Air India Flight 182

A Canadian Tragedy

VOLUME FIVE

Terrorist Financing

Cat. No: CP32-89/2-2010E
ISBN: 978-0-660-19926-9

Available through your local bookseller or through
Publishing and Depository Services
Public Works and Government Services Canada
Ottawa, Ontario
K1A 0S5

Telephone: (613) 941-5995 or 1 800 635-7943
Fax: (613) 954-5779 or 1 800 565-7757
Publications@pwgsc.gc.ca
Internet: www.publications.gc.ca

VOLUME FIVE
TERRORIST FINANCING

TABLE OF CONTENTS

CHAPTER I: TERRORIST FINANCING – AN OVERVIEW

CHAPTER II: CANADIAN LEGISLATION GOVERNING TERRORIST FINANCING

CHAPTER III: THE ROLES OF FEDERAL DEPARTMENTS ANDAGENCIES IN EFFORTS TO SUPPRESS TERRORIST FINANCING

CHAPTER IV: EXTERNAL REVIEWS OF CANADA'S ANTI-TF PROGRAM

CHAPTER V: CANADA'S RESPONSE TO REVIEWS OF ITS ANTI-TF PROGRAM

CHAPTER VI: THE LINKS BETWEEN THE CHARITABLE SECTOR AND TERRORIST FINANCING

CHAPTER VII: RESOLVING THE CHALLENGES OF TERRORIST FINANCING

VOLUME FIVE
TERRORIST FINANCING

CHAPTER I: TERRORIST FINANCING – AN OVERVIEW

1.1 Introduction

The terms of reference for the *Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182* require the Commissioner to make findings and recommendations with respect to "…whether Canada's existing legal framework provides adequate constraints on terrorist financing in, from or through Canada, including constraints on the use or misuse of funds from charitable organizations."[1]

Addressing terrorist financing (TF) involves responding to two broad questions:

1. How do terrorists obtain the resources they need to carry out terrorist acts or support terrorist networks?
2. How can governments use this knowledge to defeat terrorists?[2]

1.1.1 Defining Terrorist Financing

The *United Nations International Convention for the Suppression of the Financing of Terrorism*[3] refers to TF in the following terms:

> Article 2.1. Any 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;[4] or

---

1 Terms of Reference, P.C. 2006-293, para. b(iv).

2 These two questions guided the terrorist financing-resourcing model and study prepared by John Schmidt of the Integrated Threat Assessment Centre (ITAC): see Testimony of John Schmidt, vol. 53, September 27, 2007, p. 6651.

3 Online: United Nations Treaty Collection <http://untreaty.un.org/English/Terrorism/Conv12.pdf> (accessed February 20, 2009).

4 The same treaties are referred to in the Canadian definition of "terrorist activity" and in the FATF definition of "terrorist act."

> (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 of 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 organisation to do or to abstain from doing any act.[5]

UN Security Council Resolution 1373 (2001)[6] defines TF as follows:

> ...[the] wilful provision or collection, by any means, directly or indirectly, of funds by their nationals or in their territories with the intention that the funds should be used, or in the knowledge that they are to be used, in order to carry out terrorist acts.[7]

The Financial Action Task Force (FATF), considered to be the main international body determining policy on TF and money laundering, describes TF as follows:

> The term terrorist financing includes the financing of terrorist acts, and of terrorists and terrorist organisations…. Terrorist financing offences should extend to any person who wilfully provides or collects funds by any means, directly or indirectly, with the unlawful intention that they should be used or in the knowledge that they are to be used, in full or in part: (a) to carry out a terrorist act(s); (b) by a terrorist organisation; or (c) by an individual terrorist.[8]

These descriptions all support the notion that TF is essentially the collection and/or use of funds to accomplish or support terrorist acts or to support terrorist organizations.

---

5 The World Bank states that the definition in the United Nations International Convention for the Suppression of the Financing of Terrorism is the one most countries have adopted for purposes of defining terrorist financing: Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism: A Manual for Countries to Establish and Improve Their Institutional Framework, 2nd. ed. and Supp. on Special Recommendation IX (Washington D.C.: The International Bank for Reconstruction and Development/The World Bank/The International Monetary Fund, 2006), p. I-5 [The World Bank Guide to Anti-Money Laundering and Combating Terrorism Financing].

6 Online: United Nations <http://daccessdds.un.org/doc/UNDOC/GEN/N01/557/43/PDF/N0155743.pdf?OpenElement> (accessed February 13, 2009).

7 S. 1(b).

8 The Interpretative Notes to the Special Recommendations (SR) on Terrorist Financing (TF), Interpretative Note to Special Recommendation II: Criminalising the financing of terrorism and associated money laundering, paras. 2, 3, online: Financial Action Task Force <http://www.fatf-gafi.org/document/53/0,3343,en_32250379_32236947_34261877_1 1 1 1,00.html> (accessed February 11, 2009).

The *Criminal Code*[9] does not provide a definition of terrorist financing, but instead lists several offences in sections 83.02 to 83.04 under the heading "Terrorist Financing." For example, section 83.03 makes it an offence to collect property or make available property or financial or other related services intending that they be used for the purpose of facilitating or carrying out any terrorist activity.

1.1.2 Origins of Canada's Response to Terrorist Financing

Before 2001, no specific TF offences existed in Canadian law. Despite the enormity of the Air India tragedy in 1985, there was not much focus on TF in Canada at the turn of the millennium.[10] Terrorism-related incidents that occurred before 2001 were dealt with under existing criminal law.[11] Discussions and groundwork leading to Canadian TF legislation were under way before the terrorist attacks of September 11, 2001 ("9/11"), but began in earnest only many years after the 1985 Air India tragedy. The current provisions concerning TF, now contained in the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*[12] (*PCMLTFA*) and the *Criminal Code*, were a product of the terrorist attacks of 9/11.[13]

Blake Bromley, a Canadian lawyer practising exclusively on charities issues, wrote in a submission to the Commission that "…[i]t is noteworthy and troubling that our anti-terrorism legislation was enacted in response to the American tragedy of 2001, rather than the Canadian tragedy of 1985."[14]

Canadian law enforcement authorities did not focus on TF before 2001 simply because there was no TF legislation.[15] Canada's approach to TF was not unique. Even foreign law enforcement agencies and other bodies involved in counterterrorism efforts before 2001 apparently did not focus heavily on TF activities.[16] Keith Morrill, Director of the Criminal, Security and Treaty Law Division of the Department of Foreign Affairs and International Trade's Legal Affairs Bureau, testified that TF issues had come late in the day to the international scene.[17]

The RCMP created a task force on terrorist-related financial matters shortly after 9/11, but even that initiative sought primarily to prevent terrorist attacks[18] – an approach sometimes described as "chasing the bomber."

---

9 R.S.C. 1985, c. C-46.
10 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6818.
11 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6830.
12 S.C. 2000, c. 17.
13 See, for example, Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6939.
14 Blake Bromley, "Funding Terrorism and Charities," October 26, 2007, online: Benefic Group <http://www.beneficgroup.com/files/getPDF.php?id=120> (accessed May 12, 2009).
15 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6818. But law enforcement authorities were aware that a crime might still have been committed if the behaviour could be attached to an existing criminal offence before 2001: Testimony of Rick Reynolds, vol. 55, October 1, 2007, pp. 6818, 6830.
16 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6818.
17 Testimony of Keith Morrill, vol. 54, September 28, 2007, pp. 6680, 6705.
18 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6819.

1.1.3 Objectives of Canada's Anti-Terrorist Financing Efforts

A fundamental goal of Canada's anti-TF program is to protect Canadians and the integrity of Canada's financial system and to ensure that gaps and vulnerabilities in the financial system are being addressed.[19] The Government of Canada's stated objectives are to create a "hostile environment" towards TF, to respect international obligations and to be vigilant in dealing with TF.[20]

1.2 The International System to Combat Terrorist Financing

International efforts to combat TF flowed from the intersection of existing money laundering initiatives and the need to respond to the events of 9/11. The initiative to combat money laundering itself arose because criminal activities were generating enormous amounts of cash that had to be "laundered" to avoid detection of the money's links to crime.[21]

Professor Nikos Passas of Northeastern University's College of Criminal Justice explained that the money laundering model was adapted internationally to deal with TF:

> What characterized our [US] response, especially after the attacks of September 11th in the United States, was similarly an adoption of the methods that were in place against money laundering for the purpose of countering the financing of terrorism…. This was the approach adopted right after 9/11, not only in the United States, but internationally.[22]

Passas testified that the money laundering model was chosen because it was familiar. As well, governments were going to apply whatever tools they had available and governments had to convey to the public the impression that they were "doing something" about terrorism.[23] He also suggested that TF measures may have been created too hastily, although they "…were not resisted particularly by those to whom they applied. The private sector or politicians didn't have any problem with that, or the general public. Everybody wanted to see something done against terrorism so whatever helps we're going to go along with."[24]

---

19 Testimony of Diane Lafleur, vol. 54, September 28, 2007, pp. 6778-6779, 6753.
20 Testimony of Diane Lafleur, vol. 54, September 28, 2007, pp. 6773-6774.
21 National Commission on Terrorist Attacks Upon the United States, *Monograph on Terrorist Financing*, p. 54, online: National Commission on Terrorist Attacks Upon the United States <http://govinfo.library.unt.edu/911/staff_statements> (accessed February 20, 2009) [National Commission Monograph on Terrorist Financing]. In many countries, provisions to counter money laundering were necessary in large part to combat the drug trade: Testimony of Keith Morrill, vol. 54, September 28, 2007, p. 6688.
22 Testimony of Nikos Passas, vol. 53, September 27, 2007, pp. 6568-6569.
23 Testimony of Nikos Passas, vol. 53, September 27, 2007, p. 6569.
24 Testimony of Nikos Passas, vol. 53, September 27, 2007, p. 6570.

In general, money laundering laws focus on the large amounts of money that are proceeds of crime – "dirty money." In contrast, TF may involve smaller sums that are not necessarily proceeds of crime. The question remains: Did adding TF provisions to existing money laundering provisions lead to the most appropriate TF measures?

1.2.1 International Instruments and Organizations to Combat Terrorist Financing

1.2.1.1 The United Nations (UN)

Three UN instruments are important in TF matters: the *International Convention for the Suppression of the Financing of Terrorism, UN Security Council Resolution 1373* and *UN Security Council Resolution 1267*.

1.2.1.1.1 The International Convention for the Suppression of the Financing of Terrorism

Ratified by Canada in 2001,[25] the *International Convention for the Suppression of the Financing of Terrorism (Financing of Terrorism Convention)* states in its preamble that the parties to the Convention are "…deeply concerned about the worldwide escalation of acts of terrorism in all its forms and manifestations." The Convention requires parties to criminalize TF and to provide for the freezing, seizure and forfeiture of funds used for TF.

1.2.1.1.2 UN Security Council Resolution 1373 (2001)

The UN Security Council adopted Resolution 1373 on September 28, 2001. Security Council resolutions passed under Chapter VII of the UN Charter in response to a threat to international peace and security are binding on all UN members.[26] Each member must then implement the resolutions in its domestic law.

Resolution 1373 imposes several obligations on member states, including the following:

> 1(a) Prevent and suppress the financing of terrorist acts;
>
> (b) Criminalize the wilful provision or collection, by any means, directly or indirectly, of funds by their nationals or in their

---

25 The treaty was signed by Canada on February 10, 2000: see "Canada Signs International Convention for the Suppression of the Financing of Terrorism," online: Foreign Affairs and International Trade Canada <http://w01.international.gc.ca/minpub/PublicationContentOnly.asp?publication_id=377482&Language=E&MODE=CONTENTONLY&Local=False> (accessed February 11, 2009).

