced in Parliament on October 15, 2001 and considered by committees in both the House of Commons and the Senate. Amendments were introduced to the bill placing some restrictions on the definition of terrorism and providing for increased judicial review.

The new Act creates measures to deter, disable, identify, prosecute, convict and punish terrorist groups and to prevent and punish the financing, preparation, facilitation and commission of acts of terrorism. It also provides new preventive and investigative tools to law enforcement agencies and establishes stronger laws against hate crimes and propaganda. The Government of Canada's training materials on Bill C-36 describes the purpose and operational impact of the Act as follows:

“A key element of Canada's *Anti-Terrorism Act* is prevention. The focus on prevention is something of a cultural shift for our law enforcement community. It places the emphasis on the collection of intelligence, rather than the investigation of crimes that have already occurred.”¹

The new act also contains an extensive preamble that states that “Canada must act in concert with other nations in combating terrorism, including fully implementing United Nations and other international instruments relating to terrorism” It also states that “the Parliament of Canada, recognizing that terrorism is a matter of national concern that affects the security of the nation, is committed to taking comprehensive measures to protect Canadians against terrorist activity while continuing to respect and promote the values reflected in, and the rights and freedoms guaranteed by, the *Canadian Charter of Rights and Freedoms*.”

Bill C-36 amends the *Criminal Code*, the *Official Secrets Act* which is renamed the *Security of Information Act*, the *Canada Evidence Act*, the *Proceeds of Crime (Money Laundering) Act* which is re-named the *Proceeds of Crime (Money*

¹ “The Anti-Terrorism Act: An Act of Prevention”, CD-ROM available from the Department of Justice Canada.

Laundering) and Terrorist Financing Act and a number of other Acts. It also enacts the *Charities Registration (Security Information) Act*. Most of these Acts are outlined below, taking into consideration the numerous amendments made to them by the *Anti-Terrorism Act*, making it unnecessary to outline Bill C-36 in a comprehensive manner. However, a brief summary of Bill C-36 follows.

Part 1 of the *Anti-Terrorism Act* amends the *Criminal Code* to implement international conventions related to terrorism, to create offences related to terrorism, including the financing of terrorism and the participation, facilitation and carrying out of terrorist activities, and to provide a means by which property belonging to terrorist groups, or property linked to terrorist activities, can be seized, restrained and forfeited. It also provides for the deletion of hate propaganda from public web sites and creates an offence relating to damage to property associated with religious worship.

Part 2 amends the *Official Secrets Act*, which becomes the *Security of Information Act*. It addresses security concerns, including threats of espionage by foreign powers and terrorist groups, economic espionage and coercive activities against all persons in Canada. It creates new offences to counter intelligence-gathering activities by foreign powers and terrorist groups, as well as other offences, including the unauthorized communication of special operational information.

Part 3 amends the *Canada Evidence Act* to address the judicial balancing of interests when the disclosure of information in legal proceedings would encroach on a specified public interest or be injurious to international relations or national defence or security. The amendments impose obligations on parties to notify the Attorney General of Canada if they anticipate the disclosure of sensitive information or information the disclosure of which could be injurious to international relations or national defence or security, and they give the Attorney General the powers to assume carriage of a prosecution and to prohibit the disclosure of information in connection with a proceedings for the purpose of protecting international relations or national defence or security.

Part 4 amends the *Proceeds of Crime (Money Laundering) Act*, which becomes the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. The amendments will assist law enforcement and investigative agencies in the detection and deterrence of the financing of terrorist activities, facilitate the investigation and prosecution of terrorist activity financing offences, and improve Canada's ability to cooperate internationally.

Part 5 amends the *Access to Information Act*, *Canadian Human Rights Act*, *Canada Security Intelligence Service Act*, *Corrections and Conditional Release Act*, *Federal Court Act*, *Firearms Act*, *National Defence Act*, *Personal Information Protection and Electronic Documents Act*, *Privacy Act*, *Seized Property Management Act* and *United Nations Act*. The amendments to the *National*

Defence Act clarify the powers of the Communications Security Establishment to combat terrorism.

Part 6 enacts the *Charities Registration (Security Information) Act*, and amends the *Income Tax Act*, in order to prevent those who support terrorist or related activities from enjoying the tax privileges granted to registered charities.

Part 7, in part, provides for a comprehensive review of the provisions and operation of the *Anti-Terrorism Act* which will be undertaken by a Parliamentary Committee or Committees by December 18, 2004 (i.e. three years from the date of Royal Assent of the Act). The review is to be completed within a year unless further time is authorized by Parliament.

2. Criminal Code, 1985, c. C-46

Under the *Criminal Code* (CC) prior to Bill C-36, terrorists were prosecuted for hijacking, murder and other acts of violence. They could also be prosecuted for attempts, conspiracy, counselling or being an accessory after the fact in relation to such crimes. Bill C-36 has amended the CC to establish provisions aimed at making criminal certain activities of terrorist groups and those who support them.

a. Part II.1 – Terrorism

(i) Definitions of “Terrorist Activity”, “Terrorist Group”, and “Terrorism Offences”

Part 1 of the *Anti-Terrorism Act* amends the CC by adding Part II.1 entitled “Terrorism”. Paragraph 83.01(1)(a) of the definitions section now defines “terrorist activity”, in part, as an act or omission that takes place either within or outside Canada that is an offence under various subsections of s.7 of the *Criminal Code* that implement one of ten United Nations (U.N.) anti-terrorism conventions or protocols² (eg. hijacking, offences against internationally protected persons, hostage taking, etc.). Various subsections of s.7 of the Code are also amended to provide Canadian courts with jurisdiction over terrorist activities committed by a person outside of Canada in prescribed circumstances, usually involving some nexus to Canada. Examples of such a nexus would be that the person committing the act is a Canadian citizen, resident or present in Canada or the act was committed against a Canadian citizen.

A “terrorist activity” is also defined in paragraph 83.01(1)(b) as an act or omission, within or outside Canada, that is:

- committed for a political, religious or ideological purpose, objective and cause;

² For a list of the U.N. anti-terrorism conventions signed and ratified by Canada, see p. 33-34.

- with the intent of intimidating the public with regard to its security, including its economic security, or compelling a person, government, or a domestic or an international organization to do or to refrain from doing any act; and
- intentionally causes death, seriously harms or endangers a person, causes substantial property damage that is likely to seriously harm people, or causes serious interference with or disruption of an essential service, facility or system. Interfering with or disrupting an essential service is not a terrorist activity if it occurs as a result of advocacy, protest, dissent or stoppage of work that is not intended to harm or endanger a person or pose a serious risk to health and safety.

A “terrorist activity” includes a conspiracy, attempt or threat to commit any such act or omission described above, or being an accessory after the fact or counselling in relation to any terrorist act or omission.

There is also an interpretive clause that states that an expression of political, religious or ideological thought, belief or opinion alone is not a “terrorist activity” unless it constitutes an act or omission that meets the requirements of paragraph 83.01(1)(b) of the definition of “terrorist activity”.

The definition of terrorist activity does not in itself create a crime but it is incorporated in new offences, new police powers and new punishment powers in the *Criminal Code* that will be examined below.

A “terrorist group” means

- an entity that has as one of its purposes or activities facilitating or carrying out any terrorist activity, or
- a listed entity – an entity on a list established under s.83.05 (discussed below) -- and includes an association of such entities.

As with the definition of terrorist activity, the definition of a terrorist group does not constitute a crime, but rather is incorporated in various offences that will be examined below

Section 2 of the Code was also amended to define a “terrorism offence” as:

- (a) an offence under any of sections 83.02 to 84.04 or 83.18 to 83.23 [these crimes will be described below];

- (b) an indictable offence under this or any other Act of Parliament committed for the benefit of, at the direction of or in association with a terrorist group;
- (c) an indictable offence under this or any other Act of Parliament where the act or omission constituting the offence also constitutes a terrorist activity; or
- (d) a conspiracy or an attempt to commit, or being an accessory after the fact in relation to, or any counselling in relation to, an offence referred to in paragraph (a), (b) or (c).

Pursuant to section 83.24 of the Code, the consent of either the provincial or federal Attorney General is required before “proceedings in respect of a terrorism offence or an offence under s.83.12” are commenced. The definition of “Attorney General” in section 2 of the Criminal code was amended by Bill C-36 to give concurrent jurisdiction to the Attorney General of Canada and to provincial Attorneys-General to prosecute offences relating to terrorism, including previous offences and the new offences created by the Bill.

(ii) Financing of Terrorism

Under this new heading in the CC, it is an offence to:

- wilfully and without lawful justification or excuse provide or collect property, either directly or indirectly, intending or knowing that it will be used to carry out certain terrorist activities or acts intended to cause death or serious bodily harm to a civilian for the purpose of intimidating the public or compelling a government or international organization to do or refrain from doing any act (s.83.02);
- collect, provide or make available property or financial services for the purpose of facilitating the activities of a terrorist group or for benefiting any person who is facilitating or carrying out a terrorist activity or knowing that the property or financial services will be used in whole or part to benefit a terrorist group (s.83.03);
- use or possess property for the purpose of facilitating or carrying out a terrorist activity or possess property intending or knowing that it will be used, directly or indirectly, in whole or in part, for the purpose of facilitating or carrying out a terrorist activity (s.83.04)..

The maximum sentence for committing these offences would be ten years.

(iii) List of Entities

Under this heading, the Governor in Council may, on the recommendation of the Solicitor General, establish a list of entities where the Governor in Council is satisfied there are reasonable grounds to believe that

- the entity has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity; or
- the entity is knowingly acting on behalf of, at the direction of or in association with an entity described immediately above.

An “entity” includes a person, group, trust, partnership or fund, or an unincorporated association or organization.

Criminal and/or security intelligence reports are submitted to the Solicitor General for consideration. The Solicitor General may make this recommendation to the Governor in Council to place the entity on the list only if the Solicitor General has reasonable grounds to believe that the above test is met. If the Governor in Council is satisfied that there are reasonable grounds to believe that the above test has been met, then the entity may be placed by regulation on the list of entities. The listing of an entity is published in the *Canada Gazette*. The website for the Department of Public Safety and Emergency Preparedness Canada as of October 29, 2004 shows 35 entities as “listed entities” – 25 of the 35 listed entities are described as Islamic or Muslim extremist groups.³

Section 83.05 also provides for review of a decision to list an entity and review of the list. This includes provision for a listed entity to make an application in writing to the Solicitor General to be removed from the list as well as provision to judicially review the Solicitor General’s decision to list an entity. Every two years the Solicitor General is required to review the list to determine whether there are still reasonable grounds for an entity to be listed, and to make a recommendation to the Governor in Council as to whether the entity should remain a listed entity. Completion of the review must be reported without delay in the *Canada Gazette*.

Section 83.06 governs the admission and use of confidentially-obtained foreign information on judicial review applications to delist an entity. The Solicitor General may apply to the reviewing judge, in private and in absence of the applicant or any counsel representing it, for the admission of confidentially-obtained foreign information on the application for delisting. The judge must examine the information and give the Solicitor General’s counsel a reasonable opportunity to make representations about the relevance of the information and whether disclosure of it to the applicant or applicant’s counsel should be withheld because it would injure national security or endanger the safety of anyone. If the

³ For a list of the current listed entities, go to:
http://www.psepc-sppcc.gc.ca/national_security/counter-terrorism/AntiTerrorism_e.asp

information is relevant and not disclosable on these grounds, this information may form the basis of the reviewing judge's decision, but must not be disclosed to the applicant.

Section 83.07 allows an entity claiming not to be a listed entity to apply for a certificate from the Solicitor General stating that it is not a listed entity. This is to protect those who are victims of mistaken identity.

(iv) Freezing of Property

Under this heading, section 83.08(1) prohibits anyone in Canada, and any Canadian anywhere, directly or indirectly, from knowingly dealing in any property or being involved in any transaction in connection with any property, owned or controlled by, or on behalf of a terrorist group. It also forbids anyone from providing any financial or other related services in connection with property owned or controlled by, or on behalf of a terrorist group, for the benefit or at the direction of the group.

Section 83.09 permits an exemption from liability under section 83.08 for certain conduct authorized by the Solicitor General, and preserves the right of innocent third parties, including secured and unsecured rights and interests in the frozen property.

Section 83.1 imposes a duty on everyone to disclose to the RCMP Commissioner and the CSIS Director the existence of property in their possession or control that they know is owned or controlled by or on behalf of a terrorist group, as well as information about actual or proposed transactions involving that property. Civil and criminal immunity is given to anyone for good faith disclosure of this information.

Section 83.11 imposes a continuing obligation on certain organizations (i.e. banks, credit unions, etc.) to determine whether they have possession or control of property owned or controlled by or on behalf of a "listed entity". The obligation includes requiring these organizations to submit periodic reports to the principal agency or body that supervises or regulates it under federal or provincial law.

Section 83.12 makes contravention of sections 83.08, 83.1, or 83.11 an offence.

(v) Seizure and Restraint of Property

Section 83.13 authorizes the issuance of warrants for search and seizure of, or restraint orders for, property that is forfeitable under section 83.14 (see next heading) and enacts a scheme for the management and destruction of that property.

Applications for warrants of search and seizure or restraint orders for forfeitable property are made by the Attorney General *ex parte* to a Federal Court judge. The judge examines the application in private. An affidavit in support of the application may be sworn on information and belief and, no adverse inference shall be drawn from a failure to provide evidence of persons having personal knowledge of material facts. The judge may issue the search warrant or restraint order once being satisfied that there are reasonable grounds to believe that there is in any building, receptacle or place any property in respect of which an order of forfeiture may be made under section 83.14(5).

(vi) Forfeiture of Property

Under section 83.14(1), the Attorney General may apply to a judge of the Federal Court for an order of forfeiture in respect of

- property that is owned or controlled by or on behalf of a terrorist group; or
- property has been or will be used, in whole or in part, to facilitate or carry out a terrorist activity.

An affidavit in support of the application may be sworn on information and belief and, no adverse inference shall be drawn from a failure to provide evidence of persons having personal knowledge of material facts. The Attorney General is required to name as a respondent to an application only those persons known to own or control the property that is the subject of the application. The Attorney General must also give notice of the application to them.

By subsection 83.14(5), If a judge is satisfied on the balance of probabilities that property is property that is owned or controlled by or on behalf of a terrorist group or that has been or will be used, in whole or in part, to facilitate or carry out a terrorist activity, he or she must order that the property be forfeited to Her Majesty to be disposed of as the provincial or federal Attorney General directs or otherwise dealt with in accordance with the law. Any proceeds that arise from the disposal of this property may be used to compensate victims of terrorist activities and to fund anti-terrorist initiatives in accordance with any regulations made by the Governor in Council. The Governor in Council may make regulations for the purpose of specifying how these proceeds are to be distributed.

On an application for forfeiture, a judge may require notice to be given to any person who, in the opinion of the Court, appears to have an interest in the property. Any such person is entitled to be added as a respondent to the application. If the judge is satisfied that the person has an interest in the property, has exercised reasonable care to ensure that the property would not be

used to facilitate or carry out a terrorist activity, and is not a member of a terrorist group, the judge must order that the interest is not affected by the forfeiture.

Where all or part of the property that is the subject of an application is a dwelling-house, the judge must also consider (a) the impact of an order of forfeiture on any member of the immediate family of the person who owns or controls the dwelling-house; if the dwelling-house was the member's principal residence at the time the dwelling-house was ordered restrained or at the time the application for forfeiture was made and continues to be the member's principal residence; and (b) whether the member appears innocent of any collusion or complicity in the terrorist activity.