26 Exhibit P-227, Tab 3: Department of Finance Memorandum of Evidence on Terrorist Financing, February 28, 2007, paras. 3.8-3.9 [Department of Finance Memorandum of Evidence on Terrorist Financing].

> territories with the intention that the funds should be used, or in the knowledge that they are to be used, in order to carry out terrorist acts;
>
> (c) Freeze without delay funds and other financial assets or economic resources of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds derived or generated from property owned or controlled directly or indirectly by such persons and associated persons and entities;
>
> (d) Prohibit their nationals or any persons and entities within their territories from making any funds, financial assets or economic resources or financial or other related services available, directly or indirectly, for the benefit of persons who commit or attempt to commit or facilitate or participate in the commission of terrorist acts, of entities owned or controlled, directly or indirectly, by such persons and of persons and entities acting on behalf of or at the direction of such persons;
>
> 2(a) Refrain from providing any form of support, active or passive, to entities or persons involved in terrorist acts, including by suppressing recruitment of members of terrorist groups and eliminating the supply of weapons to terrorists.

The UN Office on Drugs and Crime (UNODC) developed model TF legislation which countries can adopt to comply with the provisions of Resolution 1373 and the *Financing of Terrorism Convention*.[27]

Resolution 1373 also established the UN Security Council Counter-Terrorism Committee (CTC). The CTC is composed of the 15 Security Council members. It monitors the implementation of the Resolution by member states and facilitates providing technical assistance to those states.[28] The Resolution calls on all states to report regularly on their progress in implementing the Resolution. Countries must perform a self-assessment of their legislation and mechanisms to combat terrorism and TF in light of the requirements of Resolution 1373. The CTC maintains a website with a directory of international best practices to help countries improve their counterterrorism infrastructures. The website also contains model legislation and related information.[29]

---

27 Online: International Money Laundering Information Network <http://www.imolin.org/imolin/tfbill03.html> (accessed February 11, 2009).

28 Online: United Nations <http://www.un.org/sc/ctc/aboutus.html> (accessed February 11, 2009).

29 The World Bank Guide to Anti-Money Laundering and Combating Terrorism Financing, p. III-7. The CTC website containing the extensive directory of best practices can be found online: <http://www.un.org/sc/ctc/practices.html> (accessed January 23, 2009).

1.2.1.1.3 UN Security Council Resolution 1267 (1999) and Subsequent Resolutions

Resolution 1373 was drafted following several Security Council resolutions requiring member states to freeze the assets of entities or individuals with links to Al-Qaida[30] and the Taliban, including entities listed by Security Council Resolution 1267 and other resolutions.[31] A 2002 World Bank report summarized the range and scope of these resolutions:

> The initial Resolution 1267 of October 15, 1999, dealt with the Taliban and was followed by 1333 of December 19, 2000, on Osama Bin Laden and Al-Qaeda. Later Resolutions established monitoring arrangements (1363 of July 30, 2001), merged the earlier lists (1390 of January 16, 2002), provided some exclusions (1452 of December 20, 2002), and measures to improve implementation (1455 of January 17, 2003).
>
> The 1267 Committee issues the list of individuals and entities whose assets are to be frozen and has procedures in place to make additions or deletions to the list on the basis of representations by member States.[32] [references to footnotes omitted.]

Collectively, these resolutions require all states to take the following measures "…in connection with any individual or entity associated with Al-Qaida, Usama bin Laden and/or the Taliban as designated by the Committee":

- freeze without delay the funds and other financial assets or economic resources of designated individuals and entities [**assets freeze**];
- prevent the entry into or transit through their territories by designated individuals [**travel ban**]; and
- prevent the direct or indirect supply, sale and transfer from their territories or by their nationals outside their territories, or using their flag vessels or aircraft, of arms and related materiel of all types, spare parts, and technical advice, assistance, or training

---

30 Also referred to as "Al-Qaeda" or "al-Qaeda." For consistency in this volume, the names "Usama bin Laden" and "Al-Qaida" are spelled according to the Canadian spelling in the *United Nations Al-Qaida and Taliban Regulations*, S.O.R./99-444 and on the website for the United Nations Security Council Committee established pursuant to Resolution 1267, online: United Nations <http://www.un.org/sc/committees/1267/index.shtml> (accessed February 20, 2009).

31 Kevin E. Davis, "The financial war on terrorism," in Victor V. Ramraj, Michael Hor and Kent Roach, eds., *Global Anti-Terrorism Law and Policy* (Cambridge: Cambridge University Press, 2005), p. 180.

32 The World Bank Guide to Anti-Money Laundering and Combating Terrorism Financing, pp. III-5-6. The most recent list of the 1267 Committee is available online: United Nations <http://www.un.org/sc/committees/1267/consolist.shtml> (accessed February 20, 2009). The list issued by the 1267 Committee should not be confused with Canada's own list, discussed below.

related to military activities, to designated individuals and entities [**arms embargo**].[33]

1.2.1.2 The Financial Action Task Force on Money Laundering (FATF)

The G-7 countries established the Financial Action Task Force on Money Laundering (FATF) as an intergovernmental body in 1989. It was created informally, not by treaty.[34] Its current goals are to develop and promote national and international policies to combat money laundering and TF. Among other activities, the FATF works to generate the necessary political will to bring about legislative and regulatory reforms in these areas.[35] It is the principal group at the international level setting standards on money laundering and TF issues.

The original mandate of the FATF was to provide guidance and a practical international framework to combat money laundering. In 1990, the FATF published its first version of "The Forty Recommendations" on money laundering.[36] The FATF met in October 2001 to evaluate the need to take action against TF activities. The FATF's mandate was then expanded to include TF.[37] Also in October 2001, the FATF published its "Eight Special Recommendations on Terrorist Financing." A ninth was added in October 2004.[38] The "Nine Special Recommendations" provide guidance about combatting TF.

The FATF has described one of its fundamental goals as the "[f]ull and effective roll-out" of the "40+9" Recommendations.[39] However, the FATF's responsibilities go far beyond the Recommendations. They include examining money laundering and TF techniques and trends, reviewing actions taken at the national or international levels, and recommending measures to combat money laundering and TF.[40] When its mandate was reviewed in 2008, the FATF stated that it would make efforts to respond to emerging threats created by globalization, such as "…proliferation financing and vulnerabilities in new technologies which could destabilise the international financial system."[41] As well, the FATF described the identification of, and appropriate response to, countries with severe deficiencies

---

33 Online: United Nations <http://www.un.org/sc/committees/1267/index.shtml> (accessed February 11, 2009).

34 Testimony of Keith Morrill, vol. 54, September 28, 2007, p. 6688.

35 Online: Financial Action Task Force <http://www.fatf-gafi.org/pages/0,2987,en_32250379_32235720_1_1_1_1_1,00.html> (accessed February 20, 2009).

36 A revision occurred in 1996, followed by a thorough review and update in 2003. The current version is available online: Financial Action Task Force <http://www.fatf-gafi.org/document/28/0,3343,en_32250379_32236930_33658140_1_1_1_1,00.html> (accessed February 11, 2009).

37 Financial Action Task Force on Money Laundering, *Annual Report 2001-2002*, June 21, 2002, paras. 16-17, online: Financial Action Task Force <http://www.fatf-gafi.org/dataoecd/13/1/34328160.pdf> (accessed February 20, 2009).

38 The current version, titled "9 Special Recommendations (SR) on Terrorist Financing (TF)" is available online: Financial Action Task Force <http://www.fatf-gafi.org/document/9/0,3343,en_32250379_32236920_34032073_1_1_1_1,00.html> (accessed February 11, 2009).

39 Financial Action Task Force, *FATF Revised Mandate 2008-2012*, April 12, 2008, para. 5, online: Financial Action Task Force <http://www.fatf-gafi.org/dataoecd/3/32/40433653.pdf> (accessed February 11, 2009) [FATF Revised Mandate 2008-2012].

40 "About the FATF."

41 FATF Revised Mandate 2008-2012, para. 2.

in their money laundering and TF programs ("weak links") as a key element of its ongoing work.[42]

The FATF Recommendations have been endorsed by more than 170 jurisdictions around the world, as well as by the boards of the International Monetary Fund (IMF) and the World Bank.[43] In July 2005, the United Nations Security Council, in Resolution 1617, stated that it "…strongly urges all Member States to implement the comprehensive, international standards embodied in the Financial Action Task Force's (FATF) Forty Recommendations on Money Laundering and the FATF Nine Special Recommendations on Terrorist Financing."[44]

The "40+9" Recommendations are not legally binding.[45] To fulfill its mandate, the FATF has established partnerships with many regional bodies and international organizations involved in combatting money laundering and TF.

In addition, the FATF has established a mutual evaluation program where experts on money laundering and TF matters examine a member state's activities against money laundering and TF. The FATF's 2007-08 annual report stated that, at that point, 75 countries had been evaluated.[46] Canada was evaluated in 2007-08 (the 2008 FATF Mutual Evaluation of Canada).[47] To facilitate its work, the FATF supports "FATF-style regional bodies" to raise awareness in their geographic locations and conduct mutual evaluations in partnership with the FATF or independently.[48]

---

42 FATF Revised Mandate 2008-2012, para. 7. For instance, the FATF has recently identified Uzbekistan, Iran, Pakistan, Turkmenistan and São Tomé and Principe, and the northern part of Cyprus as jurisdictions with severe deficiencies on ML/TF matters: see FATF Chairman's Summary, London Plenary, June 18-20, 2008, online: Financial Action Task Force < http://www.fatf-gafi.org/dataoecd/50/1/40879782. pdf> (accessed February 11, 2009) [FATF Chairman's Summary].

43 FATF Revised Mandate 2008-2012, paras. 1, 16.

44 S. 7, online: Financial Action Task Force <http://daccessdds.un.org/doc/UNDOC/GEN/N05/446/60/PDF/N0544660.pdf?OpenElement> (accessed February 11, 2009).

45 Financial Action Task Force, *Annual Report 2006-2007*, June 29, 2007, para. 4, online: Financial Action Task Force <http://www.fatf-gafi.org/dataoecd/46/1/39162982.pdf> (accessed February 11, 2009) [FATF 2006-07 Annual Report].

46 For a complete list, see Annex 4 of the FAFT *Annual Report 2007-2008*, June 30, 2008, pp. 27-28, online: Financial Action Task Force <http://www.fatf-gafi.org/dataoecd/58/0/41141361.pdf> (accessed February 25, 2009) [FATF 2007-08 Annual Report].

47 The results of the 2008 FATF Mutual Evaluation of Canada, and more details on the process, are discussed below.

48 The Asia/Pacific Group on Money Laundering (APG), the Caribbean Financial Action Task Force (CFATF), the Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), the Grupo de Acción Financiera de Sudamérica (GAFISUD) and the Middle East and North Africa Financial Action Task Force (MENAFATF) and are Associate Members: FATF 2007-08 Annual Report, para. 8.

The membership of the FATF stands at 32 countries and territories, two regional bodies and two countries with observer status.[49] Twenty-two organizations have observer status.[50] All decisions of the FATF are taken by its members by consensus in plenary meetings. The plenary is assisted by the FATF Secretariat and chaired by the FATF President. Although the FATF Secretariat is housed at the Headquarters of the Organisation for Economic Co-operation and Development (OECD) in Paris, the FATF is a fully independent body.[51]

Working groups within the FATF are established to further the work of member countries and of the organization. These include the Working Group on Terrorist Financing and Money Laundering, the Working Group on Evaluations and Implementation and the Working Group on Typologies.[52]

Delegations established by each country usually consist of government officials working in finance (in Canada's case, officials from the Department of Finance) and representatives from other government bodies, such as financial intelligence units (FIUs), law enforcement, intelligence and border control agencies, and justice and foreign affairs departments.[53]

In February 2008, the FATF published a paper entitled "Terrorist Financing." In part, it describes various TF "typologies" (methods and trends associated with TF).[54] Previous published FATF papers often dealt with both money laundering and TF issues, but appeared to attach greater importance to money laundering.