Sections 83.15 to 83.17 deal with disposition of the property and interim preservation rights.

(vii) Participating, Facilitating, Instructing and Harboursing

The new terrorism offences includes amendments to the CC which makes it an offence to:

- knowingly participate in or contribute to, directly or indirectly, any activity of a terrorist group for the purpose of enhancing the ability of a terrorist group to facilitate or carry out terrorist activities. (section 83.18);
- knowingly facilitate a terrorist activity, regardless of whether the person knows that a particular terrorist activity was planned or any particular terrorist activity was foreseen or planned when facilitated or whether it was carried out (section 83.19);
- commit any indictable offence for the benefit of, at the direction of, or in association with a terrorist group (s.83.2);
- knowingly instruct another person to carry out any activity for the purpose of enhancing the ability of any terrorist group to carry out a terrorist activity (section 83.21);
- knowingly instruct another person to carry out a terrorist activity (section 83.22);
- knowingly harbour or conceal any person who he or she knows has carried out or is likely to carry out a terrorist activity, for the purpose of enabling the person to facilitate or carry out any terrorist activity (section 83.23).

Under s. 83.18, knowing participation or contribution in an activity of a terrorist group is required. It does not matter if an individual does not know the *specific* nature of the terrorist activity that may be facilitated or carried out as a result of her or his knowing contribution or participation, as it is the individual's purpose to enhance the ability of the group to facilitate or carry out terrorist activities that is in issue. It is of no consequence that participation does not actually enhance a terrorist group's ability to terrorize – it is the individual's knowing participation or contribution for the purpose of enhancing the ability of any terrorist group to facilitate or carry out a terrorist activity that is critical. "Participating in" or "contributing to" an activity of a terrorist group includes recruiting, training, providing or offering skills or expertise, or entering or remaining in any country, for the benefit of, at the direction of or in association with a terrorist group.

Section 83.2 makes it a separate offence to commit any indictable offence under the Criminal Code or any other Act for the benefit of, at the direction of, or in association with a terrorist group, with a maximum sentence of life imprisonment.

(viii) Proceedings and Aggravated Punishment

Pursuant to section 83.26, sentences imposed for the terrorism offences created under Part II.1 are to be served consecutively to any other sentence imposed for an offence arising out of the same event or series of events, or to any other sentence, other than life imprisonment, to which the person is already subject.

Section 83.27 stipulates that an offender convicted of any indictable offence, other than an offence that carries a minimum punishment of life imprisonment, where the offence also constitutes a terrorist activity will be liable to life imprisonment, regardless of the penalty that would otherwise be applicable. This is a penalty enhancement provision applicable when a person is convicted under the relevant offence provision, unlike section 83.2, which provides for an offence which is additional to the predicate offence. Section 83.27 requires that the prosecutor has notified the offender that this provision would be invoked before plea.

(ix) Investigative Hearing

Sections 83.28 and 83.29 provide for a procedural mechanism to gather information for the purpose of investigating or preventing terrorism offences from persons believed on reasonable grounds to have relevant information. A peace officer, on the consent of the Attorney General, may apply *ex parte* to a judge for an order that requires individuals with information relevant to an ongoing investigation of a terrorist offence to appear before a judge and provide that information.

Investigative hearings may be ordered where the judge is satisfied that

- there are reasonable grounds to believe that a terrorism offence has been committed, and that information about the offence, or the whereabouts of the suspected perpetrator, is likely to be obtained as a result of the order; or
- there are reasonable grounds to believe that a terrorism offence will be committed, that the person has direct and material information relating to the offence, or may reveal the whereabouts of the suspected perpetrator who may commit, and that reasonable attempts have been made to get the information from the person to whom the order is sought.

The person named in the order has the right to legal counsel at any stage in the proceedings, but must answer questions and produce things as required by the order. The person may refuse to answer a question or produce a thing that would disclose information protected by law relating to non-disclosure of information or privilege. The presiding judge rules on any refusal to answer a question or produce a thing. The person has no right to refuse to answer questions or produce things on the ground of self-incrimination, but such information, and any evidence derived from it, cannot be used in current or future criminal proceedings against the person, except in prosecutions for perjury or giving contradictory evidence.

The Supreme Court of Canada has reviewed this new procedure in the only case that it has been used in Canada, in relation to the trial concerning the terrorist bombing of Air India. In *Application under s.83.28*⁴, the Supreme Court upheld the constitutionality of the procedure. *Iacobucci and Arbour JJ.* held for the majority that the procedure did not violate s.7 of the Charter given protections in s.83.28(10) that compelled evidence or evidence derived from that evidence could not be used against the person in subsequent criminal prosecutions, as well as the important role that the presiding judge and counsel representing the subject of the investigative hearing would play in the new procedure. The Court indicated that section 7 of the Charter would prevent the use of an investigative hearing if the predominant purpose was to determine penal liability and that it required that the compelled evidence also not be used in subsequent extradition and deportation proceedings.⁵ The majority of the Court rejected arguments that the procedure violated judicial independence and impartiality and stressed the important role of the judge in investigative hearings in ensuring the protection of common law, evidentiary and constitutional rights, as well as the presumption that such hearings be open. Two judges dissented on the basis that the procedure violated the institutional independence of the judiciary by requiring them to preside over police investigations⁶ and three judges dissented on the basis that the particular use of the investigative hearing in relation to the Air India

⁴ 2004 SCC 42

⁵ *Ibid* at para 78-79.

⁶ *Ibid* at para 180.

trial constituted an abuse of process because it was an attempt by the Crown to gain information about a witness in an ongoing criminal trial.

In the companion case of *Re Vancouver Sun*⁷, the Court held that the rebuttable open court principle applied to the conduct of investigative hearings as opposed to the application for a judge to authorize an investigative hearing which, like an application for a search warrant, would be held in private.⁸ Two judges dissented on the basis that such a presumption “would normally defeat the purpose of the proceedings by rendering them ineffective as an investigative tool” and would harm the rights of third parties and the administration of justice.⁹

(x) Recognizance with Conditions

Section 83.3 allows a police officer, with the consent of the Attorney General, who

- believes on reasonable grounds that a terrorist activity will be carried out; and
- suspects on reasonable grounds that the imposition of a recognizance with conditions on a person, or the arrest of a person, is necessary to prevent the carrying out of the terrorist activity.

to lay an information under oath before a provincial court judge. The judge may then compel the person named to appear before the judge.

Sections 83.3(4) and (5) provide for arrest without warrant by which a police officer may arrest a person and bring him or her before a provincial court judge within a specified period of time. In order to make such a preventive arrest without warrant, a peace officer must have a reasonably-grounded suspicion that detention of the person is necessary to prevent a terrorist activity, that the conditions for the laying of an information exist but exigent circumstances make it impracticable to lay an information or an information has already been laid and a summons issued. If an information has not been laid and the person is subject to arrest without a warrant, the police officer shall lay an information and obtain the

⁷ 2004 SCC 43

⁸ The Court added this caveat: “It may very well be that by necessity large parts of judicial investigative hearings will be held in secret. It may also very well be that the very existence of these hearings will at times have to be kept secret. It is too early to determine, in reality, how many hearings will be resorted to and what form they will take. This is an entirely novel procedure, and this is the first case -- to our knowledge -- in which it has been used.” Ibid at para 41 The Court also stated that: “Even in cases where the very existence of an investigative hearing would have been the subject of a sealing order, the investigative judge should put in place, at the end of the hearing, a mechanism whereby its existence, and as much as possible of its content, should be publicly released.” Ibid at para 58.

⁹ Ibid at para 60.

consent of the Attorney General without unreasonable delay and as soon as possible unless the person has been released.

Section 83.3(6) requires the person detained in custody to be taken before a provincial court judge within 24 hours or as soon as possible. A show cause hearing is contemplated under s.83.3(7) to determine if further detention is necessary to ensure the person's attendance, prevent a terrorist activity or interference with the administration of justice or to maintain confidence in the administration of justice. This hearing may be adjourned by a judge, but only for a maximum of a further 48 hours if the person is still in custody.

If satisfied that there is reasonable grounds for the suspicion that the imposition of a recognizance is necessary to prevent a terrorist activity, the judge under s.83.3(8) can order that the person enter into a recognizance to keep the peace and to comply with reasonable conditions for a period not exceeding 12 months. If the person refuses to enter into the recognizance, the judge under s.83.3(9) can commit the person to prison for a term not exceeding 12 months.

(xi) Annual Reports and Sunset Clause

Pursuant to section 83.31(1) and 83.31(2), the Attorney General of Canada and the Attorney General of every province are required to report annually on the use of the investigative hearings and the recognizance with conditions provisions. The Solicitor General of Canada and the Minister responsible for policing in every province are required under section 83.31(3) to report annually on the use of the arrest without warrant power in relation to the use of a recognizance with conditions. The annual reports shall not contain any information that would compromise or hinder an ongoing investigation of an offence under an Act of Parliament, endanger the life or safety of any person, prejudice a legal proceeding or otherwise be contrary to the public interest.

Both the investigative hearing and recognizance with conditions provisions are subject to a five year sunset provision under s.83.32. They may be extended by a resolution passed by both Houses of Parliament and subsequent extensions are possible.

(xii) Parliamentary Review of the *Anti-Terrorism Act*

Section 145 of the *Anti-terrorism Act* provides that a committee or committees of Parliament undertake a comprehensive review of the provisions and operation of the Act within three years from the date that the Act received royal assent (which was December 18, 2001). Generally, the committee(s) must report to Parliament within one year after undertaking the review.

b. Part VI – Invasion of Privacy

(i) Wiretapping Provision Prior to Bill C-36

Under Part VI, prior to Bill C-36, police had investigative powers of certain offences that included interception of private communications (i.e. wiretapping). Normally, exercise of these powers requires an *ex parte* application to the court for authorization upon describing the offence at issue and demonstrating that “other investigative procedures have been tried and have failed or why it appears they are unlikely to succeed or that the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures”. Section 187 provides that all documents relating to an application are confidential and sealed by the court.

Conventional authorizations to intercept private communications can only be valid for a period not exceeding 60 days. Section 196 requires that written notification be given to persons who have been the objects of authorized interceptions within 90 days after the period for which the authorization was given or renewed. Section 195 describes the yearly reporting requirements imposed upon certain ministers in respect of conventional and emergency authorizations obtained upon application of agents and peace officers.

In 1997, Bill C-95 made changes to these provisions in order to combat organized crime. In relation to criminal organization offences, the need to demonstrate that other investigative procedures have been tried and failed, etc., is not required (paragraphs 186(1.1)(a)(b)); this period of an authorization or its renewal may be valid for one or more periods exceeding 60 days, each not exceeding one year (paragraphs 186.1(a)(b)); and the period for giving written notification of the wiretap can be extended, or subsequently extended, for up to a year (paragraphs 196(5)(a)(b)).

(ii) Wiretapping Amendments Relating to Terrorism Offences and Groups

Bill C-36 amended Part VI so that the wiretapping provisions apply to all of the terrorism offences (section 183). The exemptions and extended time periods provided for in 1997 in relation to criminal organization offences were also made applicable to terrorism offences namely:

- 1) Sections 185(1.1) and 186(1.1) eliminate the need to demonstrate in an application for wiretapping authorization that interception of private communications is a last resort in the investigation of terrorism offences;

- 2) Section 186.1 extends the period of validity of a wiretap authorization from 60 days to up to one year when police are investigating a terrorist offence;
- 3) Section 196(5) allows the requirement to notify a target after surveillance has taken place to be delayed for up to three years.

c. Part VIII – Offences Against the Person and Reputation

Section 231 of the CC has been amended so that, irrespective of whether a murder is planned or deliberated, if a death is caused while committing or attempting to commit an indictable offence where the act or omission constituting the offence also constitutes a terrorist activity, then the murder is deemed to be first degree murder.

Section 320.1 allows courts to order the deletion of publicly available hate propaganda from computer systems such as an internet site. The provision applies to hate propaganda that is located on Canadian computer systems, regardless of where the owner of the material is located.

d. Part XI – Wilful and Forbidden Acts in Respect of Certain Property

Section 430(4.1) creates a new offence of mischief motivated by bias, prejudice or hate based on religion, race, colour or national or ethnic origin, committed against a place of religious worship or associated religious property, including cemeteries.

Section 431.2(2) creates a new offence relating to the placement of explosives or other lethal devices in “a place of public use”, “a government or public facility”, “a public transportation system” or an “infrastructure facility”. The intent to cause death or serious bodily injury or to cause extensive destruction that results in or is likely to result in major economic loss is required. The offence is punishable by life in prison.

e. Part XII.2 – Proceeds of Crime

Under the income tax information disclosure provisions in the CC, section 462.48 (1.1) provides that the Attorney General may make an application for an order for disclosure of information with respect to an investigation in relation to a terrorism offence.

f. Part XV – Special Procedure and Powers

Some amendments have been made to section 486 to provide for certain procedures when evidence is being given in the case of an accused charged with

a terrorism offence, such as testimony behind a screen and publication bans. In addition, amendments allow for the collection and retention of DNA samples in relation to various existing and new offences relating to terrorism.

g. Part XXIII – Sentencing

Section 743.6(1.2) provides for a delay in the parole eligibility date (to one half, from the normal one-third) on conviction of a terrorism offence subject to a discretionary power in the court to relieve the accused from the effect of this provision in appropriate cases.

h. Part XXVII – Summary Convictions

Section 810.01 extends peace bond provisions to cases where there are reasonable fears about the commission of a terrorism offence. A recognizance can be ordered for up to 12 months, breach of which is punishable by up to two years imprisonment. The Attorney General's reporting requirements under s.83.31 do not apply to such peace bonds.

3. Bill C-24, *An Act to Amend the Criminal Code (organized crime and law enforcement) and to Make Consequential Amendments to Other Acts* S.C. 2001 c.32

This Act gives public officers, including customs officers as well as police officers, the power to commit acts that would otherwise constitute an offence. The police officer must be engaged in the investigation of criminal activity or enforcement of an act of Parliament, must be designated by a senior officer responsible for law enforcement and must believe on reasonable grounds that the commission of the act or omission as compared to the nature of the offence or criminal activity being designated is reasonable and proportional in the circumstances. (Criminal Code s.25.1(8)). If the activity is likely to result in loss of or serious damage to property, additional authorization from a senior officer is required (s.25.1(9)). There are also provisions for public officers directing third parties to commit offences (s.25.1(10)). The intentional or criminally negligent causing of death or bodily harm to another person, the wilful attempt to obstruct justice and the violation of the sexual integrity of an individual is never justified under this section (s.25.1(11)).

The new provision provides a number of accountability measures. The public officer who commits the act must as soon as feasible file a written report to a senior officer under s.25.2 and public annual reports must be filed under s.25.3. As soon as feasible and no later than a year, a person's whose property was lost or seriously damaged must be notified under s.25.4 unless the Minister responsible for the RCMP is of the opinion that notification would compromise an ongoing investigation, compromise an undercover officer or confidential

informant, endanger the life or safety of any person, prejudice a legal proceeding or be otherwise contrary to the public interest.