Between 1995 and 2004, the FATF published in-depth papers on several subjects relating to money laundering and TF, including papers about precious metal/stones dealers, commercial websites and Internet payment systems, the trade system, real estate, corporate vehicles for raising funds, new payment methods and general typologies.[55] The FATF has agreed to undertake studies in several additional areas, including TF risks in the securities sector.[56] These studies can

---

49 FATF Chairman's Summary, notes 3-4. As per this document the 34 members of the FATF are: Argentina; Australia; Austria; Belgium; Brazil; Canada; China; Denmark; the European Commission; Finland; France; Germany; Greece; the Gulf Co-operation Council; Hong Kong; China; Iceland; Ireland; Italy; Japan; Luxembourg; Mexico; the Kingdom of the Netherlands; New Zealand; Norway; Portugal; the Russian Federation; Singapore; South Africa; Spain; Sweden; Switzerland; Turkey; the United Kingdom; and the United States. The observer countries are India and the Republic of Korea.

50 FATF Revised Mandate 2008-2012, para. 21.

51 FATF 2006-07 Annual Report, para. 8.

52 FATF 2007-08 Annual Report, paras. 10-11.

53 FATF 2007-08 Annual Report, para. 7.

54 Financial Action Task Force, *Terrorist Financing*, February 29, 2008, pp. 7-10, online: Financial Action Task Force <http:/www.fatf-gafi.org/dataoecd/28/43/40285899.pdf> (accessed February 12, 2009) [FATF Report on Terrorist Financing].

55 The papers can be found on the FATF website. They include: *RBA Guidance for Dealers in Precious Metal and Stones* (2008); *Money Laundering & Terrorist Financing Risk Assessment Strategies* (2008); *Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems* (2008); *Best Practices Paper on Trade Based Money Laundering* (2008); *Money Laundering & Terrorist Financing through the Real Estate Sector* (2007); *Laundering the Proceeds of VAT Carousel Fraud* (2007); *Trade Based Money Laundering* (2006); *The Misuse of Corporate Vehicles, Including Trust and Company Service Providers* (2006); and *Report on New Payment Methods* (2006).

56 FATF Chairman's Summary, p. 1.

help those entities in Canada which must report financial transactions to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

1.2.1.3 Other International Organizations

The World Bank and the International Monetary Fund also play important roles in fighting TF, since both normally deal with the financial sectors of countries. Both organizations assist in monitoring standards for financial institutions and in studying typologies, as well as provide assistance to countries in TF matters and in the regulation of financial institutions.[57] Other groups, such as the Basel Committee on Banking Supervision, the Wolfsberg Group of Banks, the International Association of Insurance Supervisors and the Egmont Group of Financial Intelligence Units (the Egmont Group[58]), also contribute.[59]

1.2.2 Differing Interpretations among Countries about TF Issues

As Professor Passas noted, approaches to TF vary widely among countries:

> [T]here is no uniform legal approach to countering the financing of terrorism (CFT). Some jurisdictions mirror UN model laws, while others adopt their own methods or merely extend money laundering provisions to cover CFT. The national regimes vary with respect to the range of activities and groups covered, the types of assets or financial activities included, the origin of funds raised to finance terrorist acts, the intent or knowledge of individuals, whether an activity, act or group is financed, etc. [60]

Work to counter international TF is complicated by the disagreements which may arise between countries regarding what conduct is illegal and which organizations should be pursued – a complication worsened when money flows, as it often does, between jurisdictions.

---

57 For more information on the subject, see Jae-myong Koh, *Suppressing Terrorist Financing and Money Laundering* (Berlin: Springer, 2006), pp. 168-177 [Koh, *Suppressing Terrorist Financing and Money Laundering*]. The World Bank Guide to Anti-Money Laundering and Combating Terrorism Financing is of interest to all jurisdictions because it describes useful steps which can be taken to combat TF, based on international standards.

58 The Egmont Group is the coordinating body for the international group of financial intelligence units (FIUs). It was formed in 1995 to promote and enhance international cooperation in anti-money laundering and counter-terrorist financing: The Egmont Group, Press Release, "Egmont Group Appoints Head of New Permanent Secretariat," May 17, 2007, online: The Egmont Group <http://www.egmontgroup.org/ExecSecPR.pdf> (accessed February 12, 2009).

59 For more information, see Koh, *Suppressing Terrorist Financing and Money Laundering*, pp. 143-154.

60 Nikos Passas, "Understanding Terrorism Financing" in Vol. 2 of Research Studies: Terrorism Financing Charities and Aviation Security, p. 28 [Passas Paper on Terrorism Financing]. Passas also described how several countries had implemented the international requirements on TF: Passas Paper on Terrorism Financing, pp. 25-27.

The Liberation Tigers of Tamil Eelam (LTTE) provides an example of the practical difficulties caused by differing definitions among countries of "terrorism" and "terrorist organization." The LTTE was designated as a "listed entity" (meaning, in general, a prohibited group), or its equivalent, by the United Kingdom (2001),[61] Australia (2001)[62] and the European Union (May 2006).[63] Canada listed the LTTE as a terrorist group in April 2006.[64]

Between 2001 and 2006, it would have been easier to prosecute the LTTE in the UK or Australia than in Canada because the group was not yet listed here. It was possible to prosecute an unlisted terrorist group in Canada, but the prosecution would have needed to prove that the group was terrorist; on the other hand, a group that had been listed would from that mere fact be considered terrorist, with no further proof required.[65] If Canada had listed the LTTE earlier, the group would likely have moved its fundraising activities to a country where it was still unlisted.

1.2.3 Canada's International Involvement in Anti-Terrorist Financing Matters

Canada is active on the international scene in anti-TF matters through several organizations[66]:

- the FATF: Canada is a founding member, and a former Canadian government official presided over the FATF in 2006-07. The Department of Finance is the lead Canadian department for Canada's dealings with the FATF;[67]
- the Asia/Pacific Group;
- the Caribbean Financial Action Task Force;[68]
- the Egmont Group;

---

61 *Terrorism Act 2000 (Proscribed Organisations) (Amendment) Order 2001*, S.I. 2001/1261.

62 *Charter of the United Nations (Anti-terrorism – Persons and Entities) List 2001* (No. 2), online: Government of Australia, Department of Foreign Affairs and Trade <http://www.dfat.gov.au/icat/persons_entities/2_proscribed_entities_10dec2001.html> (accessed February 11, 2009).

63 Declaration by the Presidency on behalf of the European Union concerning listing of the LTTE as a terrorist organisation, online: Europa <http://europa.eu/rapid/pressReleasesAction.do?reference=PESC/06/78&format=HTML&aged=0&language=EN&guiLanguage=en> (accessed February 11, 2009). Interestingly enough, the press release mentions that "[t]he decision of the EU to list the LTTE should come as a surprise to nobody," since the LTTE had received several warnings.

64 Public Safety Canada, "Currently listed entities," online: Public Safety Canada <http://www.publicsafety.gc.ca/prg/ns/le/cle-en.asp#ltte> (accessed February 11, 2009).

65 A "terrorist group" is defined in s. 83.01(1) of the *Criminal Code*, R.S.C. 1985, c. C-46 as either "an entity that has as one of its purposes or activities facilitating or carrying out any terrorist activity" or an entity on a list established by the Governor in Council under s. 83.05, and includes "an association of such entities."

66 For a general description of Canada's efforts, see Testimony of Diane Lafleur, vol. 54, September 28, 2007, pp. 6767-6768.

67 Testimony of Diane Lafleur, vol. 54, September 28, 2007, pp. 6753, 6767.

68 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6767.

- the Five Eyes Group;[69] and
- the World Bank and IMF.

Because of its role and status in the FATF, Canada is an active member of a core group of countries that have taken the lead on TF matters. Canada is making strong efforts to observe its obligations under international law.[70] Evaluations of Canada's efforts are examined in Chapter IV.

Although the 2008 FATF Mutual Evaluation of Canada criticized Canada in several respects, reviews of Canada's anti-TF program show that Canada respects most of its international obligations. A lawyer who specializes in charities law, Terrance Carter, even described Canada as doing more than its obligations require against TF raised through charities, violating principles of natural justice, criminal law, and due process.[71]

1.3 The Concept of Terrorism

1.3.1 "Terrorism" and "Terrorist Organization"

Defining and understanding "terrorism" is necessary to develop measures to combat TF. What constitutes terrorism and, as a result, which financial activities need to be monitored, prohibited and eliminated?[72]

The difficulty in defining terrorism helps to explain why there is no single, international approach to TF, and why it is therefore difficult to secure the international cooperation needed to deploy effective anti-TF programs.

In his paper for the Commission, Professor Passas highlighted the challenges of defining terrorism, and of identifying certain groups as terrorist entities:

> Rebels, insurgents, resisters, guerrillas, militants, militias, independence movements, nationalists etc. come in different sizes, operate in diverse contexts, enjoy differential popular (or state) support, antagonize different social actors and represent high or low priorities of domestic, regional and international controllers. Placing them all in the same category and discussing this in general terms as 'terrorist finance and its control' obscures more issues than it clarifies. Inevitably, the label 'terrorist' is a blanket political and polemical concept

69 See Chapter III for a description of the Five Eyes Group.

70 See Testimony of Diane Lafleur, vol. 54, September 28, 2007, pp. 6768-6772 and Exhibit P-227, Tab 2: Presentation of Diane Lafleur, September 28, 2007, Slides 7-10 for a general overview of Canada's compliance efforts with the FATF's 9 Special Recommendations on TF.

71 Terrance S. Carter, "The Impact of Anti-terrorism Legislation on Charities in Canada: The Need For an Appropriate Balance," October 26, 2007, p. 13, online: Carters Professional Corporation <http://www.carters.ca/pub/article/charity/2007/tsc1026.pdf> (accessed May 12, 2009).

72 Testimony of Keith Morrill, vol. 54, September 28, 2007, p. 6690.

> that varies from one legal system to another. As a result, any discussion of 'terrorist finance' is directly affected and infected by the problem of defining terrorism.[73]

A 2002 World Bank report stated that terrorism financing was a fundamentally simple concept, but that terrorism was more difficult to define:

> Not all of the countries that have adopted the [*International Convention for the Suppression of the Financing of Terrorism*] agree on specifically what actions constitute terrorism. The meaning of terrorism is not universally accepted due to significant political, religious and national implications that differ from country to country.[74]

The organization known as "Hamas" provides a case in point. Considered terrorist by several nations,[75] Hamas was elected to the government in Palestine and thereby gained a degree of legitimacy in some eyes.

In other cases, one arm of a terrorist group may be involved in humanitarian aid efforts while another arm conducts terrorist operations. Hamas may again serve as an example. Public Safety Canada's website provided the following information from Israeli intelligence officials about the alleged dual activities of Hamas:

> In March 1996, Israeli intelligence officials estimated that roughly 95 per cent of the estimated $70-million a year that it [Hamas] collected went into such charities as hospitals, clinics and schools, with only a small portion siphoned off to pay for weapons and military operations. While some funds supposedly raised for charity go directly to the military wing, some of the charity funds intended for activists, families, and institutions are "leaked" to the terrorist apparatus and are used for terrorist activities.[76]

1.3.1.1 International Efforts to Develop a Universal Definition of "Terrorism"

The United Nations continues to struggle with defining terrorism. In 1996, UN General Assembly Resolution 51/210 established an ad hoc committee to negotiate, along with the UN Sixth (Legal) Committee, the *Draft Comprehensive*

---

73 Passas Paper on Terrorism Financing, p. 21.

74 The World Bank Guide to Anti-Money Laundering and Combating Terrorism Financing, p. I-4.

75 Hamas, or Harakat Al-Muqawama Al-Islamiya, has been a "listed entity" in Canada since 2002: see Public Safety Canada, "Currently listed entities," online: Public Safety Canada <http://www.publicsafety.gc.ca/prg/ns/le/cle-eng.aspx#hhi18> (accessed February 11, 2009).