4. Canada Evidence Act, R.S.C. 1985, c. C-5

a. Specified Public Interest

Section 37 of the Act provides that a government official may object to the disclosure of information before a court, person or body on the grounds of a specified public interest. The court may order disclosure or prohibit disclosure by weighing the public interest in disclosure against the importance of the specified public interest. Pursuant to subsection 37.21, as originally enacted as part of Bill C-36, a hearing or an appeal of an order under this section shall be heard in private. In 2004, this provision was repealed so that, rather than being required to conduct a hearing *in camera*, a court can now exercise its inherent jurisdiction to provide for such a hearing when the need arises. See *An Act to amend the Criminal Code and Other Acts*, S.C. 2004, c. 12.

b. International Relations, National Defence and National Security

Section 38 of the Act deals with the disclosure of sensitive or potentially injurious information in the course of legal proceedings. Pursuant to section 38.01(1), “every participant who, in connection with a proceeding, is required to disclose, or expects to disclose or cause the disclosure of, information that the participant believes is sensitive information or potentially injurious information shall, as soon as possible, notify the Attorney General of Canada in writing of the possibility of the disclosure, and of the nature, date and place of proceeding” (emphasis added). Pursuant to section 38.01(3), “an official, other than a participant, who believes that sensitive information or potentially injurious information may be disclosed in connection with a proceeding may notify the Attorney General of Canada in writing of the possibility of the disclosure, and of the nature, date and place of proceeding”.

“Sensitive information” is defined as

“information relating to international relations or national defence or national security that is in the possession of the Government of Canada, whether originating from inside or outside Canada, and is of a type that the Government of Canada is taking measures to safeguard.”

“Potentially injurious information” is defined as

“information of a type, that if it were disclosed to the public, could injure international relations or national defence or national security.”

Pursuant to section 38.04, the Attorney General may apply to the Federal Court for an order with respect to the disclosure of information about which notice was given. A person, other than a witness, who is required to disclose information shall, in certain circumstances, apply to the Federal Court pursuant to section 38.04(2)b). In addition, a person who wishes to disclose, or cause the disclosure of, information in connection with a proceeding may apply to the Federal Court pursuant to 38.04(2)c) This application is confidential and measures may be taken by the court to protect the confidentiality of the application. Pursuant to subsection 38.06(1), “[u]nless the judge concludes that the disclosure of the information would be injurious to international relations or national defence or national security, the judge may, by order, authorize the disclosure of the information”.

Pursuant to subsection 38.06(2), “[i]f the judge concludes that the disclosure of the information would be injurious to international relations or national defence or national security but that the public interest in disclosure outweighs in importance the public interest in non-disclosure, the judge may by order, after considering both the public interest in disclosure and the form of and conditions to disclosure that are most likely to limit any injury to international relations or national defence or national security resulting from disclosure, authorize the disclosure, subject to any conditions the judge considers appropriate, of all of the information, a part or summary of the information, or a written admission of facts relating to the information”. Pursuant to subsection 38.06(3), “[i]f the judge does not authorize disclosure under subsection (1) or (2), the judge shall, by order, confirm the prohibition of disclosure”.

Pursuant to subsection 38.11(1)-(2), a hearing or an appeal or review of an order made under any of subsections 38.06(1)-(3) shall be heard in private, and the judge or court may give any person who makes representations, and shall give the Attorney General (and in some cases the Minister of National Defence), the opportunity to make representations *ex parte*. Pursuant to section 38.12, the judge or court may make any order that is considered to be appropriate in the circumstances to protect the confidentiality of the information to which the hearing, appeal or review relates. The court records are confidential and a judge may order that the records be sealed and kept in a location where the public has no access.

Under section 38.13, the Attorney General may personally issue a certificate that prohibits the disclosure of information in connection with a proceeding for the purpose of protecting information obtained in confidence from, or in relation to, a foreign entity (as defined in the *Security of Information Act*) or for the purpose of protecting national defence or national security. The certificate may only be issued after an order or decision that would result in the disclosure of the information to be subject to the certificate has been made under this or any other

Act of Parliament. This certificate expires 15 years after the day on which it was issued.

Under section 38.131, a party to the proceeding referred to in section 38.13 may apply to the Federal Court of Appeal for an order varying or cancelling the certificate. The judge who hears the application must make an order varying or cancelling the certificate if part or all of the information subject to the certificate does not relate to information obtained in confidence from or in relation to a foreign entity or to national defence or security. However, the judge must make an order to confirm the certificate if all of the information subject to the certificate relates to information contained in confidence from, or in relation to a foreign entity (as defined in the *Security of Information Act*) or for the purpose of protecting national defence or security. The judge's determination of this matter is final and is not subject to appeal. Section 38.14 recognizes that a criminal trial judge may make any order that is appropriate to protect the accused's right to a fair trial, such as an order that stays proceedings, so long as it complies with a valid certificate issued under 38.13 or any order made under s. 38.06.

5. *Access to Information Act, R.S. 1985 c. A-1, Personal Information Protection and Electronic Documents Act, 2000, c-5, Privacy Act, R.S. 1985 c. P-21*

Bill C-36 amended access to information and privacy legislation by providing that where a certificate under section 38.13 of the *Canada Evidence Act* prohibiting the disclosure of information (contained in a record or the personal information of a specific individual) is issued before a complaint is filed under the above Acts in respect of a request for access to that information, these Acts do not apply to that information. The amendments continue by stating that where this type of certificate is issued after the filing of a complaint under any of these Acts, then all the proceedings under these Acts are discontinued and the Access to Information or Privacy Commissioner, as the case may be, must not disclose the information and must return the information to the head of the government institution that controls or provided the information.

6. *Security of Information Act, R.S. 1985, c. O-5*

The *Anti-terrorism Act* substantially amended the *Official Secrets Act* and re-named it the *Security of Information Act*. Before the 2001 amendments both terrorist groups and terrorist activities were not part of the act and the act focused on foreign powers. The act now focuses on terrorist groups as well as foreign powers and has the same definition of terrorist groups and terrorist activities as under the *Criminal Code* amendments examined above. The definition of a foreign power now also includes governments in waiting and governments in

exile as well as associations of foreign governments, governments in waiting and governments in exile with one or more terrorist groups.

The old *Official Secrets Act* created espionage offences where the Crown could prove that disclosure was for 'a purpose prejudicial to the safety or interests of the state' (undefined). The new *Security of Information Act* defines this phrase in detail in paragraphs 3(1)(a) to (n) of the Act. Section 3 provides a new and comprehensive definition of "a purpose prejudicial to the safety or interests of the State" as the following:

- offences against the laws of Canada for a political, religious or ideological purpose or to benefit a foreign entity or a terrorist group;
- a terrorist activity inside or outside of Canada;
- endangerment of life, health and safety;
- interference with public or private services and computer or computer programs;
- damage to certain persons or property outside of Canada;
- impairment or interference with the Canadian Forces;
- impairment with Canadian security and intelligence capabilities;
- impairment with Canadian responses to economic threats or instability;
- impairment with Canadian diplomatic, consular and international relations;
- use of toxic or radioactive or explosive devices contrary to international treaty;
- the doing or omitting to do anything in preparation for the above activities.

The term "purpose prejudicial to the safety or interests of the State" is incorporated in many offences under the Act. These offences include under s.4 the otherwise un-amended offence of wrongful communication, use, reception or retention of confidential or other information. This section has been referred to Parliament for review.¹⁰

Section 5 provides for an offence of unauthorized use of uniforms, falsification of reports, forgery, personation and false documents for the purpose of gaining admission to a prohibited place or for any other purpose prejudicial to the safety or interests of the State.

Section 6 makes it an offence to approach or pass over a prohibited place for any purpose prejudicial to the safety or interests of the State at the direction or for the benefit of or in association with a foreign entity or a terrorist group.

Section 7 makes it an offence for a person who, in the vicinity of a prohibited place, obstructs, knowingly misleads or otherwise interferes with or impedes a

¹⁰ Press release www.psepc-sppcc.gc.ca/publications/news/20040129_e.asp

peace officer or a member of Her Majesty's forces engaged on guard, sentry, patrol or other similar duty in relation to the prohibited place.

Instead of referring to “classified information”, the new Act uses the phrase “information that the Government of Canada is taking measures to safeguard”. The concept here is that in any prosecution, the Crown will have to show that the Government has taken some measures to protect the information. Security classification would presumably be one but not the only way of showing this. For example, if the Director of CSIS tells an employee not to disclose the foreign location of a meeting with a human source that could (subject to proof in court) be information the Government has 'taken measures to safeguard'. This information would fall within the provisions of the *Security of Information Act* even though it was not contained in a classified document.

There is also a new concept which attempts to define the most operationally sensitive kind of Government information; 'special operational information'. This concept is defined in section 8 of the Act as follows:

“Special operational information” means information that the Government of Canada is taking measures to safeguard that reveals, or from which may be inferred,

- (a) the identity of a person, agency, group, body or entity that is or is intended to be, has been approached to be, or has offered or agreed to be, a confidential source of information, intelligence or assistance to the Government of Canada;
- (b) the nature or content of plans of the Government of Canada for military operations in respect of a potential, imminent or present armed conflict;
- (c) the means that the Government of Canada used, uses or intends to use, or is capable of using, to covertly collect or obtain, or to decipher, assess, analyze, process, handle, report, communicate or otherwise deal with information or intelligence, including any vulnerabilities or limitations of those means;
- (d) whether a place, person, agency, group, body or entity was, is or is intended to be the object of a covert investigation, or a covert collection of information or intelligence, by the Government of Canada;
- (e) the identity of any person who is, has been or is intended to be covertly engaged in an information- or intelligence-collection activity or program of the Government of Canada that is covert in nature;
- (f) the means that the Government of Canada used, uses or intends to use, or is capable of using, to protect or exploit any information or

intelligence referred to in any of paragraphs (a) to (e), including, but not limited to, encryption and cryptographic systems, and any vulnerabilities or limitations of those means; or

- (g) information or intelligence similar in nature to information or intelligence referred to in any of paragraphs (a) to (f) that is in relation to, or received from, a foreign entity or terrorist group.

Another new concept introduced in this Act is the description of individuals who should be held to a higher level of accountability for unauthorized communication or confirmation of special operational information. This concept is that of "persons permanently bound to secrecy". This concept is defined in section 8 of the Act as follows:

"person permanently bound to secrecy" means

- (a) a current or former member or employee of a department, division, branch or office of the public service of Canada, or any of its parts, set out in the schedule (to the Act); or
- (b) a person who has been personally served with a notice issued under subsection 10(1) in respect of the person or who has been informed, in accordance with regulations made under subsection 11(2), of the issuance of such a notice in respect of the person (in other words, by notice).

Section 13 creates an offence - for which the maximum penalty is 5 years less a day - for those persons permanently bound to secrecy who 'intentionally and without authority communicate or confirm information that, if it were true, would be special operational information'. This offence of purported communication recognizes both that (a) insiders are under a special duty with respect to the most sensitive information they had or have access to and (b) that the Crown does not need to prove the truth of the information (since experience has shown that to do so can simply increase the harm already done). Therefore, for example, former or current employees of CSIS who publicly reveal the identity of targets or sources of the Service can be prosecuted whether or not the information is true and without the Crown having to address this issue at all.

Section 14 makes it an offence for a person permanently bound to secrecy to intentionally and without lawful authority communicate or confirm special operational information. It is punishable by up to 14 years' imprisonment.

For both of these offences, section 15 of the Act provides a 'public interest' defence - if an accused can show that information has been disclosed 'for the purpose of disclosing an offence under an Act of Parliament that he or she reasonably believes has been, is being or is about to be committed by another

person in the purported performance of that person's duties and functions for, or on behalf of, the Government of Canada and the public interest in the disclosure outweighs the public interest in non-disclosure. The section sets out factors that a judge must consider when deciding if the public interest in disclosure outweighs the public interest in non-disclosure. They include: the seriousness of the offences, the extent of the disclosure, the harm caused by the disclosure and whether the accused resorted to 'other reasonably accessible alternatives' before disclosing the information. In addition, this public interest defence can only be relied on if the accused has first (a) advised his or her Deputy Minister (or the Attorney General of Canada) and (b) if this fails, brought his or her concerns to the attention of either the Security Intelligence Review Committee or the Communications Security Establishment Commissioner.

Section 16 sets out two offences. By subsection 16(1), every person commits an offence who, without lawful authority, communicates to a foreign entity or a terrorist group information that the Government of Canada or of a province is taking measures to safeguard, if the person believes or is reckless as to whether the information is information that the Government of Canada or of the province is taking measures to safeguard and the person intends, by communicating the information, to increase the capacity of a foreign entity or a terrorist group to harm Canadian interests or is reckless as to whether the communication of the information is likely to increase the capacity of the foreign entity or terrorist group to harm Canadian interests.. By subsection 16(2), every person commits an offence who, without lawful authority, communicates to a foreign entity or a terrorist group information that the Government of Canada or of a province is taking measures to safeguard, if the person believes or is reckless as to whether the information is information that the Government of Canada or of the province is taking measures to safeguard and harm to Canadian interests results. A person who commits any of these two crimes is liable to imprisonment for life.

Section 17 provides that every person commits an offence who, intentionally and without lawful authority, communicates "special operational information" to a foreign entity or terrorist group if the person believes, or is reckless as to whether the information is special operational information. Here, unlike the offences in section 16, no intent to harm, recklessness as to the capacity to harm, or actual harm to Canadian interests is required. This offence is punishable by up to life in prison.

Section 18 focuses on the breach of trust in respect of safeguarded information by a person with a security clearance. It provides that every person with a security clearance given by the Government of Canada who, intentionally and without lawful authority, communicates, or agrees to communicate, to a foreign entity or terrorist group any information that is of a type that the Government of Canada is taking measures to safeguard commits an offence and is liable to imprisonment for two years.

Section 19 focuses on economic espionage. It provides that every person commits an offence who, at the direction of, for the benefit of, or in association with a foreign economic entity (as defined by the Act), fraudulently and without colour of right and to the detriment of Canada's economic interests, international relations or national defence or national security communicates a trade secret to another person, group or organization or obtains, retains, or destroys a trade secret. The offence is punishable by up to 10 years in prison.

Section 20 provides that every person commits an offence who, at the direction of, for the benefit of, or in association with a foreign entity or terrorist group induces or attempts to induce, by threat, accusation, menace or violence, any person to do anything or to cause anything to be done that is for the purpose of increasing the capacity of a foreign entity or a terrorist group to harm Canadian interests or that is reasonably likely to harm Canadian interests, whether or not the threat, accusation, menace or violence occurred in Canada. The punishment is up to life in prison.

Section 21 makes it an offence for a person who, for the purpose of enabling or facilitating an offence under the Act, knowingly harbours or conceals a person whom he or she knows to be a person who has committed or is likely to commit an offence under the Act.

Section 22 sets out a number of offences that are preparatory acts done for the purpose of committing certain offences under the Act. Every person commits an offence who, for the purpose of committing an offence under subsection 16(1) or (2) [communicating safeguarded information], 17(1), [communicating special operational information], 19(1) [economic espionage] or 20(1) [foreign-influenced or terrorist-influenced threats or violence], does anything that is specifically directed towards or specifically done in preparation of the commission of the offence, including

- (a) entering Canada at the direction of or for the benefit of a foreign entity, a terrorist group or a foreign economic entity;
- (b) obtaining, retaining or gaining access to any information;
- (c) knowingly communicating to a foreign entity, a terrorist group or a foreign economic entity the person's willingness to commit the offence;
- (d) at the direction of, for the benefit of or in association with a foreign entity, a terrorist group or a foreign economic entity, asking a person to commit the offence; and
- (e) possessing any device, apparatus or software useful for concealing the content of information or for surreptitiously communicating, obtaining or retaining information.

Section 23 makes it an offence to conspire, attempt to commit, be an accessory after the fact or counsel in relation to an offence under the Act. A person is liable to the same punishment as is provided for the completed offence.

Section 24 requires the consent of the Attorney General of Canada before any prosecution can take place for an offence against the Act. Pursuant to section 26 extraterritorial jurisdiction exists in certain circumstances (e.g., where the person who commits the act or omission outside Canada is a Canadian citizen).