76 Public Safety Canada, "Currently listed entities," online: Public Safety Canada <http://www.publicsafety.gc.ca/prg/ns/le/cle-en.asp#hhi18> (accessed July 28, 2008).

Convention on Terrorism.[77] That process is ongoing. DFAIT witness Keith Morrill testified that defining terrorism "has proved and will continue to prove, I think, extraordinarily difficult."[78] In the end, there is no universally accepted definition, adding to the challenges of the international fight against both terrorism and TF.

In the meantime, the international community has been dealing with terrorism by using what Morrill described as a "piecemeal" approach.[79] The international community responds to very specific and defined actions when they occur and as they have impact on world affairs. Morrill further explained that, "…[i]f you can't get people to agree on what terrorism is, you can perhaps get them to agree that it is always wrong to blow up an aircraft."[80] This latter approach to terrorism began with the 1963 *Convention on Offences and Certain Other Acts Committed on Board Aircraft* (the "Tokyo Convention").[81]

As Morrill explained, the international community reacts to a situation by adopting an appropriate convention that can then be ratified by individual countries. These countries are then responsible for implementing the convention's obligations in their domestic law.

Morrill testified that these conventions are not created in a vacuum. Canadian officials participate in their negotiation and are vocal about Canada's views. The collective views of all participants ultimately form part of the conventions.[82]

1.3.1.2 The Life Cycle of a Terrorist Organization

The structure and operations of terrorist organizations change over time. Understanding these changes is important because they may in turn lead

---

77 For more information, see C.L. Lim, "The question of a generic definition of terrorism under general international law" in Victor V. Ramraj, Michael Hor and Kent Roach, eds., *Global Anti-Terrorism Law and Policy* (Cambridge: Cambridge University Press, 2005), p. 37; Antonio Maria Costa, "Drugs, Crime and Terrorist Financing: Breaking the Links," Speech delivered at the Conference on Combating Terrorist Financing, Vienna, November 9, 2005, online: United Nations <http://www.unodc.org/pdf/ED%20speech%20to%20OSCE.pdf> (accessed February 24, 2009).

78 Testimony of Keith Morrill, vol. 54, September 28, 2007, p. 6682.

79 Testimony of Keith Morrill, vol. 54, September 28, 2007, p. 6684.

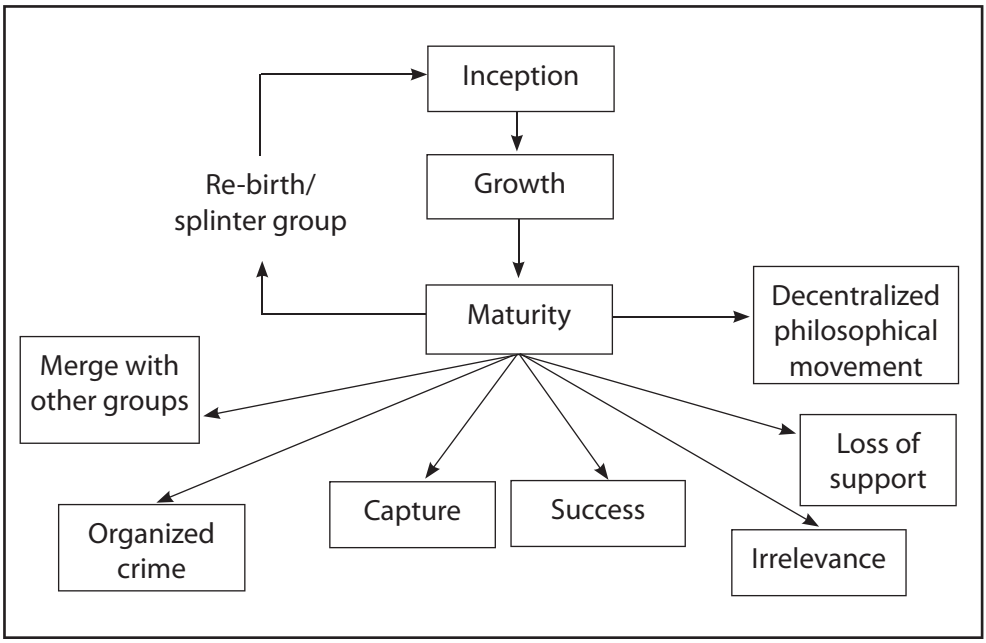
80 Testimony of Keith Morrill, vol. 54, September 28, 2007, p. 6683.

81 See the United Nations Treaty Collection, Conventions on Terrorism, online: United Nations <http://untreaty.un.org/English/Terrorism.asp> (accessed February 24, 2009); Exhibit P-226, Tab 2: Presentation of Keith Morrill, September 27, 2007. Other such conventions include: *Convention for the Suppression of Unlawful Seizure of Aircraft* (1970); *Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation* (1971); *Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents* (1973); *International Convention against the Taking of Hostages* (1979); *Convention on the Physical Protection of Nuclear Material* (1980); *Protocol on 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* (1988); *Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation* (1988); *Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf* (1988); *Convention on the Marking of Plastic Explosives for the Purpose of Detection* (1991); *International Convention for the Suppression of Terrorist Bombings* (1997); *International Convention for the Suppression of the Financing of Terrorism* (1999) and *International Convention for the Suppression of Acts of Nuclear Terrorism* (2005).

82 Testimony of Keith Morrill, vol. 54, September 28, 2007, p. 6746.

to changes in financing requirements and the methods used to raise and move funds. Law enforcement and security intelligence authorities need to understand where in its life cycle a given organization stands. For example, if a "mature" terrorist group is preparing an immediate attack, the authorities may, by monitoring the movement of funds, identify those who are likely to carry out the strike.

The stages in the life of a terrorist organization are shown in the following chart, and the main stages are described below.



1.3.1.2.1 Inception

In their initial stages, terrorist groups often have relatively few members. They may devote resources to raising their profile, possibly through violent acts and propaganda. Raising a group's profile may in turn lead to an increase in resources.

This stage in which resources are still meagre may be the most vulnerable stage in the life of a terrorist organization. Professor Bruce Hoffman, a terrorism expert from Georgetown University in Washington, DC, cited an estimate that at least 90 per cent of all such organizations die out within a year.[83]

---

83 Bruce Hoffman, *Inside Terrorism*, revised and expanded edition (New York: Columbia University Press, 2006), p. 241 [Hoffman, *Inside Terrorism*].

1.3.1.2.2 Growth

During its growth phase, a terrorist group usually gains recruits and establishes a support base. This growth leads to the group's increased influence as it acquires financial and other resources. This in turn results in an increase in activities, often violent, which may yield a further increase in size and influence.

As Hoffman noted, "…a terrorist movement's longevity ultimately depends upon its ability to recruit new members as well as appeal to an expanding pool of both active supporters and passive sympathizers."[84]

A tension exists between the size of an organization (and the corresponding influence it exerts) and its ability to maintain its own security. The larger it becomes, the more resources (human and material) it has at its disposal and the more influence it can exert through terrorist and other measures. However, the larger it becomes, the more difficulty it faces operating "underground," maintaining its own security and keeping its plans secret.

As a group grows, it may face challenges that require additional resources. These challenges commonly include the following:

- organizational challenges requiring a more formal structure for managing and coordinating the group's operational and support functions, while ensuring its own security;
- political challenges, such as the need to refine and clarify the group's objectives, beliefs and principles to maintain or increase support;
- identifying ever better targets for violent actions to maintain or increase the group's profile; and
- for those organizations initially supported by nation states, the need to identify new, more independent sources of financial support.

1.3.1.2.3 Maturity

A mature terrorist organization is well-established in terms of membership, support and objectives. It is concerned with maintaining the momentum for its cause and, in some cases, seeking out realistic options for achieving its goals.

After it reaches maturity, the evolution of a terrorist organization may proceed in one or more of several directions:

- Faced with dissatisfaction with the state of the organization (which may have become an inefficient and possibly corrupt bureaucracy),

84 Hoffman, *Inside Terrorism*, p. 225.

or with its methods (which may have become less violent), smaller and more violent splinter groups may emerge;[85]

- The organization may merge with, or establish a network of, affiliated terrorist organizations with similar or complementary objectives and aspirations;[86]
- It may evolve into a criminal organization that is concerned only with the accumulation of wealth;[87]
- Key members and resources, or both, may be captured or destroyed, effectively ending operations or returning the group to an earlier stage in the life cycle.[88]
- The organization may lose support because its objectives become stale or its tactics alienate its core support groups (for example, by engaging in excessively violent actions);[89]
- It may succeed in achieving its goals and gain legitimacy as a political party or even as the government; and
- It may become irrelevant if its objectives and environment change.[90]

1.3.2 Kinds of Terrorist Groups

Professor Passas underlined the importance of understanding how terrorist groups operate in order to undermine their TF activities. Understanding the structure and organizational methods of a group will often provide direct insight into its fundraising mechanisms and make it more vulnerable to law enforcement and surveillance efforts.

Professor Passas identified three types of terrorist groups:

- Large and popular groups that control some geographical areas and engage in providing *de facto* government services,

---

85 MIPT Terrorism Knowledge Base, "Group Profile: Real Irish Republican Army (RIRA)," online: <http://www.tkb.org/Group.jsp?groupID=91> (accessed February 14, 2007). See also MIPT Terrorism Knowledge Base, "Group Profile: Continuity Irish Republican Army (CIRA)," online: <http://www.tkb.org/Group.jsp?groupID=37> (accessed February 14, 2007).

86 MIPT Terrorism Knowledge Base, "Group Profile: Bersatu," online: <http://www.tkb.org/Group.jsp?groupID=3569> (accessed February 14, 2007).

87 MIPT Terrorism Knowledge Base, "Group Profile: Ulster Volunteer Force (UVF)," online: <http://www.tkb.org/Group.jsp?groupID=124> (accessed February 14, 2007).

88 MIPT Terrorism Knowledge Base, "Group Profile: Babbar Khalsa International (BKI)," online: <http://www.tkb.org/Group.jsp?groupID=4568> (accessed February 14, 2007).

89 Hoffman notes that "…[t]he more successful ethno-nationalist/separatist terrorist organization will be able to determine an effective level of violence that is at once 'tolerable' for the local populace, tacitly acceptable to international opinion, and sufficiently modulated not to provoke massive governmental crackdown and reaction.… For some terrorists, however, the desire for action can lead to an obsession with violence itself.": Hoffman, *Inside Terrorism*, pp. 233, 246.

90 MIPT Terrorism Knowledge Base, "Group Profile: Contras," online: <http://www.tkb.org/Group.jsp?groupID=250> (accessed February 14, 2007). For more details on the decline of terrorist groups, see Steven Hutchinson and Pat O'Malley, "How Terrorist Groups Decline," ITAC Presents, Trends in Terrorism Series, Vol. 2007-1, online: Integrated Threat Assessment Centre <http://www.itac-ciem.gc.ca/pblctns/tc_prsnts/2007-1-eng.asp> (accessed February 24, 2009).

as well as militant activities (John Schmidt, a senior financial intelligence analyst seconded from FINTRAC to the Integrated Thread Assessment Centre (ITAC), referred to these as "large international hierarchical organizations[91]); Passas testified that current anti-TF regulatory programs appear most effective against this type of group;[92]

- Small and isolated groups that act independently, even though they may be inspired by other groups (the fully autonomous "lone wolves," as Schmidt described them[93]); and
- Small groups operating on their own but interacting with wider networks.[94]

In testimony, Schmidt added to these categories other groups or individuals whose role consists solely of funding and directing others to carry out terrorist acts as surrogates.[95]

Many terrorist groups have a regional or local focus:

- The terrorist activities of the Euskadi Ta Askatasuna (ETA) are largely contained within Spain and France. ETA's fundraising activities focus on the Basque population of the region, and tend to support criminal activities;[96]
- The Liberation Tigers of Tamil Eelam (LTTE) are also regionally focused in that terrorist acts are directed at Sri Lanka and India.[97] Despite having only regional objectives, the LTTE raises funds abroad through Tamil communities in North America, Europe and Asia.[98]

Other terrorist groups may have an international focus. Al-Qaida is the most notorious example:

> Al-Qaeda acts in part to fend off perceived attacks on Muslims, to replace 'un-Islamic regimes' that oppress Muslim citizens with true Islamic governments, expel U.S. soldiers and Western influence from the Gulf and Iraq and to take control of Jerusalem as a Muslim city.[99]

---

91 Testimony of John Schmidt, vol. 53, September 27, 2007, p. 6655.
92 Testimony of Nikos Passas, vol. 53, September 27, 2007, p. 6572.
93 Testimony of John Schmidt, vol. 53, September 27, 2007, p. 6655.
94 Passas Paper on Terrorism Financing, pp. 56-57.
95 Testimony of John Schmidt, vol. 53, September 27, 2007, p. 6655.
96 Loretta Napoleoni, *Terror Incorporated: Tracing the Dollars Behind the Terror Networks* (New York: Seven Stories Press, 2005), p. 38 [Napoleoni, *Terror Incorporated*]. ETA is a Basque nationalist and separatist organization, known also by its English name, "Basque Homeland and Freedom."
97 Napoleoni, *Terror Incorporated*, p. 242.
98 This is the designation given to the LTTE by MIPT Terrorism Knowledge Base: MIPT Terrorism Knowledge Base, "Group Profile: Liberation Tigers of Tamil Eelam (LTTE)," online: <http://www.tkb.org/Group.jsp?groupID=3623> (accessed February 14, 2007).
99 MIPT Terrorism Knowledge Base, "Group Profile: Al-Qaeda," online: <http://www.tkb.org/Group.jsp?groupID=6> (accessed February 14, 2007).

Al-Qaida operations are pursued internationally and so is its fundraising.[100] Other groups with international goals may have narrower objectives. Hamas, for example, is said to aim for broad social, moral and political reform based on Islamic principles, as well as to destroy Israel and create a Palestinian Islamic state.[101]

In general, groups with differing ideologies have differing objectives, targets and methods. As a result, the sources and uses of financing will also differ. Recognizing the differences among groups is important. An anti-TF measure that targets funds flowing to a large regional terrorist organization may not be successful with a smaller, isolated group. Still other measures may be needed to suppress the flow of funds to international terrorist networks.

1.3.3 Costs Flowing from Terrorism

Governments and terrorist groups each want to deprive the other of funds. Terrorists know that government money spent on anti-TF measures cannot be spent on other programs, while governments know that money seized from terrorist groups cannot be used for their organizational and operational needs.

Terrorist acts impose both direct and indirect costs on the general public:

- Direct costs include the loss of human life and health and the loss of physical capital due to the physical destructiveness of a terrorist attack;
- Indirect costs are those incurred by society as terrorist acts raise the level of fear in the population.

The cost of losing physical capital is relatively easy to estimate. That, however, is less true of other direct and indirect costs.

1.3.3.1 Direct Costs

The physical costs of many terrorist attacks are small relative to the value of national or local economies. For example, the cost when an aircraft is destroyed, while significant in absolute dollar terms, is small in terms of the overall economy of a country. The physical cost of the 9/11 attacks, including property damage and clean-up costs, is estimated at US$21.8 billion,[102] only a tiny proportion of the US Gross Domestic Product.

---

100 This is the designation given to Al-Qaida by MIPT Terrorism Knowledge Base: MIPT Terrorism Knowledge Base, "Group Profile: Al-Qaeda," online: <http://www.tkb.org/Group.jsp?groupID=6> (accessed February 14, 2007).

101 MIPT Terrorism Knowledge Base, "Group Profile: Hamas," online: <http://www.tkb.org/Group.jsp?groupID=49> (accessed February 14, 2007).

102 William C. Thompson, Jr., Comptroller, City of New York, *One Year Later: The Fiscal Impact of 9/11 on New York City*, September 4, 2002, p. 2 [New York Comptroller Report on Fiscal Impact of 9/11].

The human cost is impossible to quantify. Even if it were possible, no figure would reflect the enormity of the trauma suffered by victims and their families. One option, looking at "human capital" very clinically, is to estimate the lost earnings of terrorist victims. The Comptroller for the City of New York estimated that the present value of the total loss in future earnings of those killed during the 9/11 terrorist attacks was about US$8.7 billion.[103]

In the Air India bombing, the value of the destroyed Air India aircraft was about US$260 million. In addition, the loss of 329 individuals carried substantial financial consequences for their families. All this, it bears emphasizing, was dwarfed by the unquantifiable and devastating emotional trauma. As detailed in the Commission's first report, there was "…an enormous loss of human potential" on June 23, 1985, and many most promising lives were extinguished in the bombing – "…[p]arents and children, scholars, scientists, doctors, social workers, business people, artists, humanitarians and students…."[104] The victims included leaders in many fields.[105]

Most terrorist attacks to date have inflicted smaller direct costs than did the 9/11 or Air India attacks.

1.3.3.2 Indirect Costs

Terrorist acts are often designed to intimidate and disrupt in a manner that makes the indirect costs far exceed the direct costs. Following a terrorist incident, citizens and governments, savaged by fear, take many actions to avoid a repetition. Both governments and the private sector will step up their counterterrorism efforts. Many individuals, seeking to avoid becoming victims, will change their behaviour in ways that carry costs both for them and for society. Examples include the following:

- because of fears about air travel, an individual might avoid travel by airplane, causing the longer travel times that other transportation modes require; might use more dangerous transport (automobiles, for example); or might forego travel altogether if a good substitute for air travel is not available;
- an individual might choose to locate business and personal activities in locations where terrorism is less likely, but where economic opportunities may also be less attractive; and
- some insurance costs might increase, and, if insurance coverage were reduced or denied for damage or death caused by terrorism, the individual might bear a greater level of risk.

---

103 New York Comptroller Report on Fiscal Impact of 9/11, p. 1.

104 Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, *The Families Remember* (Ottawa: Public Works and Government Services Canada, 2007), p. 9 [*The Families Remember*].

105 *The Families Remember*, p. 49.

1.3.3.3 Costs of Counterterrorism Policies

1.3.3.3.1 Public Costs

Counterterrorism efforts by governments can be expensive, involving airport security and border control measures, the monitoring of the financial system, and even military operations. Apart from the benefits to security industries and to those employed by government to deal with terrorism issues, these efforts drain resources from economically productive activities.

Increased security expenditures by government may be one response to terrorism. However, terrorism may also create a political climate for governments to introduce intrusive and expensive security measures and surveillance that the public would not otherwise tolerate. In both cases, there is an increased cost to government and a redirection of limited government resources.

1.3.3.3.2 Private Costs

Examples of costs imposed on the private sector by counterterrorism policies include:

- direct financial costs borne by individuals and businesses to comply with enhanced counterterrorism laws and policies (such as the additional costs incurred by private sector financial institutions to comply with reporting requirements under the *PCMLTFA*);
- reduced economic activity caused by greater costs to individuals and businesses (such as higher taxes to support counterterrorism efforts); and
- the non-monetary cost of the loss of civil liberties and other freedoms because of counterterrorism laws and policies.

1.3.3.3.3 Economics of Terrorism and Terrorist Financing

Terrorist groups must be selective, choosing the attacks and other activities that will best help them reach their objectives. Financial constraints limit both the number and the type of terrorist acts that a group can carry out. In addition, financial constraints limit the supporting activities (such as propaganda, recruiting and fundraising) that a group can pursue.

A "substitution effect" occurs when the costs of terrorist activities change. In general, terrorist groups will limit costly activities and substitute activities that are less costly. For example, metal detectors began to be installed at airports in the 1970s. This did not deplete terrorist resources, but it did raise the cost of carrying out a successful "skyjacking." As a result, terrorists moved away from skyjackings but increased the taking of hostages.[106]

---

106 Walter Enders and Todd Sandler, *The Political Economy of Terrorism* (New York: Cambridge University Press, 2006), pp. 127-128.

1.4 The Terrorist Financing Concept

1.4.1 The Extent of Terrorist Financing

Much terrorist activity, including TF, is covert. As a result, the value of the funds and property involved is difficult to estimate.[107] Differing definitions among countries of what constitutes terrorism and, by extension, what constitutes TF further complicate valuations.[108]

No witness who appeared before this Commission felt it possible to estimate the dollar value of TF activity, whether in Canada or globally. In short, anti-TF measures must seek to contain an activity of unknown value.

In Canada, the sums identified in disclosures by FINTRAC to law enforcement agencies and CSIS are often used to estimate the value of funds involved in TF.[109] In 2006, FINTRAC reported $256 million in disclosures related to *suspected* TF and other threats to the security of Canada.[110] In 2007, the corresponding figure was $208 million.[111] However, witnesses before the Commission raised doubts about using these figures as indicators of the value of TF in Canada. Mark Potter, Assistant Director for Government Relationships at FINTRAC, testified that, at best, these numbers provide raw intelligence that requires further analysis to make it useful.[112] RCMP Superintendent Rick Reynolds indicated that the amounts reported by FINTRAC as being connected to TF seemed high in light of the RCMP's own observations.[113]

Other jurisdictions have similar problems in determining the value of funds involved in TF.

1.4.2 Understanding the TF Process

The purposes for which terrorists use funds are commonly described as operational or organizational.[114] Acts of terrorism themselves may cost relatively little, while maintaining the groups and networks behind those acts generally costs more.

---

107 The World Bank Guide to Anti-Money Laundering and Combating Terrorism Financing, p. I-6; Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6826.

108 Martin Rudner, "Using Financial Intelligence Against the Funding of Terrorism" (2006) 19(1) International Journal of Intelligence and Counterintelligence 32 at 45 [Rudner Article on Using Financial Intelligence].

109 A review of several media reports and analyses has shown that these numbers are often cited.

110 Financial Transactions and Reports Analysis Centre of Canada, *FINTRAC 2006 Annual Report*, p. 8, online: Financial Transactions and Reports Analysis Centre of Canada <http://www.fintrac.gc.ca/publications/ar/2006/AR-eng.pdf> (accessed February 12, 2009).

111 Exhibit P-440, Tab 7: FINTRAC Response to Outstanding Questions related to Terrorist Financing, Question 2(e).

112 Testimony of Mark Potter, vol. 56, October 2, 2007, pp. 6952-6953.

113 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6868.