7. *Canadian Security Intelligence Service Act, R.S. 1985, c. C-23*

This Act creates the Canadian Security Intelligence Service (CSIS) which is a domestic civilian agency that provides security intelligence to the Government. The Director of the Service is appointed by the Governor in Council (s.4). The Director, under the direction of the Minister (who is the Solicitor General of Canada), has the control and management of the Service and all matters connected therewith (subs.6(1)). The Minister “may issue to the Director written directions with respect to the Service”, with a copy being issued forthwith to the Security Intelligence Review Committee.

CSIS is required to collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyze and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada, and, in relation thereto, must report to and advise the Government of Canada (s.12). It may also provide security assessments to departments of the Government of Canada (subs.13(1)), or, with the approval of the Minister, enter into arrangements with the government of a province or any police force in a province, with the approval of the minister responsible for policing in the province, authorizing the Service to provide security assessments (subs.13(2)). It may also, with the approval of the Minister and after consultation with the Minister of Foreign Affairs, enter into similar arrangements with the government of a foreign state or an international organization of states or an institution of either of them (subs. 13(3)).

“Threats to the security of Canada” means

- espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage;
- foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person;

- activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state;¹¹ and
- activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada.

but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities described above.

“Security assessment” means an appraisal of the loyalty to Canada and, so far as it relates thereto, the reliability of an individual.

CSIS may advise any minister of the Crown on matters relating to the security of Canada, or provide any minister of the Crown with information relating to security matters or criminal activities, that is relevant to the exercise of any power or the performance of any duty or function by that Minister under the *Citizenship Act* or the *Immigration and Refugee Protection Act* (s. 14). CSIS may conduct such investigations as are required for the purpose of providing security assessments pursuant to section 13 or advice pursuant to section 14.

Under subsection 16(1) of the Act, in relation to the defence or conduct of the international affairs of Canada, CSIS may assist the Ministers of Defence or the Minister of Foreign Affairs, within Canada, in collecting information or intelligence relating to the capabilities, intentions or activities of any foreign state or group of states, or of any person who is not a Canadian citizen, permanent resident of Canada or corporation incorporated by or under an Act of Parliament or a provincial legislature. However, CSIS must not perform its duties and functions under subsection 16(1) unless it does so: (a) on the personal request in writing of the Minister of National Defence or the Minister of Foreign Affairs; and (b) with the personal consent in writing of the Minister (i.e., the Solicitor General of Canada) (subs. 16(3)).

CSIS may, with the approval of the Minister, enter into an arrangement with any department of the government or, with the approval of the Minister and after consultation with the Minister of Foreign Affairs, into any arrangement with the government of a foreign state or an institution thereof for the purpose of performing its duties and functions (s.17).

Sections 18 deals with the offence of disclosing identities of sources or employees involved in covert operations. Section 19 specifies the persons to

¹¹ The addition of the words “religious or ideological” was the only amendment of the *CSIS Act* by Bill C-36.

whom and the purposes for which CSIS may disclose information it obtains in the performance of its duties and functions.

CSIS uses a wide range of investigative techniques and may be authorized to “intercept any communication or obtain any information, record, document or thing” it needs to investigate a threat to the security of Canada or to perform its duties and functions under s.16(1) (s.21(3)). Permission to proceed with intrusive measures is provided by the courts through warrant applications which have been approved by the Solicitor General. (s.21-28). The judge must be satisfied that there are reasonable grounds to believe that a warrant is required to enable the Service to investigate a threat to the security of Canada or perform its duties under s.16 and that other investigative procedures have or would fail or be impractical or not obtain important information. (s.21(2)(b)) An application for a warrant or renewal of a warrant is heard in private (s.27) and is subject to renewal (s.22) and is not subject to the requirements of Part VI of the Criminal Code (s.26).

Sections 30-33 establish the position and functions of the Inspector-General, who is appointed by the Governor in Council and is responsible to the Deputy Minister. The Inspector-General monitors CSIS compliance with its operational policies, reviews CSIS operational activities and certifies his/her degree of satisfaction with the CSIS Director’s classified annual report to the Minister (s.30). The certificate states whether in the opinion of the Inspector-General, CSIS has undertaken any action that contravenes the Act or ministerial direction, or whether CSIS has made any unreasonable or unnecessary use of its powers (s.33(2)). The Inspector-General has access to any information under the control of CSIS that relates to the performance of his/her duties and functions, except for confidences of the Queen's Privy Council for Canada in respect of which subsection 39(1) of the *Canada Evidence Act* applies (in other words, Cabinet confidences) (s.31). The Inspector-General is also entitled to receive information, explanations and reports from the director and employees of CSIS as the Inspector General deems necessary for the performance of those duties and functions (s.31(1)).

Section 34(1) establishes the Security Intelligence Review Committee (SIRC), an external, independent review body, which reviews the performance of CSIS. SIRC consists of 3-5 members of the Privy Council who are not members of the Senate or the House of Commons and who are appointed by the Governor in Council after the Prime Minister consults with the Leader of the Opposition and the Leader of each party having at least 12 Members of Parliament.

SIRC’s mandate is to “review generally the performance by the Service of its duties and functions” and includes (s. 38).

- reviewing the director’s annual report and the Inspector-General’s certificate;

- arranging for or conducting reviews of the legality of CSIS's conduct and whether the activities of the Service involve any unreasonable or unnecessary exercise by the Service of its powers; and
- investigating complaints made against CSIS.

SIRC has access to any information under the control of CSIS or the Inspector-General that relates to the performance of its duties and functions, except for advice to, and certain discussions between ministers (s.39(2)&(3)). SIRC is also entitled to receive information, explanations and reports from the Inspector-General, Director and employees of CSIS (s.39(2)). SIRC has the power to summon witnesses and require them to produce evidence (s. 50). SIRC publishes an annual report on the activities of CSIS to Parliament (s.53).

SIRC also investigates complaints from the public to ensure that the powers of CSIS are used appropriately. Under section 41, SIRC investigates a complaint "with respect to any act or thing done by the Service" and under section 42, SIRC investigates complaints relating to the denial of a security clearance for federal employment or federal contracts. Investigations and hearings are conducted in private and, although a party to the proceedings has the right to make representations to SIRC, no one is entitled as a right to be present when other witnesses give evidence (s.48). Following a hearing, SIRC will set out its findings and any recommendations in a report that is submitted to the Minister and Director (s.52). SIRC also provides the complainant with the report, taking into consideration the obligation to protect sensitive information (s.52).

Pursuant to the Act and its Rules of Procedure, SIRC may also receive

- referrals from the Canadian Human Commission that relate to the security of Canada made pursuant to the *Canadian Human Rights Act*. Upon receipt of such a referral, the Committee carries out an investigation and reports its findings to the Commission, the respondent and the complainant; and
- reports from the Minister responsible for Citizenship under the *Citizenship Act* if that Minister is of the opinion that a person should not be granted citizenship, or should be issued a certificate of renunciation of citizenship, because there are reasonable grounds to believe that the person will engage in activities that constitute a threat to the security of Canada or organized criminal activities. Upon receipt of such a report, SIRC carries out an investigation and reports its findings to the Governor in Council.

8. **Royal Canadian Mounted Police Act, R.S.C. 1985, c. R-10**

The Royal Canadian Mounted Police (RCMP), Canada's federal law enforcement agency, as well as other police officers, have, through the 2001 enactment of Bill C-36 of terrorism offences and the creation of powers such as an investigative hearing an even more important role in investigating and preventing terrorist activity that before 2001 would have been investigated and prevented under the existing offences of the *Criminal Code* and the *Security Offences Act*.

Section 3 of the Act establishes Canada's national police force and section 4 provides that the RCMP may be employed both within and outside Canada. The RCMP consists of a Commissioner who controls and manages the RCMP under the direction of the Solicitor General of Canada (s.5)¹², officers (s.6) and other members and supernumerary special constables (s.7), as well as civilian staff (s.10).

Every officer and every other person designated as a peace officer under subsection 7(1) (e.g., a member other than an officer) is a peace officer in every part of Canada and has the powers, authority, protection and privileges that a peace officer has by law until dismissed or discharged (s.9).

Section 18 provides that it is the duty of members who are peace officers, subject to the orders of the Commissioner,

- to perform all duties that are assigned to peace officers in relation to the preservation of the peace, the prevention of crime and of offences against the laws of Canada and the laws in force in any province in which they may be employed, and the apprehension of criminals and offenders and others who may be lawfully taken into custody;
- to execute all warrants, and perform all duties and services in relation thereto, that may, under the RCMP Act or the laws of Canada or the laws in force in any province, be lawfully executed and performed by peace officers;
- to perform all duties that may be lawfully performed by peace officers in relation to the escort and conveyance of convicts and other persons in custody to or from any courts, places of punishment or confinement, asylums or other places; and
- to perform such other duties and functions as are prescribed by the Governor in Council or the Commissioner.

¹² This reference to Ministerial direction has, however, been qualified, in *R. v. Campbell*, [1999] 1 S.C.R. 565 at para. 33, to exclude Ministerial direction of criminal investigations.

Section 24.1 provides for the Minister or the Commissioner to appoint a board of inquiry to investigate the conduct of members and employees. Boards can compel testimony and their hearings are conducted in private unless the Minister or Commissioner directs otherwise.

The RCMP External Review Committee (ERC), established under section 25, reviews certain types of grievances, decisions of formal disciplinary hearings that are referred by the Commissioner of the RCMP when an appeal is being sought, and decisions of discharge and demotion boards referred by the Commissioner when an appeal is being sought (s.25-36).

Section 37 of the Act sets out the standards that must be met by every member of the RCMP and, pursuant to section 38 and *RCMP Regulations 1988*, a Code of Conduct governs the conduct of members. The standards in section 37 include respecting the rights of all persons and ensuring that any improper or unlawful conduct of any member is not concealed or permitted to continue. The Code of Conduct includes requirements to obey lawful orders, not publicly criticize the Force unless authorized by law, obligations to aid a person exposed to danger or in impending danger, not to destroy or conceal official documents, and to respect the rights of every person including rights against discrimination.

Informal and formal disciplinary action may be taken in respect of a contravention of the Code of Conduct (s.41-45.17). Sections 45.18-45.28 focus on the discharge and demotion procedure for officers including the Commissioner, Deputy Commissioners, Chief Superintendents, Superintendents and Inspectors, as well as other members who are not officers.

Part VI of the Act establishes and organizes the Commission for Public Complaints Against the RCMP (CPC) whose mandate under Part VII is to review public complaints about RCMP members' conduct (s.45.29(1), 45.32(1) and 45.35(1)). Part VII of the Act sets out the procedure for making complaints and for review by the Commission of those complaints.

Under Part VII, any member of the public having a complaint concerning the conduct, in the performance of any duty or function under the RCMP Act or the *Witness Protection Program Act*, of any member or other person appointed or employed under the authority of the Act may, whether or not that member of the public is affected by the subject-matter of the complaint, make a complaint to the Commission, any member or other person appointed or employed under the authority of the RCMP Act, or the provincial authority in the province in which the subject-matter of the complaint arose that is responsible for the receipt and investigation of complaints by the public against police. The Commissioner of the RCMP is to be notified of every complaint so made.

Subsection 45.36(1) to(3) of the Act provides for a procedure for attempting to informally dispose of a complaint where the complainant and the RCMP member

who is the subject of the complaint consent to the attempt. Where complaints are not disposed of informally, generally the RCMP initially investigates the complaint and provides a report to the complainant (s.45.36(4) and s.45.4). However, by subsection 45.36(5), the Commissioner of the RCMP may direct that no investigation of a complaint be commenced or that an investigation of such a complaint be terminated if, in the Commissioner's opinion,(a) the complaint is one that could more appropriately be dealt with, initially or completely, according to a procedure provided under any other Act of Parliament; (b) the complaint is trivial, frivolous, vexatious or made in bad faith; or (c) having regard to all the circumstances, investigation or further investigation is not necessary or reasonably practicable.

If the complainant is not satisfied with the RCMP's disposition of the complaint or a direction under section 45.36(5), he or she may ask the CPC to conduct a review under section 45.41. The Chair of the Commission is then required to review the complaint. If satisfied with the RCMP's disposition of the complaint, the Chair sends a written report to that affect to the Minister, the Commissioner, the RCMP member who is the subject of the complaint, and to the person who complained to the Commission.

However, if, on review of the complaint, the Chair of the CPC is dissatisfied with the disposition of the complaint by the RCMP, the Chair may

- (a) prepare and send to the Minister and the Commissioner a report in writing setting out such findings and recommendations with respect to the complaint as the Commission Chairman sees fit;
- (b) request the Commissioner to conduct a further investigation into the complaint; or
- (c) investigate the complaint further or institute a hearing to inquire into the complaint (s. 45.42(3)).

The Chair of the CPC may also initiate a complaint where he or she is satisfied that there are reasonable grounds to investigate the conduct of any member (s.45.37) and this complaint is then investigated by the RCMP (s.45.37(4)). For example, the Chair initiated a public complaint relating to the Maher Arar case, but it has since been suspended by the Commission.

The Chair of the CPC may, where he or she deems it to be in the public interest, investigate or institute a public hearing to inquire into a complaint concerning the conduct of a member whether or not the complaint has been investigated, reported on or otherwise dealt with by the RCMP (s.45.43(1)). In this situation, the RCMP is not required to investigate or deal with the complaint until the CPC provides it with a report (s.45.43(2)).

The CPC's powers to access information are not specified in the Act.

By subsection 45.45(4), when holding a public hearing the Commission has, in relation to the complaint before it, the powers conferred on a board of inquiry, in relation to the matter before it, by paragraphs 24.1(3)(a), (b) and (c) of the *RCMP Act* (such as the power to summons a person and receive evidence on oath). Section 45.45(11) allows the Commission to order that a hearing or part of a hearing shall be held in private if

- the disclosure of the information could reasonably be expected to be injurious to the defence of Canada or any state allied or associated with Canada or the detection, prevention or suppression of subversive or hostile activities;
- the disclosure of the information could reasonably be expected to be injurious to law enforcement; or
- it is information respecting a person's financial or personal affairs where that person's interests or security outweighs the public's interest in the information.

Where the Chair is dissatisfied with the disposition of a complaint by the RCMP, when the review is complete, the Chair sends an interim report to the RCMP Commissioner and to the Solicitor General of Canada setting out his or her findings and recommendations. The Commissioner then informs the Chair and the Solicitor General of Canada, in writing, of any action to be taken in response to the Chair's findings and recommendations. Should the Commissioner reject any findings or recommendations, the Commissioner must include in this notice the reasons for the rejection. The Chair then prepares a final report that includes the Commissioner's response, as well as the Chair's final findings and recommendations and sends it to everyone involved. This procedure is also used in the case of a public interest investigation and a public hearing.

The CPC submits an annual report of its activities to Parliament (s.45.34).

9. Security Offences Act, R.S. 1985, c. S-7

Pursuant to section 2 of the Act, the Attorney General of Canada may conduct proceedings in respect of an offence under any law of Canada where

- the alleged offence arises out of conduct constituting a threat to the security of Canada within the meaning of the *CSIS Act*; or
- the victim of the alleged offence is an internationally protected person within the meaning of section 2 of the *Criminal Code*.

Section 3 of the Act provides that section 2 does not affect the authority of the Attorney General of a province to conduct proceedings in respect of an offence referred to in section 2. However, this is subject to section 4. Section 4 provides that, where the Attorney General of Canada believes that an offence referred to in section 2 has been committed in any province, the Attorney General of Canada may serve a fiat to that effect on the Attorney General of the province. That fiat establishes the “exclusive authority” of the Attorney General of Canada with respect to the conduct of any proceedings in respect of the offence described in the fiat.

Under section 6 of the Act, members of the RCMP who are peace officers have the primary responsibility to perform the duties that are assigned to peace officers in relation to “any offence referred to in section 2 or the apprehension of the commission of such an offence.”

10. *Department of Foreign Affairs and International Trade Act, R.S. 1985, c. E-22*

The former Department of Foreign Affairs and International Trade (DFAIT) has now been split into two separate departments, Foreign Affairs Canada and International Trade Canada. Pursuant to section 10 of this Act, the powers, duties and functions of the Minister of Foreign Affairs extends to, and includes all matters over which Parliament has jurisdiction not by law assigned to any other department, board or agency of the Government of Canada, relating to the conduct of the external affairs of Canada. In exercising his or her duties and functions, the Minister must

- conduct all diplomatic and consular relations on behalf of Canada;
- conduct all official communication between the Government of Canada and the government of any other country and between the Government of Canada and any international organization;
- conduct and manage international negotiations as they relate to Canada;
- coordinate the direction given by the Canadian government to the heads of Canada’s diplomatic and consular missions;
- have the management of Canada’s diplomatic and consular missions;
- administer the foreign service of Canada;

- foster the development of international law and its application in Canada's external relations; and
- carry out such other duties and functions as are by law assigned to him or her.

11. *National Defence Act, R.S. 1985, c. N-5*

The primary focus of the Act is on the Canadian Forces, the Code of Service discipline and complaints about or by military police. However, as discussed below, Part V.1 of the *National Defence Act* R.S. 1985, c. N-5 outlines the legislative framework of the Communications Security Establishment (CSE) and the Commissioner of the CSE.

a. *Defence Intelligence*¹³

Since the primary mandate of the National Defence is defending Canada, intelligence activities abroad or in Canada are conducted in support of this mandate. The Director General Intelligence Division in the Department of National Defence provides defence intelligence on issues involving the use or potential use of the Canadian Forces abroad. As such, they are concerned with defence intelligence. The Department and the Canadian Forces have the capacity to collect domestic intelligence, but do so only in rare circumstances and under clear legal authority in support of domestic Canadian Forces operations. There are three units that may be involved in domestic intelligence collection: the National Counter-Intelligence Unit, the Canadian Forces Information Operations Group, and the Canadian Forces Joint Imagery Centre.

The National Counter-Intelligence Unit is primarily responsible for the identification and investigation of security threats to National Defence and the Canadian Forces. It also provides liaison with other security agencies such as CSIS. Investigations can extend beyond Defence employees where the security of the Department or the Canadian Forces is involved. It is their practice to hand over the investigation to the relevant lead agency, usually the RCMP or CSIS, if the subject matter of the investigation is other than a defence employee. The Canadian Forces Information Operations Group conducts signals intelligence collection activities in support of the Canadian Forces. The Group is also involved in signals intelligence collection in support of the Communications Security Establishment (CSE). In this case, the collection activities are subject to the CSE's mandate and review mechanisms. All of the Canadian Forces Information Operations Group's activities are subject to the laws of Canada, in particular the *Criminal Code* and the *Privacy Act*. The Canadian Forces Joint

¹³ Part of the following information was taken from Chapter 10 – Independent Reviews of Security and Intelligence Agencies in “Other Audit Observations” of the November 2003 Report of the Auditor General of Canada (pg. 35-36).

Imagery Centre may under certain circumstances co-ordinate the collection of images of areas of Canada to support the domestic and international operations of the Canadian Forces. There are express limitations on the role of National Defence and the Canadian Forces in collecting imagery intelligence on Canadian individuals and groups within Canada.

The Joint Task Force Two (JTF 2) of the Canadian Forces is a Special Operations Force that is responsible for federal counter-terrorist operations. The mission of JTF 2 is to provide a force capable of rendering armed assistance in the resolution of an incident that is affecting, or has the potential to affect, the national interest. The JTF 2 falls under the responsibility of the Deputy Chief of the Defence Staff.

b. Communications Security Establishment (CSE)

Bill C-36 added Part V.1 to the *National Defence Act*, R.S. 1985, c. N-5 which outlines the legislative framework of the CSE and the Commissioner of the CSE. The definition section sets out that a “Canadian” means a Canadian citizen, a permanent resident within the meaning of the *Immigration and Refugee Protection Act* or a body corporate incorporated in Canada. “Foreign intelligence” means “information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international affairs, defence or security”. Section 273.62(1) statutorily provides for the continuation of the CSE as a part of the public service of Canada and its mandate, set out in section 273.64(1), is to (a) to acquire and use information from the global information infrastructure (signals intelligence) for the purpose of providing foreign intelligence, in accordance with Government of Canada priorities; (b) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and (c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their duties. However, section 273.64(2) states that activities carried out under paragraphs 1(a) and (b) shall not be directed at Canadians or any person in Canada, and shall be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information.

Bill C-36 amended the *National Defence Act* to clarify the mandate of the CSE to intercept the communications of foreign targets abroad and undertake security checks of government computer networks to protect them from terrorist activity. Thus, the *Anti-Terrorism Act* created broader powers for the CSE. Prior to Bill C-36, the CSE was not permitted to intercept private communications that entered or left Canada. Now, as a result of Bill C-36, the Minister of National Defence may, for the sole purpose of obtaining foreign intelligence, authorize the CSE in writing to intercept such communications if they are acquired while targeting foreign entities abroad during specific or related activities (s.273.65(1)&(2)).

Authorization is based on a number of conditions, including having satisfactory measures in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security (s.273.65(2)(d)). Under section 273.65(3) the Minister may, for the sole purpose of protecting the computer systems or networks of the Government of Canada, authorize the CSE in writing to intercept private communications acquired while targeting foreign entities abroad during specific or related activities. Authorization is based on a number of conditions set out in section 273.65(4). Section 273.65(8) requires the Commissioner of the CSE to review all activities under Ministerial authorizations to ensure that they are authorized and to report the results of this review annually to the Minister.

Pursuant to section 273.66, the CSE can only undertake activities that are within its mandate, consistent with ministerial direction and, if an authorization is required, consistent with the authorization.

Section 273.63 provides for the appointment of a Commissioner of the CSE and stipulates that his or her duties are

- to review the activities of the CSE to ensure that they are in compliance with the law;
- in response to a complaint, to undertake any investigation that the Commissioner considers necessary; and
- to inform the Minister and the Attorney General of Canada of any activity of the CSE that the Commissioner believes may not be in compliance with the law.

The Commissioner must submit an annual report on his or her activities and findings to the Minister who then tables it in Parliament (s.273.63(3)). In carrying out his or her duties, the Commissioner has all the powers of a commissioner under Part II of the *Inquiries Act*.

12. *Charities Registration (Security Information) Act, 2001 c-41*

Enacted under Part 6 of Bill C-36, the *Anti-Terrorism Act*, the purpose of this Act is

- to demonstrate Canada's commitment to participating in concerted international efforts to deny support to those who engage in terrorist activities;

- to protect the integrity of the registration system for charities under the *Income Tax Act*; and
- to maintain the confidence of Canadian taxpayers that the benefits of charitable registration are made available to organizations that operate exclusively for charitable purposes.

Under section 4, the Solicitor General and the Minister of National Revenue may sign a certificate on the basis that they have reasonable grounds to believe, based on security or criminal intelligence reports, that an applicant, to become a registered charity or a registered charity,

- a) has made, makes or will make available any resources, directly or indirectly to a terrorist group listed under s.83.05 of the Criminal Code;
- b) made available any resources to an entity that was at the time and continues to be engaged in terrorist activities or activities in support of them; or
- c) makes or will make available any resources to any entity that engages or will engage in terrorist activities or activities in support of them.

Once the certificate is signed, the applicant or registered charity will be provided with notice of the certificate and the matter will automatically be referred to the Federal Court for judicial review (s.5(1)).

When the certificate is referred to the court, the judge will determine its reasonableness. If the judge is of the view that the disclosure of information would injure national security or endanger the safety of any person, evidence may be heard in the absence of the applicant or registered charity and its lawyer. The applicant will be given an opportunity to be heard and a summary of information considered by the judge unless such a summary would in the judge's view injure national security or endanger the safety of any person.

Section 8 allows for the use of information obtained in confidence from a government, an institution or an agency of a foreign state or from an international organization of states without a summary being provided to the applicant if the judge decides that the information is relevant but that its disclosure would injure national security or endanger the safety of any person.

If a certificate is determined to be reasonable under section 6(1)(d), then the certificate is conclusive proof that an applicant to become a registered charity is ineligible or, in the case of an already registered charity, that the charity does not comply with the requirements to continue to be a registered charity (s.9).

Pursuant to section 10, an applicant or former registered charity can apply to the Ministers for a review of a certificate determined to be reasonable if they believe that there has been a material change in circumstances since the determination. The Ministers have 120 days to decide whether the certificate continues to be reasonable. Section 11 allows the applicant or former registered charity to apply to the Federal Court for a review of the Ministers' decision under section 10 with the judge determining whether the certificate is reasonable on the basis of the information available to the judge. Unless it is cancelled earlier, a certificate is effective for seven years from the date it was determined to be reasonable (s.13).

In order to coordinate with this new Act, section 168 of the *Income Tax Act* was amended by Bill C-36 so that if a registered charity is the subject of a certificate that has been determined to be reasonable, the registration of that charity is revoked as of the making of that determination.

13. *Proceeds of Crime (Money Laundering) and Terrorist Financing Act, 2000* c.17 and the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)

In 2000, the federal government launched the National Initiative to Combat Money Laundering to bring Canada's efforts in line with international standards. Central to this strategy was a new *Proceeds of Crime (Money Laundering) Act* requiring financial institutions to report suspicious transactions. The Act also created the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) which analyses these transaction reports and releases information to intelligence and law enforcement agencies when appropriate. The Act and the mandate of the Centre were amended by Bill C-36 to add provisions to detect and deter terrorist financing. The act is now titled the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. The definition section defines "terrorist activity" as having the same meaning as in the *Criminal Code* and "terrorist activity financing offence" to mean an offence under section 83.02, 83.03 or 83.04 of the *Criminal Code* or under section 83.12 of the Code arising out of a contravention of section 83.08 of the Code. "Threats to the security of Canada" has the same meaning as in section 2 of the *CSIS Act*.

Section 3 states that the object of the Act is

- a) to implement specific measures to detect and deter money laundering and the financing of terrorist activities and to facilitate the investigation and prosecution of money laundering offences and terrorist activity financing offences, including
 - i. establishing record keeping and client identification requirements for financial services providers and other persons or entities that engage in businesses, professions or activities that are susceptible

- to being used for money laundering or the financing of terrorist activities;
- ii. requiring the reporting of suspicious financial transactions and of cross-border movements of currency and monetary instruments; and
 - iii. establishing an agency that is responsible for dealing with reported and other information.
- b) to respond to the threat posed by organized crime by providing law enforcement officials with the information they need to deprive criminals of the proceeds of their criminal activities, while ensuring that appropriate safeguards are put in place to protect the privacy of persons with respect to personal information about themselves; and
- c) to assist in fulfilling Canada's international commitments to participate in the fight against trans-national crime, particularly money laundering, and the fight against terrorist activity.

Part 1 of the Act focuses on record keeping and reporting of suspicious and other prescribed financial transactions and applies to such entities as *inter alia* banks, credit unions, certain companies and persons and entities when they engage in certain business, profession or activity. Pursuant to section 7 these entities must report every financial transaction to FINTRAC that occurs in respect of which there are reasonable grounds to suspect that the transaction is related to a money laundering offence or a terrorist activity financing offence. Pursuant to section 9, these entities must report certain other transactions, (eg. international electronic funds transfers over \$10,000 and large cash transactions over \$10,000).

Part 2 focuses on the cross border movement of currency and monetary instruments. Section 12(1) states that every person or entity must report to an officer (same meaning as in section 2(1) of the *Customs Act*) the importation or exportation of currency or monetary instruments of a value equal to or greater than the prescribed amount. Section 14 states that an officer, after giving notice to the entity, may retain the currency or monetary instruments if an entity has indicated to the officer that they have something to report and the report is not yet complete. Sections 15-17 provide for searches of the person, searches of a conveyance or baggage and the examination and opening of mail if there are reasonable grounds for suspicion. The reasonable suspicion standard relates to unreported currency above an amount proscribed by regulation under s.12.

Sections 18-20 focus on the search and forfeiture of currency or monetary instruments. Section 21 deals with exported mail. Section 23 deals with forfeiture and sections 24-31 focus on the review and appeal of forfeiture of currency and

monetary instruments seized under this Act. Sections 32-35 focus on third party claims to the currency or monetary instruments seized. Sections 36 and 37 deal with disclosure of information.

As originally adopted, Part 3 of the Act enabled FINTRAC to disclose only information relating to money laundering. Bill C-36 amended Part 3 of the Act to require FINTRAC to analyze financial transactions and to disclose certain information to the police when FINTRAC has reasonable grounds to suspect that the information would be relevant to an investigation of a terrorist activity financing offence. In addition, the Act requires FINTRAC to disclose information to CSIS when FINTRAC has reasonable grounds to suspect that the information would be relevant to threats to the security of Canada.

Part 3 of the original Act established FINTRAC, an independent agency that (s.40)

- acts at arm's length from law enforcement agencies and other entities to which it is authorized to disclose information;
- collects, analyses, assesses and discloses information in order to assist in the detection, prevention and deterrence of money laundering and now as a result of the Bill C-36 amendments of the financing of terrorist activities;
- ensures that personal information under its control is protected from unauthorized disclosure;
- operates to enhance public awareness and understanding of matters related to money laundering; and
- ensures compliance with Part 1.

Sections 41-72 deal with the establishment of the Centre; organization and head office; human resources; authority to provide services; disclosure of information; reports and information; disclosure and use of information; compliance measures; contracts and agreements; legal proceedings; audits; and reports.

The sections on disclosure and use of information require FINTRAC, after analyzing and assessing reports and information, to disclose “designated information” to the appropriate police force if it has reasonable grounds to suspect that this information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence (s.55(3)(a)). “Designated information” means particular information relating to a financial transaction or an importation or exportation of currency or monetary instruments such as names, addresses, amounts and account numbers (s.55(7)). FINTRAC shall record its reasons in writing for disclosing information to the police force

under s.55(5.1). FINTRAC also must disclose designated information to CSIS if it has reasonable grounds to suspect that the information would be relevant to threats to the security of Canada (s.55.1). FINTRAC shall record its reasons in writing for disclosing information to CSIS under s.55.1(2).

FINTRAC must also disclose “designated information” to CCRA and to the Department of Citizenship and Immigration if, having met the test for money laundering or terrorist activity financing, it meets a second test relevant to either the CCRA or to Immigration (s.55(3)(b) and (d)).

In addition, the Minister of Finance or FINTRAC may enter into arrangements with a foreign state or an international organization regarding the exchange of information between FINTRAC and other similar institutions or agencies of the state or international organization, and the disclosure of designated information is restricted to purposes relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence (s.56 and s.56.1). In such cases, FINTRAC may disclose “designated information”. The Centre shall record its reasons in writing for disclosing information to foreign states or to an international organization under s.56.1(4).

Section 60 sets out the procedure under which the Attorney General, for the purposes of a money laundering or terrorist financing investigation, may apply for a production order. Section 60.1 provides a separate procedure for CSIS to obtain a production order from a specially designated Federal Court judge in a private hearing for disclosure of information from FINTRAC on the basis that there are reasonable grounds to believe that the information is required to investigate a threat to the security of Canada. Such an application may only be brought after CSIS has obtained the approval of the Solicitor General of Canada to make such an application.