114 See, for example, the FATF Report on Terrorist Financing.

1.4.2.1 Operational Funding

Operational funding usually includes the cost of an attack, salaries, communications, travel and training.[115] All these expenditures relate to a specific terrorist operation. Professor Passas gave the Commission estimates of the operational costs of several terrorist attacks:

Operational Costs of Terror
Madrid 2004 bombings – about €15,000 (in addition to these operational costs, explosives were acquired in a barter deal for illicit drugs with a street value of about €35,000)
Bali nightclub bombings – about $20,000
US embassy bombings in Kenya and Tanzania – about $10,000
Attacks in Istanbul – less than $40,000
9/11 attacks – about $320,000 for 19 hijackers over about two years
Paris bombs – a few hundred euros
USS Cole 2000 attack in Aden – less than $10,000
Bishopsgate IRA attack – £3000
London 2005 attacks – a few hundred British pounds Jakarta 2003 Marriott Hotel bombing – about $30,000
Chechnya: $4,000 to down the airplanes; $7,000 for bomb attacks on Kashirskoye Highway and near metro station.
Nord-West operation in Beslan – $9,500
Germany Planned 2006 train bomb attempt – less than €200 Cologne bomb – $241
Air India bombings – $3000 CAD
Planned Amman, Jordan chemical attack – $170,000 [116]

115 FATF Report on Terrorist Financing, pp. 7-8.

116 Passas Paper on Terrorism Financing, p. 55. Passas states the following as the sources for this information: "Personal interviews with investigators and prosecutors from the US, UK, France, Germany, Spain, Turkey, FBI; UN Monitoring Team reports; on Jordan: Air Security International; on Chechnya: Shamil Basaev statement; on US East Africa embassy and Bali bombings, 9/11 Commission Staff report: 27-28. It should be noted that an official inquiry into the London bombings in 2005 estimated the total cost of overseas and UK trips, bomb-making equipment, rent, car hire, to less than £8,000. This was funded through defaulted loans, account overdrafts and cheques that eventually bounced.": pp. 55-56. See also Testimony of Nikos Passas, vol. 53, September 27, 2007, p. 6610.

Passas testified about the difficulties in estimating the value of actual terrorist operations: "Everybody is going to have a different counting method and this is why we have a very wide range of estimates in all of these cases."[117] However, it is striking that relatively small sums are needed to fund actual terrorist operations.

1.4.2.2 Organizational Funding

Terrorist groups need money for organizational matters such as recruitment, planning and infrastructure support.[118] As noted, it is significantly more costly to support terrorist organizations and networks than to carry out terrorist acts.[119]

1.4.3 Terrorist Financing in Practice[120]

Some methods of TF are widely used, while others are closely identified with specific groups.[121] One TF method might be more suited to a particular group than to another, and one group may use several fundraising methods. The methods (though not the planned uses of the funds) may be legal[122] or illegal.

One ITAC intelligence assessment stated, for example, that with Al-Qaida, "… [i]n the absence of a central command to allocate expenditure, the locally compartmentalized cells have increasingly resorted to raising funds through whatever local or regional means are available."[123]

The reasons for forming a terrorist group, its location, its means, its members and its objectives all play a role in the way funds are raised and moved.[124] To combat TF, intelligence and law enforcement agencies must acquire an understanding of how these differences among terrorist groups influence their fundraising methods.

In his evidence before the Commission, Detective Inspector Paul Newham of the United Kingdom's National Terrorist Financial Investigations Unit discussed the variety of TF methods used in the UK: "Terrorist financing is quite a complex

117 See also Testimony of Nikos Passas, vol. 53, September 27, 2007, p. 6610.
118 Rudner Article on Using Financial Intelligence, p. 35.
119 See, for example, the FATF Report on Terrorist Financing, p. 10: "…[A]lthough individual terrorist attacks can yield great damage at low financial cost, a significant infrastructure (even if relatively loosely organised) is required to sustain international terrorist networks and promote their goals over time."
120 For an in-depth analysis of the phenomenon, see Passas Paper on Terrorism Financing.
121 See Testimony of John Schmidt, vol. 53, September 27, 2007, pp. 6656-6657, for a general description of fundraising activities, both legitimate and illegitimate.
122 These may be "significant amounts": Passas Paper on Terrorism Financing, p. 34.
123 Exhibit P-223, Tab 2: Integrated Threat Assessment Centre Intelligence Assessment, "Terrorist Financing: How it is Done, and How it is Countered," March 24, 2006, para. 2 [ITAC Intelligence Assessment on Terrorist Financing].
124 The Passas Paper on Terrorism Financing offers a tentative general typology of why certain terrorists groups would choose one fundraising/transfer method over others at pp. 56-57. See also Testimony of Nikos Passas, vol. 53, September 27, 2007, p. 6567.

picture [in the United Kingdom]. It varies regionally. It varies from organization to organization in terms of terrorist groupings. So there is no one single method of terrorist financing."[125]

John Schmidt from ITAC also spoke about the variety of TF methods: "…[T]errorist activities can range from being highly specific, planned and organized to being essentially random and opportunistic and these differences result in different resourcing needs, capabilities and mechanisms."[126] He said that TF methods were constantly evolving.[127] Professor Passas wrote about the variety of fundraising methods: "One aspect of terrorist finance is clear and undisputed: there is a wide range of fund-raising methods and sources, some of which are particular to specific groups or contexts, while others are quite common across the board."[128]

One ITAC intelligence assessment spoke of the "…great variety of relatively anonymous methods for raising and moving money" and stated that "…terrorists have proven resilient in circumventing restrictions and shifting their reliance among the many conventional and unconventional financial transaction options."[129]

However, Passas warned that "…trivialized conclusions to the effect that 'everything funds terrorism' and 'all channels are used for fund transfers' … would not be particularly helpful to strategic planning, prioritization and focus of limited resources."[130]

Those involved in TF go to great lengths to avoid detection by the authorities. Professor Passas testified that UK police had discovered a manual attributed to Al-Qaida. The manual discussed the following:

> ...how to not put all their eggs in the same basket; to have operational funds in multiple places; not tell other members of the group where the funds are; take precautions when carrying amounts of money; to keep it at lower amounts; and also, using non-members for the facilitation of their transactions.[131]

---

125 Testimony of Paul Newham, vol. 58, October 4, 2007, pp. 7227-7228.
126 Testimony of John Schmidt, vol. 53, September 27, 20007, p. 6655.
127 Testimony of John Schmidt, vol. 53, September 27, 2007, p. 6655.
128 Passas Paper on Terrorism Financing, p. 30. See also Testimony of Nikos Passas, vol. 53, September 27, 2007, pp. 6564-6565.
129 ITAC Intelligence Assessment on Terrorist Financing, para. 1. This document encompasses the kind of work ITAC does, but it is not an example of a standard threat assessment. The document attempts to give an overview, which John Schmidt qualifies as "good." The document and model are exceptions to the work of ITAC because they focus on methodology instead of a specific threat: Testimony of John Schmidt, vol. 53, September 27, 2007, pp. 6646-6648.
130 Passas Paper on Terrorism Financing, p. 23.
131 Testimony of Nikos Passas, vol. 53, September 27, 2007, p. 6578.

1.4.3.1 Raising Funds

1.4.3.1.1 State Support

A Department of Finance Memorandum of Evidence on Terrorist Financing provided to the Commission explained that there are two primary sources of funding: state sponsors and "revenue-generating" activities. The Memorandum placed wealthy donors in the same category as state sponsors.[132] Revenue-generating activities may involve legal or illegal sources.

State support for terrorism is not new. During the Cold War, for example, superpowers sponsored militant groups around the globe.[133] Examples include state support for extremist Irish, Palestinian, Central and South American, Angolan and South African groups.[134]

Even after the Cold War, state sponsorship continued, though in a different context and for different purposes. The U.S. Department of State currently designates the following countries as sponsors of terrorism: Cuba, Iran, Sudan and Syria.[135] Professor Passas identified Hamas, Hezbollah, Hizbul Mujahideen, the Islamic Militant Union (IMU), Islamic Jihad, Lashkar e Taiba (LeT), Jaish-e-Mohammad (JeM) and Sipah-e-Sahiba (SSP) as among the groups sponsored by states.[136]

Professor Hoffman argued that direct state sponsorship of terrorism is used by some countries "…as a deliberate instrument of foreign policy: a cost-effective means of waging war covertly, through the use of surrogate warriors or 'guns for hire' – terrorists."[137]

However, dependence on states for funding also means that such groups may become beholden to the wishes of those states. As a result, some terrorist groups try to reduce their dependence on state sponsorship. Beginning in the early 1960s, the Palestine Liberation Organization (PLO) took steps to become independent of state sponsorship, especially that of Egypt and Syria. The PLO feared that the flow of funds depended on the perceived usefulness of the group to the domestic politics of the sponsoring states.[138]

Professor Passas wrote that state sponsorship may include "turning of blind eyes" to questionable activities rather than providing direct state funding.[139] This might mean a loose application by states of rules governing financial transactions or charitable organizations. Such states are referred to in this volume as the "weak links" in the anti-TF process.

---

132 Department of Finance Memorandum of Evidence on Terrorist Financing, para. 2.2.
133 Passas Paper on Terrorism Financing, p. 31.
134 Passas Paper on Terrorism Financing, p. 31.
135 Office of the Coordinator for Counterterrorism, "State Sponsors of Terrorism," online: U.S. Department of State <http://www.state.gov/s/ct/c14151.htm> (accessed February 12, 2009).
136 Passas Paper on Terrorism Financing, p. 31.
137 Hoffman, *Inside Terrorism*, p. 258.
138 Napoleoni, *Terror Incorporated*, p. 45.
139 Passas Paper on Terrorism Financing, p. 19.

Besides the desire of some terrorist groups to end reliance on state support, international pressures may have played a role in the decline of state sponsorship.[140] As state sponsorship diminishes, terrorist groups must find other ways to raise funds. Still, state sponsorship remains an important component of TF. Passas noted that "…[e]ven though virtually everyone agrees that state sponsorship is in decline, the phenomenon has not disappeared."[141]

1.4.3.1.2 "Legitimate" Sources of Funds

Employment and Business Income

One relatively simple way to raise money for terrorism purposes is to use money gained by legitimate means.[142] The owner of a legal business could use its profits to subsidize terrorist activities. The profits would be legitimate, but giving them to a terrorist group would violate the *Criminal Code*. In other cases, a terrorist organization itself controls a business. It can both use the profits and rely on any "synergy" between the business and the objectives of the organization, as in the following situations:

- The business provides goods or services that the terrorist organization can use in its own operations; or
- The business provides goods or services that a community needs but cannot otherwise obtain, generating goodwill among the community members whose support the terrorist organization is seeking.

In his report, Professor Passas stated that the most resilient and well-organized groups were diversifying into legitimate businesses. These included the Abu Nidal Organisation, LeT, LTTE, the Fuerzas Armadas Revolucionarias de Colombia (FARC), Hezbollah, the Irish Republican Army (IRA) and Jemaah Islamiya.[143]

One oft–cited, but controversial, example of a legitimate business that was reportedly controlled by a terrorist entity and that may have financed terrorism is the Gum Arabic Company Ltd. Napoleoni wrote that Usama bin Laden had acquired the company and that it had a near monopoly in the Arabic gum market.[144] The controversy arises about whether the company was actually used to finance terrorist activity. The U.S. 9/11 Commission, for example, concluded that Al Qaida did not benefit from businesses belonging to bin Laden or from his personal fortune.[145] Whether or not the business was used to fund terrorist activity, the Gum Arabic Company stands as a possible example of how a legitimate business could be controlled by a terrorist organization and used to facilitate TF.

---

140 FATF Report on Terrorist Financing, p. 15.
141 Passas Paper on Terrorism Financing, p. 31.
142 Testimony of Nikos Passas, vol. 53, September 27, 2007, p. 6564.
143 Passas Paper on Terrorism Financing, p. 34.
144 See, for example, Napoleoni, *Terror Incorporated*, p. 167.
145 National Commission Monograph on Terrorist Financing, pp. 17, 20.

Self-funding through a business or the personal finances of members of an organization is ideal for financing smaller attacks,[146] and where the group's operating costs are not great.

Charitable Organizations[147]

The 2006 ITAC Intelligence Assessment, *Terrorist Financing: How it is Done, and How it is Countered*, states that "…[c]harities constitute, wittingly or not, a significant source of financing."[148] Professor Passas wrote that "…[w]ith respect to charities, a distinction can be drawn between those that have had their funds unknowingly diverted and those that have been corrupted and act as fronts."[149] The funds provided to charities by well-meaning contributors can be diverted "on the ground."[150] As Professor Rudner, Professor Emeritus and distinguished research professor at Carleton University, wrote, "…[e]xtremist clerics, corrupt officials, and well-placed facilitators have functioned as critical enablers for that redirection of funds from religious institutions and humanitarian organizations to terrorist activities and operations."[151] In some cases individuals knowingly contribute to charities that are "fronts" for terrorist organizations.

The FATF noted that, because of the large volume of funds and assets handled by the charitable sector, even a small part of those funds ending up in terrorist hands would pose a serious problem.[152]

An extensive discussion of the role of charities in TF, and particularly the role of Canadian charities, appears in Chapter VI.

1.4.3.1.3 Illegal Sources of Funds

The relationship between terrorism and other types of crimes is complex.[153] Criminal activity can provide funds for terrorist groups, although criminals may not work in the same ways as terrorist groups to raise funds. Professor Passas noted that "...criminal groups for-profit have very different motives and often

---

146 FATF Report on Terrorist Financing, p. 14.
147 See also Testimony of Nikos Passas, vol. 53, September 27, 2007, pp. 6578-6588.
148 ITAC Intelligence Assessment on Terrorist Financing, para. 5.
149 Passas Paper on Terrorism Financing, p. 34. For examples of fronts, see Rudner Article on Using Financial Intelligence, p. 44.
150 Testimony of Nikos Passas, vol. 53, September 27, 2007, p. 6565.
151 Rudner Article on Using Financial Intelligence, p. 44.
152 FATF Report on Terrorist Financing, p. 25.
153 See passages in the Passas Paper on Terrorism Financing, pp. 35-42; Testimony of Nikos Passas, vol. 53, September 27, 2007, pp. 6565-6666; Yvon Dandurand and Vivienne Chin, "Links Between Terrorism and Other Forms of Crime" (2004), Report to Foreign Affairs Canada and The United Nations Office on Drugs and Crime, online: International Centre fro Criminal Law Reform and Criminal Justice Policy <http:/www.icclr.law.ubc.ca/Publications/Reports/TNOC_LINKS_STUDY_REPORT.pdf> (accessed February 24, 2009); and Pat O'Malley and Steven Hutchinson, "Actual and Potential Links Between Terrorism and Criminality," ITAC Presents, Trends in Terrorism Series, Vol. 2006-5, online: Integrated Threat Assessment Centre <http://www.itac-ciem.gc.ca/pblctns/tc_prsnts/2006-5-eng.asp> (accessed February 24, 2009) [O'Malley and Hutchinson Article on Links Between Terrorism and Criminality], among many others.

different methods, different objectives, than militant ideologically motivated groups."[154] As a result, security intelligence and law enforcement authorities must be alert to numerous criminal fundraising options when developing anti-TF measures.

An ITAC intelligence assessment described the shift towards criminal activity to provide TF:

> As a result of the crackdown on charities and front companies, some experts believe terrorist reliance on illegal money has increased exponentially....Criminal activity associated with terrorists includes the drug trade, smuggling of weapons and other goods, fraud, kidnapping, extortion, credit card and bank account fraud and manipulation, and simple robbery.[155]

The range of criminal activity that can be used to raise funds is broad. Passas identified robberies, extortion, kidnapping, hijacking, informal taxation of both legal and criminal enterprises, blackmail, protection rackets, fraud, counterfeiting, drug trafficking and smuggling.[156] The FATF noted that some terrorist groups might move from one type of criminal activity to another as the situation requires.[157]

The extortion of members of expatriate communities is an oft-used and effective TF technique, especially where there are substantial expatriate communities originating from current or former conflict zones. The extortion may involve the unofficial "taxation" of the legitimate earnings, savings or businesses of community members.[158] They often cooperate out of fear of retribution against themselves or their families in Canada or abroad.[159]

In Canada, two groups have been exposed for their alleged extortion – the LTTE and the World Tamil Movement (WTM). Both target the sizeable Tamil community in Canada. One RCMP affidavit in a case involving the LTTE stated that its investigation of the LTTE revealed that the World Tamil Movement and the LTTE "…have been demonstrated to utilize pressure tactics to elicit

---

154 Testimony of Nikos Passas, vol. 53, September 27, 2007, p. 6565.
155 ITAC Intelligence Assessment on Terrorist Financing, para. 11. The ITAC document also discusses the North Carolina case and similar examples in Europe at paras. 12-13.
156 Passas Paper on Terrorism Financing, pp. 35-36; Testimony of Nikos Passas, vol. 53, September 27, 2007, p. 6565.
157 FATF Report on Terrorist Financing, p. 19.
158 FATF Report on Terrorist Financing, p. 18.
159 FATF Report on Terrorist Financing, p. 18.

funds and donations as well as to participate in veiled threats."[160] The same affidavit presented many examples of alleged TF activities, and stated that "… [f]undraising activities were being conducted aggressively by WTM members in the Montreal area. The WTM members were visiting families and businesses in the Tamil community, demanding amounts which ranged from $2500 to $30,000.[161]

The profit generated by criminal activity can be much greater than that of legitimate businesses. This is because criminal activity typically involves either appropriation from others or the enormous profits that criminals make in illicit ("black") markets, such as those created by drug prohibition, excessive or differential tax rates on alcohol and tobacco, high import duties and other trade barriers.[162] In a black market, criminal organizations, often using physical intimidation, can assert monopoly control, charging exorbitant prices and bringing in correspondingly large profits.

Smuggling and selling contraband on the black market is not restricted to developing countries. The trade in illegal drugs is one example of an illegal market that thrives even in wealthy countries. Hezbollah is known to have benefited from smuggling cigarettes between North Carolina and Michigan, exploiting the differences in sales taxes between the two states.[163]

Because of the black market created by their prohibition, illegal drugs are a major source of income for some terrorist and insurgent groups. Law enforcement and security intelligence authorities have observed a recurring link between drugs and terrorism.[164] The 9/11 Commission's monograph on TF stated that drugs were an important source of income for the Taliban. However, the Commission found no substantial evidence of links, before or after 9/11, between Al-Qaida and the drug trade.[165]

---

160 Affidavit of Shirley Davermann, April 1, 2008, para. 3 [Affidavit of Shirley Davermann]. The LTTE also apparently benefited from pre-authorized payment plans. For an interesting read on the LTTE in Canada (and other groups), see Stewart Bell, *Cold Terror: How Canada Nurtures and Exports Terrorism Around the World* (John Wiley & Sons Canada, Ltd., 2007). Bell quotes a leading world expert on the LTTE as stating that Canada is the bank of the LTTE. Bell also notes estimates that the LTTE was raising millions of dollars per year in Canada: pp. 49-50. He gives examples of alleged trade-business fraud and fraud companies (p. 68), false charitable donations (p. 66), collection jars and the sale of paraphernalia (pp. 52-65) and government grants (pp. 59-61). Furthermore, according to Bell, one reason for the significant LTTE presence in Canada is the relative speed with which the organization was designated in the U.S. (in contrast to Canada): p. 79.

161 Affidavit of Shirley Davermann, para. 239.

162 Napoleoni, *Terror Incorporated*, p. 202.

163 For more information, see O'Malley and Hutchinson Article on Links Between Terrorism and Criminality, p. 4.

164 FATF Report on Terrorist Financing, p. 15. In his paper, Passas warned the Commission that links between drugs and terrorism should not be made too hastily: "Even though such links are not surprising, it must be impressed that there are very good reasons why any alliances between terrorists and drug traffickers *cannot* last for very long, due to fundamental incompatibilities of objectives and outlook as well as attitudes toward the State.": Passas Paper on Terrorism Financing, p. 38.

165 National Commission Monograph on Terrorist Financing, pp. 22-23.

1.4.3.1.4 Other Sources of Funds

Professor Rudner observed that "…[m]ilitant groups have also raised substantial funds through the sale of inspirational tracts, advocacy literature, audio cassettes, videos and CDs, and other iconic paraphernalia."[166] Some sales would be legitimate, but others could be illegal, such as sales of material promoting hatred.

1.4.3.2 Movement of Funds

Raising funds is the first major component of TF. The second is moving the funds after they are raised. Funds may need to leave Canada to fund a terrorist attack or terrorist organization abroad, or they may be sent to Canada to fund an organization or attack here. Because funds may be more "exposed" while they are being moved, authorities can sometimes use these movements to help identify terrorists and TF. FINTRAC and most of the world's FIUs are set up mainly to detect movements of money through reports of suspicious transactions. FINTRAC receives such reports as well as information about other financial transactions, including international wire transfers. The fundraising mechanisms themselves, rather than movements of funds, are easier to combat through CSIS or RCMP operations or, in the case of charities, through monitoring by the CRA.

In his paper, Passas argued that "…one can hardly find a method that has not been used by one group or another to make payments or transfer funds and value."[167] In his testimony, he added that "…the range…is only limited by your imagination."[168] The FATF reached a similar conclusion: "[E]xperience suggests that *all* of the mechanisms that exist to move money around the globe are to some extent at risk" of being used for TF.[169]

A terrorist group involved in "self-funding" through a business or through the personal finances of its members might not have to move the funds, making it much easier to avoid notice by agencies such as FINTRAC and the entities that report to it.

1.4.3.2.1 Traditional Banking and Financial Systems

Terrorist groups, like most organizations, use formal banking and financial systems in Canada and abroad to transfer and store money. They may hold accounts in the names of individuals, businesses, charities and other entities. In addition, terrorist groups may use traditional fund transfer methods such as cheques and electronic funds (wire) transfers. They may also use money laundering methods to disguise the source and intended use of funds, including the following:

---

166 Martin Rudner, "Building Canada's Counter-Terrorism Capacity: A Proactive All-of-Government Approach to Intelligence-Led Counter-Terrorism" in Vol. 1 of Research Studies: Threat Assessment RCMP/CSIS Co-operation, p. 120 [Rudner Paper on Building Counter-Terrorism Capacity].

167 Passas Paper on Terrorism Financing, p. 42.

168 Testimony of Nikos Passas, vol. 53, September 27, 2007, p. 6566.

169 FATF Report on Terrorist Financing, p. 21.

- opening numerous banking accounts containing relatively small amounts, to create complex paper trails;
- using "front" businesses to reintegrate funds into the financial system and make the funds appear to have come from legitimate sources; and
- placing funds in off-shore tax havens.

In Western countries, financial systems are well developed and involve extensive electronic records. However, most accounts held with banks in these countries and the transactions which terrorist organizations conduct through them are sufficiently small that it is extremely difficult, if not impossible, for authorities to distinguish these transactions from ordinary banking activity.[170]

The funds needed to support terrorist groups and acts amount to only a tiny fraction of the hundreds of millions of dollars of transactions processed by the Canadian banking system daily, and the billions processed in the United States. Because transactions linked to terrorism do not have unique characteristics that allow them to be singled out by electronic searches or the monitoring of transaction records, it is impossible to identify all flows of funds that could relate to terrorism.

Financial institutions also have little incentive to monitor flows of funds relating to terrorism, unless obliged by law to do so. However, most financial institutions in developed countries likely see value in being good corporate citizens and would not want to be seen as facilitating or being complicit in TF. However, would-be good corporate citizens face a cost disincentive since they must bear the full cost of their monitoring systems.

1.4.3.2.2 Informal and Unregulated Channels for Moving Funds

The focus of anti-TF measures on the conventional banking system may have led terrorist financiers to shift to methods of moving funds that are more difficult for authorities to monitor. A 2006 ITAC intelligence assessment observed that, "…[d]eprived of safe access to conventional banking, terrorists have turned to harder-to-detect remittance methods, such as hawalas and couriers."[171]

Much has been said and written about the use of informal channels to move terrorist funds, especially hawala,[172] an informal value transfer system (IVTS). Through international migration and the Internet, hawala has spread around

---

170 See, for example, Ilias Bantekas, "The International Law of Terrorist Financing" (2003) 97(2) American Journal of International Law 315.