Part 4 of the Act focuses on regulations and Part 5 deals with offences and punishment. Section 80 provides exemptions for a peace officer or a person acting under the direction of a peace officer to commit some of the offences under the act if those offences are committed for the purpose of investigating a money laundering offence or a terrorist activity financing offence.

14. *United Nations Suppression of Terrorism Regulations, SOR/2001-360*

The *United Nations Act*, a Canadian piece of legislation, enables the Canadian government to give effect to decisions of the United Nations Security Council (UNSC) under Chapter VII (Article 41) of the United Nations Charter. The *United Nations Suppression of Terrorism Regulations* aim to suppress the financing in Canada of terrorism and to freeze the assets of listed persons. The regulations were made on October 2, 2001, by the Canadian government, pursuant to s. 2 of

the *United Nations Act*. The regulations implement a key measure in UNSC Resolution 1373, which was unanimously adopted by the UN Security Council on September 28, 2001. The Security Council decided that all member states shall freeze without delay the assets of those who commit or attempt to commit terrorist acts or facilitate the commission of terrorist acts. It also required members to prohibit the provision and collection of funds for terrorist activities.

Section 2 of the regulations establishes a list of persons who there are reasonable grounds to believe have carried out, attempted to carry out or participated in or facilitated the carrying out of a terrorist activity. Section 3 prohibits the provision and collection of funds for the use of a listed person by any person in Canada or any Canadian outside Canada. Section 4 states that no person shall knowingly deal directly or indirectly with any asset owned or controlled by a listed person. Section 6 prohibits the assistance or promotion of any activity prohibited by section 3 or 4. Pursuant to section 7, financial institutions must report on a monthly basis to their regulating body whether they are in possession of any assets that belong to a listed person and they must disclose the number of persons, contracts or accounts involved and the total value of the assets. Section 8 states that any person in Canada or any Canadian outside Canada who has in its possession or control assets they believe are owned or controlled by a listed person must report this information to the RCMP or CSIS.

15. *United Nations Afghanistan Regulations, SOR/99-444*

The United Nations Afghanistan Regulations were enacted by the Canadian government in November 1999 in order to comply with UN Security Council Resolution 1267 of October 15, 1999. In condemning the Taliban for the use of Afghan territory for the sheltering and training of terrorists and providing Al Qaeda a safe haven, Security Council Resolution 1267 called upon states to impose stated measures against the Taliban. The Regulations prohibit, *inter alia*, any person in Canada and any Canadian outside Canada from knowingly becoming involved, either directly or indirectly, in any financial situations or transactions involving the Taliban or Al Qaeda. Also prohibited are the exporting, shipping, selling or supplying of arms and related material to the parts of Taliban-controlled Afghanistan, and the provision of technical assistance related to the military activities of armed personnel under Taliban control. Further, no person in Canada and no Canadian outside of Canada shall knowingly do anything that causes, assists or promotes, or is intended to cause, assist or promote any of the prohibited acts listed the Regulations.

16. *An Act to Amend the Aeronautics Act, S.C. 2001, c. A-2 (Bill C-44)*

This amending Act ensures that an operator of an aircraft departing from Canada or of a Canadian aircraft departing from any place outside Canada may provide to an authority in a foreign state any information that is in its control regarding persons on board or expected to be on board and that is required by the laws of the foreign state (s.4.83)(1)). It also states that no information provided to an authority in a foreign state may be collected from that foreign state by a government institution unless it is collected for the purpose of protecting national security or public safety or for the purpose of defence, and any such information collected by the government institution may be used or disclosed by it only for one or more of those purposes (s.4.83(2)).

17. *Immigration and Refugee Protection Act, S.C. 2001, c. 27*

The Act defines “foreign national” to mean “a person who is not a Canadian citizen or a permanent resident, and includes a stateless person”. “Permanent resident” means “a person who has acquired permanent resident status and has not subsequently lost that status under section 46” (s.2).

Two of the objectives of the Act with respect to immigration are (s.3(1)(h)&(i)):

- to protect the health and safety of Canadians and to maintain the security of Canadian society; and
- to promote international justice and security by fostering respect for human rights and by denying access to Canadian territory to persons who are criminals or security risks.

Two of the objectives of this Act with respect to refugees are:

- to protect the health and safety of Canadians and to maintain the security of Canadian society; and
- to promote international justice and security by denying access to Canadian territory to persons, including refugee claimants, who are security risks or serious criminals.

Sections 34-43 of Division 4 of the Act, entitled “Inadmissibility”, focus on who is deemed to be inadmissible and on what grounds. Grounds of inadmissibility under s.34 include being a danger to the security of Canada, engaging in acts of violence that would or might endanger the lives or safety of persons in Canada or being a member of an organization that there are reasonable grounds to believe engages, has engaged or will engage in espionage, subversion or terrorism.

Sections 34-37 state that a permanent resident or foreign national is inadmissible on security grounds (i.e., espionage, subversion, terrorism), and on the grounds of violating human or international rights, serious criminality or organized criminality.

Sections 44-53 of Division 5 entitled "Loss of Status and Removal" focus on the referral by the Minister of a report on inadmissibility to the Immigration Division and the subsequent admissibility hearing. The Immigration Division can make several decisions at the conclusion of the hearing, including a removal order against a foreign national or a permanent resident if it is deemed that they are inadmissible (s.45(d)).

Sections 54-61 of Division 6 is entitled "Detention and Release". Section 55(1) states that a warrant for the arrest and detention of a foreign national or permanent resident may be issued if there are reasonable grounds to believe that they are inadmissible and a danger to the public or unlikely to appear at a proceeding. Under section 57(1) and (2), within 48 hours after they are taken into detention, the Immigration Division must review the reasons for the continued detention and at least once during the seven days following the initial review and at least once during each 30-day period following each previous review, the Immigration Division must review the reasons for the continued detention.

Section 58(1) provides for the release of a permanent resident or a foreign national unless the Immigration Division is satisfied that they are a danger to the public, or that they are unlikely to appear at the hearing or that the Minister is taking necessary steps to inquire into a reasonable suspicion that they are inadmissible on grounds of security or for violating human or international rights or that detention is necessary to establish the identity of the person. Section 58(2) states that the Immigration Division may order the detention of a permanent resident or a foreign national if it is satisfied that they are the subject of an examination or an admissibility hearing or are subject to a removal order and that they are a danger to the public or are unlikely to appear for a proceeding.

Sections 62-71 of Division 7 deal with rights of appeal. Section 64(1) states that "[n]o appeal may be made to the Immigration Appeal Division by a foreign national or their sponsor or by a permanent resident if the foreign national or permanent resident has been found to be inadmissible on grounds of security, violating human or international rights, serious criminality or organized criminality".

A security certificate is one way to remove a person who poses a security threat and it is only issued for removal purposes when there is information that needs to be protected for security reasons. When a security certificate is issued, all other immigration proceedings are suspended until the court makes a decision on the

reasonableness of the certificate (s.77(2)). Sections 76-87 of Division 9 entitled “Protection of Information” deal with the referral of the certificate by the Minister and the Solicitor General of Canada to the Federal Court-Trial Division for determination. The certificate states that a permanent resident or a foreign national is inadmissible on grounds of security, violating human or international rights, serious criminality or organized criminality. Foreign nationals who are the subject of a security certificate are automatically detained, and permanent residents may be detained on a case-by-case basis if there are reasonable grounds to believe that the permanent resident is a danger to national security or to the safety of any person or is unlikely to appear at a proceeding or for removal (s.82). Section 83 governs the review of the decision for determination.

Section 78 governs the determination and directs the judge to “ensure the confidentiality of the information on which the certificate is based and of any other evidence that may be provided to the judge if, in the opinion of the judge, its disclosure would be injurious to national security or to the safety of any person”. The information is heard *in camera* and may be heard *ex parte* if a request is made by the Minister to do so. Section 78 also provides that any summary of evidence shall not include information that would be injurious to national security or the safety of any person and that the judge may receive any appropriate information even if inadmissible in a court of a law.

Pursuant to section 80, the judge determines whether the certificate is reasonable or not and, if it is deemed to be reasonable, then under section 81 the certificate automatically becomes a removal order. The court’s decision cannot be appealed (s.80(3)).

Part 2 of the Act focuses on “Refugee Protection” and under section 101(1)(f) refugee claimants who are determined to be inadmissible on grounds of security, human rights violations or organized criminality will not be eligible to have their claims heard by the Refugee Protection Division. A decision of ineligibility on any of these grounds terminates the proceedings and nullifies any decision of the Refugee Protection Division respecting the claim. Section 115 sets out the principle of non-refoulement in Division 3, entitled “Pre-Removal Risk Assessment”. This principle prohibits the deportation of a person to a place where his or her life or safety would be threatened. However, pursuant to section 115(2), this principle “does not apply in the case of a person (a) who is inadmissible on grounds of serious criminality and who constitutes, in the opinion of the Minister, a danger to the public in Canada; or (b) who is inadmissible on grounds of security, violating human or international rights or organized criminality if, in the opinion of the Minister, the person should not be allowed to remain in Canada on the basis of the nature and severity of acts committed or of danger to the security of Canada”. The Supreme Court of Canada has determined that in most cases, deportation of a security threat will be an

unjustified violation of s.7 of the Charter if there is a substantial risk that the person will be tortured.¹⁴

The *Immigration and Refugee Protection Regulations* (SOR/2002-227) focus in greater detail on such things as inadmissibility, refugee claimants, pre-removal risk assessment, removals, and detention and release.

According to Fact Sheet #6, “Keeping Canada Safe”, published by Citizenship and Immigration Canada (CIC), background checks are carried out on anyone over the age of 18 who applies for immigration or comes to Canada and claims refugee status, in order to identify criminals and known security threats. The Fact Sheet states that various sources are used for background checks, including intelligence information. According to the same Fact Sheet, “danger opinions” are issued if the Minister of Citizenship and Immigration believes that a person is a danger to the Canadian public or a danger to Canada’s security. They can be issued against Convention refugees facing removal and against a person claiming protection. According to the Fact Sheet, a person’s history is reviewed to determine if they pose a danger to Canada that outweighs the risk of removal to the country from which they fled persecution. A “danger opinion” allows CIC to remove a Convention refugee from Canada and also makes a refugee claimant ineligible for referral to the Refugee Protection Division of the Immigration and Refugee Board.

18. *Canadian Human Rights Act, R.S. 1985 c. H-6*

Bill C-36 amended this Act to clarify that the prohibition against spreading repeated hate messages by telephonic communications includes all telecommunications technologies.

19. *Public Safety Act, S.C. 2004 c. 15*

This law amends certain Acts of Canada, and enacts the *Biological and Toxin Weapons Convention Implementation Act*, in order to enhance public safety.

Part 1 amends the *Aeronautics Act* to enhance the scope and objectives of the existing aviation security regime. The amendments permit the Minister and delegated officers to make emergency directions of no more than 72 hours duration in order to provide an immediate response to situations involving aviation security, and they permit the Minister to delegate to his or her deputy, for the same purpose, the power to make security measures. They clarify and expand the regulation-making power relating to screening. They require air carriers or operators of aviation reservation systems to provide information concerning specified flights or persons. They also require them to provide

¹⁴ *Suresh v. Canada (Minister of Immigration and Citizenship)* [2002] 1 S.C.R. 3.

information for transportation security purposes and national security purposes. They create a new offence concerning passengers who are unruly or who jeopardize the safety or security of an aircraft in flight. They provide a legislative basis for security clearances. They also authorize the making of regulations that require the establishment of security management systems by the Canadian Air Transport Security Authority and by air carriers and operators of aerodromes and other aviation facilities.

Part 2 amends the definitions of “screening” and “screening point” in the *Canadian Air Transport Security Authority Act* to include emergency directions made under the *Aeronautics Act*. It also permits the Authority to enter into agreements with operators of designated aerodromes respecting the sharing of policing costs.

Part 3 amends the *Canadian Environmental Protection Act, 1999* to authorize the Minister to make an interim order under Part 8 of that Act if the appropriate Ministers believe that immediate action is required to deal with a significant danger to the environment or to human life or health.

Part 4 adds a new offence to the *Criminal Code* for communicating information or committing any act that is likely to lead others to falsely believe that terrorist activity is occurring, with the intention of causing persons to fear death, bodily harm, substantial damage to property or serious interference with the lawful use or operation of property.

Part 5 amends the *Department of Citizenship and Immigration Act* to permit the Minister to enter into agreements or arrangements to share information with a province or group of provinces, foreign governments or international organizations.

Part 6 amends the *Department of Health Act* to authorize the Minister to make an interim order if the Minister believes that there is a significant risk to health or safety and immediate action is required to deal with the risk.

Part 7 amends the *Explosives Act* to implement the *Organization of American States Inter-American Convention Against the Illicit Manufacturing of and Trafficking in Firearms, Ammunition, Explosives, and Other Related Materials* as it relates to explosives and ammunition. It prohibits the illicit manufacturing of explosives, and illicit trafficking in explosives. It allows for increased control over the importation, exportation, transportation through Canada, acquisition, possession and sale of explosives and certain components of explosives, and provides increased penalties for certain offences.

Part 8 amends the *Export and Import Permits Act* by providing for control over the export and transfer of technology, as defined, in addition to control over the export of goods as provided for in the *Export and Import Permits Act* at present. It

also authorizes the Minister of Foreign Affairs to address security concerns when considering applications for permits to export or transfer goods or technology.

Part 9 amends the *Food and Drugs Act* to authorize the Minister to make an interim order if the Minister believes that there is a significant risk to health, safety or the environment and immediate action is required to deal with the risk.

Part 10 amends the *Hazardous Products Act* to authorize the Minister to make an interim order if the Minister believes that there is a significant risk to health or safety and immediate action is required to deal with the risk.

Part 11 amends the *Immigration and Refugee Protection Act* to allow for the making of regulations relating to the collection, retention, disposal and disclosure of information for the purposes of that Act. The amendments also allow for the making of regulations providing for the disclosure of information for the purposes of national security, the defence of Canada or the conduct of international affairs. Part 12 amends the *Marine Transportation Security Act* to permit the Minister to enter into agreements respecting security of marine transportation and to make contributions or grants in respect of actions that enhance security on vessels or at marine facilities.

Part 13 amends the *National Defence Act* to allow for the identification and prevention of the harmful unauthorized use of, or interference with, computer systems and networks of the Department of National Defence or the Canadian Forces, and to ensure the protection of those systems and networks. The amendments also clarify the provisions dealing with active service and the definition of "emergency". In cases of aid to the civil power, the amendments allow the Minister to provide direction to the Chief of the Defence Staff on how to respond to provincial requisitions. The amendments provide for a member of the reserve force who is called out on service during an emergency to be reinstated with their former employer at the conclusion of the period of call out. The amendments also establish the Reserve Military Judges Panel, thus making it possible to increase, according to the needs of the military justice system, the number of officers who can be selected to hear military cases.

Part 14 amends the *National Energy Board Act* by extending the powers and duties of the National Energy Board to include matters relating to the security of pipelines and international power lines. It authorizes the Board, with the approval of the Governor in Council, to make regulations respecting the security of pipelines and international power lines. It provides the Board with authority to waive the requirement to publish notice of certain applications in the *Canada Gazette* if there is a critical shortage of electricity. It authorizes the Board to take measures in its proceedings and orders to ensure the confidentiality of information that could pose a risk to security, in particular the security of pipelines and international power lines.

Part 15 amends the *Navigable Waters Protection Act* to authorize the Minister to make an interim order if the Minister believes that there is a significant risk to safety or security and immediate action is required to deal with the risk.

Part 16 amends the *Office of the Superintendent of Financial Institutions Act* by authorizing the Superintendent of Financial Institutions to disclose to the Financial Transactions and Reports Analysis Centre of Canada information related to compliance by financial institutions with Part 1 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.

Part 17 amends the *Personal Information Protection and Electronic Documents Act* to permit the collection and use of personal information for reasons of national security, the defence of Canada or the conduct of international affairs, or when the disclosure of the information is required by law.

Part 18 amends the *Pest Control Products Act* to authorize the Minister to make an interim order if the Minister believes that there is a significant risk to health, safety or the environment and immediate action is required to deal with the risk.

Part 19 amends the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* by extending the types of government databases from which the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) may collect information considered relevant to money laundering or terrorist financing to include national security databases. The amendments also authorize FINTRAC to exchange information related to compliance with Part 1 of that Act with regulators and supervisors of persons and entities subject to that Act, in order to facilitate FINTRAC's compliance responsibilities under that Act.

Part 20 amends the *Quarantine Act* to authorize the Minister to make an interim order if the Minister believes that there is a significant risk to health or safety and immediate action is required to deal with the risk.

Part 21 amends the *Radiation Emitting Devices Act* to authorize the Minister to make an interim order if the Minister believes that there is a significant risk to health or safety and immediate action is required to deal with the risk.

Part 22 amends the *Canada Shipping Act* and the *Canada Shipping Act, 2001* to authorize the appropriate Minister or Ministers to make an interim order if the Minister or Ministers believe that there is a significant risk to safety, security or the environment and immediate action is required to deal with the risk.

Part 23 enacts the *Biological and Toxin Weapons Convention Implementation Act*.

B. International Law

1. United Nations Anti-Terrorism Conventions

Canada has implemented all 12 of the United Nations conventions and protocols commonly described as anti-terrorism instruments, of which 10 are listed in s.83.01. These 12 international instruments are as follows:

- *Convention on Offences and Certain Other Acts Committed on Board Aircraft*, signed at Tokyo on September 14, 1963;
- *Convention for the Suppression of Unlawful Seizure of Aircraft*, signed at The Hague on December 16, 1970;
- *Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation*, signed at Montreal on September 23, 1971;
- *Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents*, adopted by the General Assembly of the United Nations on December 14, 1973;
- *International Convention against the Taking of Hostages*, adopted by the General Assembly of the United Nations on December 17, 1979;
- *Convention on the Physical Protection of Nuclear Material*, done at Vienna and New York on March 3, 1980;
- *Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation*, supplementary to the *Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation*, signed at Montreal on February 24, 1988;
- *Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation*, done at Rome on March 10, 1988;
- *Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf*, done at Rome on March 10, 1988;
- *Convention on the Marking of Plastic Explosives for the Purpose of Detection*, signed at Montreal on March 1, 1991;
- *International Convention for the Suppression of Terrorist Bombings*, adopted by the General Assembly of the United Nations on December 15, 1997;

- *International Convention for the Suppression of the Financing of Terrorism*, adopted by the General Assembly of the United Nations on December 9, 1999.

2. U.N. Security Council Resolution 1373

Shortly after the terrorist attacks of 11 September 2001, the UN Security Council adopted Resolution 1373. The Resolution was adopted under Chapter VII of the UN Charter and thus has binding force on all member states. This Resolution is a wide-ranging anti-terrorism resolution that calls for suppressing the financing of terrorism and international cooperation between states.

Paragraph 1 of the Resolution decides that all States should prevent and suppress the financing of terrorism, as well as criminalize the wilful provision or collection of funds for such acts. The Resolution also decides that all States should freeze the funds, financial assets and economic resources of those who commit or attempt to commit terrorist acts or participate in or facilitate the commission of terrorist acts and of person and entities acting on behalf of terrorists. Paragraph 1 of the Resolution also decides that States should prohibit their nationals or any persons and entities within their territories from making funds, financial assets, economic resources, financial or other related services available to persons who commit or attempt to commit, facilitate or participate in the commission of terrorist acts.

Paragraph 2 of the Resolution decides that all States should refrain from providing any form of support to entities or persons involved in terrorist acts; take the necessary steps to prevent the commission of terrorist acts, including by provision of early warning to other States by exchange of information; deny safe haven to those who finance, plan, support, or commit terrorist acts, or provide safe havens; prevent those who finance, plan, facilitate or commit terrorist acts from using their respective territories for those purposes; and ensure that any person who participates in the financing, planning, preparation or perpetration of terrorist acts or in supporting terrorist acts is brought to justice and ensure that such terrorist acts are established as serious criminal offences in domestic laws and regulations.

Pursuant to Paragraph 2, States should also afford one another the greatest measure of assistance in connection with criminal investigations or criminal proceedings relating to the financing or support of terrorist acts and prevent the movement of terrorists or terrorist groups by effective border controls and controls on issuance of identity papers and travel documents.

Paragraph 3 of the Resolution calls upon all States to:

- “(a) Find ways of intensifying and accelerating the exchange of operational information, especially regarding actions or movements of terrorist persons or networks; forged or falsified travel documents; traffic in arms, explosives or sensitive materials; use of communications technologies by terrorist groups; and the threat posed by the possession of weapons of mass destruction by terrorist groups;
- “(b) Exchange information in accordance with international and domestic law and cooperate on administrative and judicial matters to prevent the commission of terrorist acts;
- “(c) Cooperate, particularly through bilateral and multilateral arrangements and agreements, to prevent and suppress terrorist attacks and take action against perpetrators of such acts;
- “(d) Become parties as soon as possible to the relevant international conventions and protocols relating to terrorism, including the International Convention for the Suppression of the Financing of Terrorism of 9 December 1999;
- “(e) Increase cooperation and fully implement the relevant international conventions and protocols relating to terrorism and Security Council resolutions 1269 (1999) and 1368 (2001);
- “(f) Take appropriate measures in conformity with the relevant provisions of national and international law, including international standards of human rights, before granting refugee status, for the purpose of ensuring that the asylum seeker has not planned, facilitated or participated in the commission of terrorist acts;
- “(g) Ensure, in conformity with international law, that refugee status is not abused by the perpetrators, organizers or facilitators of terrorist acts, and that claims of political motivation are not recognized as grounds for refusing requests for the extradition of alleged terrorists.”

Paragraph 6 establishes a Committee of the Security Council to monitor the implementation of this Resolution and calls upon all States to report back to the new Committee within 90 days of the adoption of the Resolution on the steps they have taken to implement this Resolution.

3. U.N. Security Council Resolution 1269

On October 19, 1999, the Security Council adopted Resolution 1269 condemning all acts of terrorism as criminal and unjustifiable, reaffirming that the suppression of acts of international terrorism is an essential contribution to the maintenance of

international peace and security, and emphasizing the importance of enhanced coordination among States, international and regional organizations.

Paragraph 4 of Resolution 1269 “[c]alls upon States to take, *inter alia*, in the context of such cooperation and coordination, appropriate steps to:

- cooperate with each other, particularly through bilateral and multilateral agreements and arrangements, to prevent and suppress terrorist acts, protect their nationals and other persons against terrorist attacks and bring to justice the perpetrators of such acts;
- prevent and suppress in their territories through all lawful means the preparation and financing of any acts of terrorism;
- deny those who plan, finance, or commit terrorist acts safe haven by ensuring their apprehension and prosecution or extradition;
- take appropriate measures in conformity with the relevant provisions of national and international law, including international standards of human rights, before granting refugee status, for the purpose of ensuring that the asylum-seeker has not participated in terrorist acts;
- exchange information in accordance with international and domestic law, and cooperate on administrative and judicial matters in order to prevent the commission of terrorist acts.”

4. *International Convention for the Suppression of the Financing of Terrorism, Adopted by the General Assembly of the United Nations on December 9, 1999*

The International Convention for the Suppression of the Financing of Terrorism recognizes the need to enhance international cooperation among states in devising and adopting effective measures for the prevention of the financing of terrorism, as well as for its suppression through the prosecution and punishment of its perpetrators. Article 2(1) states that “[a]ny person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out: (a) An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex [U.N. anti-terrorism conventions]; or (b) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation or armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.”

Article 18(3) states that “States Parties shall further cooperate in the prevention of the offences set forth in article 2 by exchanging accurate and verified information in accordance with their domestic law and coordinating administrative and other measures taken, as appropriate, to prevent the commission of offences set forth in article 2, in particular by:

- (a) Establishing and maintaining channels of communication between their competent agencies and services to facilitate the secure and rapid exchange of information concerning all aspects of offences set forth in article 2;
- (b) Cooperating with one another in conducting inquiries, with respect to the offences set forth in article 2, concerning:
 - (i) The identity, whereabouts and activities of persons in respect of whom reasonable suspicion exists that they are involved in such offences;
 - (ii) The movement of funds relating to the commission of such offences.”

Article 18(4) states that “States Parties may exchange information through the International Criminal Police Organization (Interpol).”

5. *Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc. A/810 at 71 (1948)*

The Universal Declaration of Human Rights (UDHR) is a resolution of the General Assembly of the United Nations and not a binding treaty. However, the UDHR is the basis for the fundamental principles of international human rights and it is commonly accepted that some of its provisions were or may have become obligations under customary international law. The fundamental principles of the UDHR are reflected in two legally binding international conventions, the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural rights, the first of which is discussed below.

The following are the relevant articles from the UDHR. Article 2 of the UDHR states that everyone is entitled to all the rights and freedoms set forth, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Article 3 states that everyone has the right to life, liberty and security of the person. Article 5 states that no one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment. Under Article 6, everyone has the right to

recognition everywhere as a person before the law. Article 7 stipulates that all are equal before the law and are entitled without any discrimination to equal protection of the law. Pursuant to Article 8, everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him by the constitution or by law.

Article 9 states that no one shall be subjected to arbitrary arrest, detention or exile. Article 10 stipulates that everyone is entitled in full equality to a fair and public hearing by an independent and impartial tribunal, in the determination of his rights and obligations and of any criminal charges against him. Under Article 12, no one shall be subjected to arbitrary interference with his privacy, family home or correspondence, nor to attacks upon his honour and reputation and everyone has the right to the protection of the law against such interference or attacks. Pursuant to Article 13(2), everyone has the right to leave any country, including his own, and to return to his country.

6. *International Covenant on Civil and Political Rights. Concluded at New York, Dec. 16, 1966. Entered Into Force March 23, 1976. 999 U.N.T.S. 171*

The International Covenant on Civil and Political Rights (ICCPR) is a legally binding international instrument that was created based on the principles enshrined in the Universal Declaration of Human Rights. The ICCPR contains an explicit prohibition of torture in Article 7 which pursuant Article 4(2) is expressly exempt from any possibility of derogation, including in time of “public emergency”. Article 7 of the ICCPR states that “[n]o one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment”. Article 9(1) provides that “[e]veryone has the right to liberty and security of person”. Article 9(1) also provides that “[n]o one shall be subject to arbitrary arrest or detention” or “deprived of his liberty except on such grounds and in accordance with such procedure as are established by law”. Article 9(4) states that “[a]nyone who is deprived of his liberty by arrest or detention shall be entitled to take proceedings before a court, in order that the court may decide without delay on the lawfulness of his detention and order his release if the detention is not lawful”. Pursuant to Article 10, “[a]ll persons deprived of their liberty shall be treated with humanity and with respect for the inherent dignity of the human person”.

Canada, the United States, Jordan and Syria are all parties to the ICCPR. Canada acceded to the treaty on August 19, 1976. The United States ratified it on September 8, 1992, Jordan ratified it on March 23, 1976, and Syria acceded to the ICCPR on March 23, 1976.

Unlike Canada and the United States, Jordan and Syria have not accepted the competence of the United Nations Human Rights Committee under Article 41 of

the ICCPR to consider a state to state complaint. Canada and the United States have accepted the competence of the Human Rights Committee to receive and consider communications under this article of the ICCPR whereby a State Party can claim that another State Party is not fulfilling its obligations under the treaty. In addition, Canada acceded to the First Optional Protocol to the ICCPR on August 19, 1976. Thus, Canada recognizes the competence of the Human Rights Committee to receive and consider communications from individuals subject to Canada's jurisdiction who claim to be victims of a violation by Canada of any of the rights set out in the ICCPR.

7. *Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment. Concluded at New York, Dec. 10, 1984. Entered Into Force June 26, 1987. 1465 U.N.T.S. 85*

Article 1.1 of the Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT) defines torture to mean "any act by which severe pain or suffering, whether physical or mental, is intentionally inflicted on a person for such purposes as obtaining from him or a third person information or a confession, punishing him for an act he or a third person has committed or is suspected of having committed, or intimidating or coercing him or a third person, or for any reason based on discrimination of any kind, when such pain or suffering is inflicted by or at the instigation of or with the consent or acquiescence of a public official or other person acting in an official capacity. It does not include pain or suffering arising only from, inherent in or incidental to lawful sanctions".

Article 2.2 states that "[n]o exceptional circumstances whatsoever, whether a state of war or a threat of war, internal political stability or any other public emergency, may be invoked as a justification of torture".

Article 3.1 states that "[n]o State Party shall expel, return ("refouler") or extradite a person to another State where there are substantial grounds for believing that he would be in danger of being subjected to torture." Article 3.2 states that "[f]or the purpose of determining whether there are such grounds, the competent authorities shall take into account all relevant considerations, including, where applicable, the existence in the State concerned of a consistent pattern of gross, flagrant or mass violations of human rights".

Article 15 states that "[e]ach State Party shall ensure that any statement which is established to have been made as a result of torture shall not be invoked as evidence in any proceedings, except against a person accused of torture as evidence that the statement was made".

Article 16 states that “[e]ach State Party shall undertake to prevent in any territory under its jurisdiction other acts of cruel, inhuman or degrading treatment or punishment which do not amount to torture as defined in article I, when such acts are committed by or at the instigation of or with the consent or acquiescence of a public official or other person acting in an official capacity. In particular, the obligations contained in articles 10, 11, 12 and 13 shall apply with the substitution for references to torture of references to other forms of cruel, inhuman or degrading treatment or punishment”.

Under Article 21, “[a] State Party to this Convention may at any time declare under this article 3 that it recognizes the competence of the Committee to receive and consider communications to the effect that a State Party claims that another State Party is not fulfilling its obligations under this Convention. Such communications may be received and considered according to the procedures laid down in this article only if submitted by a State Party which has made a declaration recognizing in regard to itself the competence of the Committee. No communications shall be dealt with by the Committee under this article if it concerns a State Party which has not made such a declaration”.

Under Article 22, “[a] State Party to this Convention may at any time declare under this article that it recognizes the competence of the Committee to receive and consider communications from or on behalf of individuals subject to its jurisdiction who claim to be victims of a violation by a State Party of the provisions of the Convention. No communication shall be received by the Committee if it concerns a State Party to the Convention which has not made such a declaration”.

Canada signed CAT on August 23, 1985 and ratified the treaty on June 24, 1987. Canada did not make any reservations to CAT. On November 13, 1989 Canada recognized the competence of the Committee Against Torture under Articles 21 and 22. It declared “that it recognizes the competence of the Committee Against Torture, pursuant to Article 21 of the said Convention to receive and consider communications to the effect that a state party is not fulfilling its obligations under this Convention”. Canada also declared “that it recognizes the competence of the Committee Against Torture, pursuant to Article 22 of the said Convention, to receive and consider communications from or on behalf of individuals subject to its jurisdiction who claim to be victims of a violation by a State Party of the provisions of the Convention”.

Jordan is also a State Party to CAT and its date of accession was November 13, 1991. Jordan did not make any reservations. Jordan has not submitted any declarations.

The United States signed CAT April 18, 1988 and ratified it on October 21, 1994 with numerous reservations and understandings. The US only recognizes the Committee’s competence under Article 21 and declared “pursuant to Article 21,

paragraph 1, of the Convention, that it recognizes the competence of the Committee against Torture to receive and consider communications to the effect that a State Party claims that another State Party is not fulfilling its obligations under the Convention. It is the understanding of the United States that, pursuant to the above-mentioned article, such communications shall be accepted and processed only if they come from a State Party which has made a similar declaration.

Syria acceded to CAT on August 19, 2004. Syria declared that it does not recognize the competence of the Committee Against Torture provided for in Article 20 with respect to the confidential inquiry procedure.

8. *American Declaration of the Rights and Duties of Man. Adopted at Bogota by the Ninth International Conference of American States, Mar. 30-May 2, 1948. O.A.S. Res. XXX. O.A.S. Off. Rec. OEA/Ser. L/V/I.4 Rev. (1965)*

Article I states that “[e]very human being has the right to life, liberty and the security of his person”. Article XXV provides that “[n]o person may be deprived of his liberty except in the cases and according to the procedures established by pre-existing law” and that every person has the right to have the legality of his detention ascertained without delay by a court. Every individual also has “the right to humane treatment during the time he is in custody”. Article XXVI provides that “[e]very person accused of an offence has the right . . . not to receive cruel, infamous or unusual punishment”.

Canada, being a member of the Organization of American States (OAS) since January 8, 1990, is subject to the human rights standards set out in the Declaration. Canada has not acceded to the American Convention on Human Rights.

The United States has been a member state of the OAS since 1948 and is also subject to the human rights standards set out in the Declaration. The United States has signed the American Convention on Human Rights but has not ratified it.

9. *Vienna Convention on Consular Relations and Optional Protocols, 596 U.N.T.S. 261, Entered Into Force March 19, 1967*

Pursuant to Article 36 of the Vienna Convention on Consular Relations, law enforcement agencies must notify foreign nationals, without delay, of their right to seek consular assistance and, upon the detainee’s request, must also notify the consulate and allow consular officers access to the detainee and the ability to arrange for legal representation.

II. THE ORGANIZATIONAL FRAMEWORK FOR THE NATIONAL SECURITY ENVIRONMENT APPLICABLE IN CANADA PRIOR TO DECEMBER 2003

Prior to December 2003, and when the Solicitor General of Canada released his performance report for the Department of the Solicitor General for the period ending March 31, 2003, the portfolio of the Solicitor General was comprised of the Department of the Solicitor General and five agencies: RCMP, CSIS, Correctional Service of Canada, National Parole Board, and Canada Firearms Centre. There were also three review bodies: the RCMP External Review Committee, the Commission for Public Complaints against the RCMP and the Office of the Correctional Investigator. The Inspector General of CSIS carried out internal, independent reviews of CSIS for the Solicitor General and reported directly to the Solicitor General. SIRC, an independent review body of CSIS, publishes its findings in an annual report to Parliament that was tabled by the Solicitor General.

Prior to December 2003, the Office of Critical Infrastructure Protection and Emergency Preparedness fell under the jurisdiction of the Department of National Defence. Before December 2003 the Canada Customs and Revenue Agency (CCRA) was responsible for both customs and tax issues. On December 12, 2003, CCRA became the Canada Revenue Agency (CRA) and the customs program became part of the new Canada Border Services Agency (CBSA). The CBSA includes the domestic enforcement units of the old Department of Citizenship and Immigration.

III. THE ORGANIZATIONAL FRAMEWORK FOR THE NATIONAL SECURITY ENVIRONMENT APPLICABLE IN CANADA IN JUNE 2004

A. Public Safety and Emergency Preparedness Portfolio

On December 12, 2003, Prime Minister Paul Martin announced restructuring changes to the government on "Securing Canada's Public Health and Safety". As part of this restructuring a new portfolio was created. The new Public Safety and Emergency Preparedness Portfolio headed by the new Minister of Public Safety and Emergency Preparedness integrates into a single portfolio the activities of the previous Department of the Solicitor General, the Office of Critical Infrastructure Protection and Emergency Preparedness, previously in the department of National Defence, the National Crime Prevention Centre, previously in the Department of Justice and the new Canadian Border Service Agency.

This new portfolio includes emergency preparedness, crisis management, national security, corrections, policing, oversight, crime prevention and border

functions. It consists of the Department of Public Safety and Emergency Preparedness and six agencies. The agencies are:

- RCMP;
- CSIS;
- Correctional Service of Canada (CSC);
- National Parole Board (NPB);
- Canada Firearms Centre; and
- Canada Border Services Agency (CBSA).

The portfolio also includes three independent review bodies and two statutory reviews of CSIS. The three independent review bodies are:

- the Commission for Public Complaints against the RCMP (CPC-RCMP);
- the Office of the Correctional Investigator (OCI); and
- the RCMP External Review Committee (ERC).

The two statutory review bodies of CSIS are SIRC and the Office of the Inspector-General of CSIS.

The newly created Canada Border Services Agency (CBSA) builds on the Smart Border Initiative and manages Canada's borders by administering domestic laws with reference to international agreements and conventions governing trade and travel. The CBSA brings together the major players involved in managing the movement of people and goods across Canadian borders. It integrates customs functions (from the former Canada Customs and Revenue Agency), intelligence, enforcement functions and overseas interdiction (from Citizenship and Immigration Canada), and passenger and initial import inspection services at ports of entry (formerly with the Canadian Food Inspection Agency).

The work of the CBSA includes conducting border security activities, such as screening visitors and immigrants and working with law enforcement agencies to maintain border integrity and ensure national security; and engaging in enforcement activities, including investigations, detentions, hearings, and removals. The CBSA collaborates with several partners, including Citizenship and Immigration, RCMP, CSIS, national, provincial and municipal police, and international police, intelligence and law enforcement agencies.

B. The Canada-US Smart Border Agreement

In December 2001, the Government of Canada and the Government of the US signed the Smart Border Declaration and its companion 30-point Action Plan to enhance the security of the shared border while facilitating the flow of people and goods. The Action Plan has four pillars: the secure flow of people, the secure

flow of goods, secure infrastructure, and information sharing and coordination in the enforcement of these objectives. Under the pillar “the secure flow of people”, two of the thirteen actions points are #8 Advance Passenger Information/Passenger Name Record and #9 Joint Passenger Analysis Units. Under #8, the two governments are to share Advance Passenger Information and agreed-to Passenger Name Records on flights between Canada and the US, including in-transit flights, and explore means to identify risks posed by passengers on international flights arriving in each other’s territory.¹⁵ Under #9, the two governments are to establish joint passenger analysis units at key international airports in Canada and the US.

Under the pillar “coordination and information sharing in the enforcement of these objectives”, four of the eight actions points are: #24 Joint Enforcement Coordination; #25 Integrated Intelligence; #27 Removal of Deportees; and, #29 Freezing of Terrorist Assets. Under #24, the two governments are to work towards ensuring comprehensive and permanent coordination of law enforcement, anti-terrorism efforts and information sharing, such as by strengthening the Cross-Border Crime Forum and reinvigorating Project Northstar. Under #25, the governments are to establish joint teams to analyze and disseminate information and intelligence, and to produce threat and intelligence assessments. Discussions were also to be initiated regarding a Canadian presence on the US Foreign Terrorist Tracking Task Force. Under #27, the governments are to address legal and operational challenges to joint removals, and are to coordinate initiatives to encourage uncooperative countries to accept their nationals. Under #29, the governments are to exchange advance information on designated individuals and organizations in a timely manner with respect to the freezing of terrorist assets.

C. Canada/US Integrated Border Enforcement Teams (IBETs)

Originally developed in 1996 to address cross-border crimes along international land and marine borders between British Columbia and Washington State, IBETs have evolved over time. The Integrated Border Enforcement Team is a multi-agency law enforcement team that targets cross-border criminal activity. The original six core partner agencies from Canada and the US which were involved in IBETs were: RCMP, Canada Customs and Revenue Agency, US Customs and Border Patrol, Citizenship and Immigration Canada, US Immigration and Customs Enforcement, and the US Coast Guard. IBETs enable US and Canadian national police services and law enforcement communities to work together daily with local, state and provincial enforcement agencies. IBETs have been established in ten Canadian locations.

¹⁵ As examined below, the *Aeronautics Act* was amended in 2001 providing for the exchange of passenger information to a foreign state that is required by the laws of a foreign state.

D. Integrated National Security Enforcement Teams (INSET)

The RCMP has refocused some of its National Security Intelligence Sections (NSIS) to become Integrated National Security Enforcement Teams (INSETs). The purpose for this is to: increase the capacity for the collection, sharing and analysis of intelligence among partners with respect to targets that are a threat to national security; create an enhanced enforcement capacity to bring such targets to justice; and, enhance partner agencies collective ability to combat national security threats. INSETs are made up of representatives of the RCMP, federal partners and agencies such as Canada Border Services Agency, Citizenship and Immigration Canada and CSIS, and provincial and municipal police services. INSETs were originally formed in Vancouver, Toronto, Ottawa and Montreal. The Canadian government began investing funds towards the creation of INSETs in April 2002.

E. Integrated National Security Assessment Centre (INSAC) and Integrated Threat Assessment Centre (ITAC)

On October 16, 2003, the Canadian government announced the establishment of a new terrorism assessment centre to enhance the capability of CSIS to inform the Government of Canada regarding threats to national security and public safety. The Centre is based at CSIS headquarters in Ottawa. INSAC brings an integrated approach to intelligence analysis and dissemination. It draws personnel from the broader Canadian intelligence community, including those involved with defence, immigration, transport, communications, customs, critical infrastructure, foreign affairs, and law enforcement, to prepare intelligence assessments. The primary objective of INSAC is to assist in the prevention and disruption of national security threats at the earliest possible stage, thereby weakening threats to infrastructures and pre-empting future threat-related activities. This is to be accomplished through the production of assessments which combine strategic and operational intelligence. The assessments produced by the Centre are then distributed to the Government of Canada and recipient departments which forward them, as appropriate, to their partners to improve warning, response and incident mitigation capabilities.

INSAC has been replaced by the Integrated Threat Assessment Centre (ITAC). It will be staffed and supported by departments and agencies including Public Safety and Emergency Preparedness, CSIS, the RCMP, CSE, the Department of National Defence, the Department of Foreign Affairs, the Privy Council Office, Transport Canada and the Canada Border Services Agency. Like INSAC, ITAC will be housed in CSIS but will work in conjunction with the National Security Advisor to the Prime Minister.¹⁶

¹⁶ See p. 18 of http://www.pco-bcp.gc.ca/docs/Publications/NatSecurnat/natsecurnat_e.pdf

F. Canadian Air Transport Security Authority (CATSA)

The Canadian Air Transport Security Authority (CATSA) was established on April 1, 2002 as part of a package of aviation security initiatives. CATSA is responsible for several key aviation security services. CATSA reports to Parliament through the Minister of Transport. CATSA's responsibilities fall into six major areas: (1) pre-board screening of passengers and their belongings; (2) acquisition, deployment, operation and maintenance of explosives detection systems at airports; (3) contracting for RCMP policing services on selected flights and all flights to Reagan National Airport; (4) implementation of a restricted area identification card; (5) the screening of non-passengers entering airport restricted areas; and (6) contributions for supplemental airport policing services.

G. National Security Advisor to the Prime Minister

When Prime Minister Paul Martin announced restructuring changes to the government on "Securing Canada's Public Health and Safety" on December 12, 2003, he created a new position in the Privy Council Office of National Security Advisor to the Prime Minister. The person appointed to this new position is responsible for intelligence and threat assessment, integration and interagency cooperation, and in assisting the Minister of Public Safety and Emergency Preparedness in the development and overall implementation of an integrated policy for national security and emergencies, to be referred to the appropriate House Standing Committee.

H. Cabinet Committee on Security, Public Health and Emergencies

On December 12, 2003, the Prime Minister also established a new Cabinet Committee on Security, Public Health and Emergencies, chaired by the Minister of Public Safety and Emergency Preparedness, to manage national security and intelligence issues and activities, and to coordinate government-wide responses to all emergencies, including public health, natural disasters and security.

I. National Security Standing Committee

On December 12, 2003, the Prime Minister also proposed a National Security Standing Committee in the House of Commons whose members would be sworn-in as Privy Councillors so that they could be briefed on national security issues. On March 31, 2004, the Deputy Prime Minister released a consultation paper that proposes to create a new National Security Committee of Parliamentarians.¹⁷ The proposal provides for a broader role for Parliament in guiding and reviewing Canada's national security activities. It would grant the

¹⁷ The consultation paper that was tabled on March 31, 2004 has been published on PSEPC's website at: http://www.psepc-sppcc.gc.ca/publications/national_security/nat_sec_cmte_e.asp

Opposition members of the Committee access to classified materials and Opposition Leaders would also be asked to be sworn in as Privy Councillors so that they could be briefed as needed on national security issues.

J. Privy Council Office (PCO)

The PCO supports the Prime Minister in his responsibility for the security and integrity of Canada and related intelligence matters. The Clerk of the Privy Council chairs a deputy minister-level group, the Interdepartmental Committee on Security and Intelligence (ICSI), which discusses strategic policy and resource issues, considers sensitive national security matters and recommends the annual intelligence priorities for the Meeting of Ministers on Security and Intelligence. Reporting to the Clerk is the Deputy Clerk, Counsel and Security and Intelligence Co-ordinator, who has a mandate from the PM to coordinate the security and intelligence activities of all Canadian government departments and agencies and to promote effective international intelligence relationships. Two PCO secretariats – a policy unit, the Security and Intelligence Secretariat, and an assessment unit, the Intelligence Assessment Secretariat – report to this Deputy Clerk.

The Security and Intelligence Secretariat provides advice to the PM on national security and foreign intelligence matters, including major policy developments, public issues, crises and community priorities. The Assistant Secretary, Security and Intelligence, chairs the interdepartmental Intelligence Policy Group of ADM-level officials. This group is the principal forum for policy and operational coordination within the community. Under a PCO-DFAIT memorandum of understanding, both departments contribute to the staffing and management of the Intelligence Assessment Secretariat (IAS) which produces assessments of conditions and trends in foreign countries including the implications for Canadian policy-makers. The Executive Director of the IAS chairs the Intelligence Assessment Committee (IAC) which brings together representatives of domestic departments and agencies that are involved in gathering or assessing intelligence and are major users of assessed intelligence.

K. Other Parliamentary Committees on National Security

The Standing Senate Committee on National Security and Defence focuses on matters in relation to national defence and security generally.

There are also the following committees:

- House of Commons Subcommittee on National Security of the Standing Committee on Justice and Human Rights;
- Standing Senate Committee on Security and Intelligence.

L. New National Security Policy

On April 28, 2004 the government of Canada released a new national security policy entitled "Security an Open Society: Canada's National Security Policy".¹⁸ It sets for a commitment to establish a National Security Advisory Council made up of security experts external to the government and an advisory Cross-Cultural Roundtable on Security. It re-affirms the government's prior commitment to an arm-length review mechanism for the RCMP's national security activities and for a National Security Committee of Parliamentarians. It focuses on six key security activities: intelligence, emergency planning and management, public health emergencies, transportation security, border security and international security.

¹⁸ It is available at http://www.psepc-pcc.gc.ca/publications/national_security/nat_sec_cmte_e.asp