171 ITAC Intelligence Assessment on Terrorist Financing, para. 16.

172 For a history and explanation of hawala, see Nikos Passas, "Demystifying Hawala: A Look Into Its Social Organisation and Mechanics" (2006) 7(1) Journal of Scandinavian Studies in Criminology and Crime Prevention 46 [Passas Article on Hawala]; Passas Paper on Terrorism Financing, pp. 44-45; Testimony of Nikos Passas, vol. 53, September 27, 2007, pp. 6589-6599. INTERPOL also describes hawala on its website, online: <http://www.interpol.int/Public/FinancialCrime/MoneyLaundering/hawala/default.asp> (accessed February 24, 2009).

the world, although it is most popular in the Middle East and Asia and within immigrant communities in the West.

At a minimum, hawala involves a remitter, a recipient and two hawala operators, one working in each country with the remitter and recipient respectively. Hawala has two main elements: 1) the sending and receiving of money (this involves a hawala operator (hawaladar) and the client), and 2) the settlement process (this involves intermediaries and agents who play a role in the transaction). According to Passas, the first element is relatively straightforward, while the settlement process can be much more complex.[173]

In 2006, the Canadian Centre for Intelligence and Security Studies described a transfer of funds using hawala as follows:

> *Hawala* transfers money from one country to another without actually moving it, and the system is based on trust, to move funds and settle accounts with almost no paper trail. The transfer takes place as follows. Person A from country X wants to send money to person B in country Y. Person A gives the money to a broker (*Hawaladar*) in country X, who charges her a relatively low fee together with a more favorable exchange rate than what is offered by the bank. The broker then contacts another broker in country Y by phone, fax or email, who gives the money to person B based on a prearranged code word or number. To settle accounts with each other, the broker in country X can either reduce the debt owed by her to the broker in country Y, or else, expect a remittance from the latter.[174]

In his paper, Passas identified several other informal value transfer systems:

> Hawala, Hundi, Black market peso exchange networks, Fei chien (door-to-door and other Asian varieties), Invoice manipulation schemes, In-kind transfers, Trade diversion schemes, Courier services and physical transfer methods, Corresponding banking accounts, Charities, Gift and money transfer services overseas via special vouchers and internet web sites, Digital/Internet based transfers, Stored value (such as pre-paid telephone cards) and finally, Debit and credit cards used by multiple individuals.[175]

---

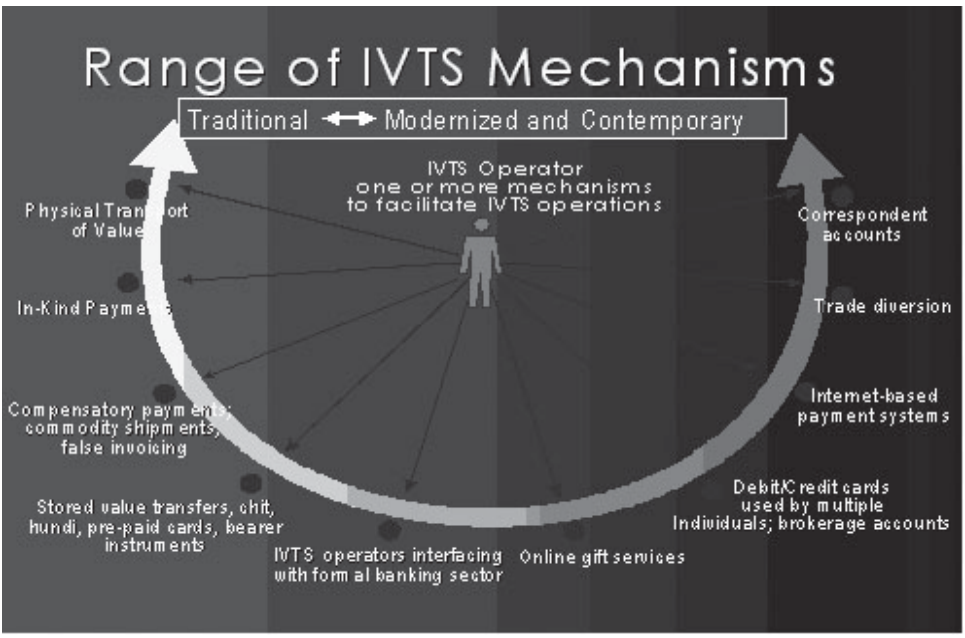
173 Passas Article on Hawala, p. 50; Testimony of Nikos Passas, vol. 53, September 27, 2007, pp. 6589-6599.

174 Canadian Centre for Intelligence and Security Studies, "Terrorism Financing and Financial System Vulnerabilities: Issues and Challenges," Vol. 2006-3, pp. 7-8, online: Integrated Threat Assessment Centre <http://www.itac-ciem.gc.ca/pblctns/tc_prsnts/2006-3-eng.pdf> (accessed February 12, 2009) [CCISS Paper on Terrorism Financing].

175 Passas Paper on Terrorism Financing, p. 43. As can be seen from the list, Passas believed that using charities, for example, to move money is an informal channel.

There may be other, lesser known, informal transfer methods, and additional methods will emerge over time.

The chart below illustrates numerous types of informal value transfer mechanisms, ranging from physical transport using couriers to more sophisticated means that include brokerage accounts and Internet payment systems.[176]



Source: Passas Paper on Terrorism Financing, p. 43.

Passas stated in his paper for the Commission that informal value transfer systems, especially hawala, became the target of aggressive policy-making "… after the word was uttered during a US Congressional hearing suggesting that this was the preferred method for al Qaeda and similar Islamist groups."[177] The international community views IVTS as a weakness in global anti-TF efforts. As well, these systems are not always fully understood by Western government authorities.[178] In addition, some see IVTS as a vulnerable point in anti-TF efforts because they believe that the systems leave a less substantial paper trail than formal transfer mechanisms. However, in his testimony, Passas criticized the "absence of paper trail" argument, at least as it related to hawala, stating that it was a "…myth that [hawala] is something without trails." He gave several examples of the types of records that hawala produces. He added, "…instead of talking about paperless [transactions], lack of trail and so on, sometimes there's just too much of it."[179]

---

176 Passas Paper on Terrorism Financing, p. 43.
177 Passas Paper on Terrorism Financing, p. 44.
178 See CCISS Paper on Terrorism Financing, p. 7.
179 Testimony of Nikos Passas, vol. 53, September 27, 2007, pp. 6591-6594.

The FATF responded to concerns about the use of IVTS in its Special Recommendation VI:

> Each country should take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network, should be licensed or registered and subject to all the FATF Recommendations that apply to banks and non-bank financial institutions. Each country should ensure that persons or legal entities that carry out this service illegally are subject to administrative, civil or criminal sanctions.

Passas warned the Commission to be cautious about demonizing some mechanisms, especially hawala. He stated that "…there are very legitimate reasons why this [hawala] is happening." Pointing during his testimony to a graphic photo of desolation to show that, in some places "…there is no ATM machine," he added, "…[i]f we misapply financial controls and take out useful services to these regions, they are the victims of misapplied law enforcement actions – innocent people who rely on Hawala in order to get the means of survival for them today."[180]

Professor Rudner also acknowledged that a system such as hawala might be used to move money for TF. However, he also cautioned against disproportionate concern about hawala:

> Although terrorism finance may in fact flow through informal value-transfer systems, little evidence suggests that traditional hawala-type mechanisms represent terrorists' preferred vehicle for financial transfers, or that these informal systems are more prone to terrorist exploitation than the formal, regulated financial sector.[181]

Hawala and other informal value transfer systems can be used for TF. However, they are not instruments of TF *per se* – an important distinction. In the end, hawala is simply one of many ways to move money for TF.[182] As Passas testified, "It is…recognized widely that the overwhelming majority of Hawala customers are legitimate people sending honestly earned money overseas. But it is also confirmed that it is subject to abuse just as is any other financial institution you can think of." [183]

---

180 Testimony of Nikos Passas, vol. 53, September 27, 2007, p. 6660.
181 Rudner Article on Using Financial Intelligence, p. 46. Rudner cited a report from the Netherlands Ministry of Justice Research and Document Centre that came to the same conclusion.
182 Testimony of Nikos Passas, vol. 53, September 27, 2007, p. 6609.
183 Testimony of Nikos Passas, vol. 53, September 27, 2007, p. 6609.

1.4.3.2.3 Couriers

FATF Special Recommendation IX calls for countries to have measures in place "…to detect the physical cross-border transportation of currency and bearer negotiable instruments, including a declaration system or other disclosure obligation." The FATF noted that the movement of cash across borders is prevalent and that couriers were one means of doing this.[184] Couriers might be more expensive than ordinary wire transfers, but less likely to leave an audit trail.[185]

A 2006 ITAC intelligence assessment reported that since 9/11 "…major terrorist cash transfers are also done by trusted couriers or, for added security, by the main operatives themselves."[186]

1.4.3.2.4 Trade Diversion

Passas identified commercial trade transactions as being vulnerable to TF and money laundering:[187]

> Literally volumes can be written about the vulnerabilities to abuse of trade transactions, which constitute a weak link (possibly the weakest and riskiest link) in AML/CFT [anti-money laundering/countering the financing of terrorism] efforts and other regulatory regimes….[188]

With trillions of dollars changing hands worldwide daily, it is almost impossible to escape the conclusion that trade transactions provide a "sea of possibilities" for TF.[189]

John Schmidt of ITAC agreed with the concerns of Passas about the trade sector.[190] The FATF recently observed that the trade sector is vulnerable[191] (and published a 40-page paper on the subject in 2006[192]), but it has not made specific recommendations relating to trade transactions. However, the international community has addressed some aspects of the trade issue, such as trading in diamonds produced in conflict zones ("conflict diamonds").[193]

---

184 FATF Report on Terrorist Financing, p. 23.
185 FATF Report on Terrorist Financing, p. 24.
186 ITAC Intelligence Assessment on Terrorist Financing, para. 18. Passas reached a similar conclusion: Passas Paper on Terrorism Financing, p. 45.
187 For a general study of the commercial trade area as it relates to TF, see Testimony of Nikos Passas, vol. 53, September 27, 2007, pp. 6614-6622.
188 Passas Paper on Terrorism Financing, p. 46.
189 Testimony of Nikos Passas, vol. 53, September 27, 2007, p. 6614.
190 Testimony of John Schmidt, vol. 53, September 27, 2007, p. 6658.
191 FATF Report on Terrorist Financing, p. 23.
192 Financial Action Task Force, *Trade Based Money Laundering*, June 23, 2006, online: Financial Action Task Force <http://www.fatf-gafi.org/dataoecd/60/25/37038272.pdf> (accessed February 12, 2009).
193 Passas also testified that the gold trade has been used to support terrorism in Colombia. For more information on gold and the conflict diamonds as they concern TF, see Testimony of Nikos Passas, vol. 53, September 27, 2007, pp. 6614-6618.

1.4.3.3 Terrorist Financing "Typologies" (Trends and Methods)

The methods and trends associated with a given phenomenon are known as "typologies."[194] Typologies can help officials to understand a phenomenon and develop better responses to it.

Several international organizations have identified typologies in money laundering and TF matters. The FATF considers developing typologies a key component of its work and has published several documents showing the typologies of money laundering and TF cases.[195] A quick review of these documents shows that the FATF focuses primarily on money laundering, but recognizes that there is some similarity between TF and money laundering typologies. Several FIUs throughout the world, including FINTRAC, provide typologies to the FATF.

Several of the TF typologies published by the FATF are set out below.

Case study: Diversion of funds from legitimate business

The personal bank account of Person A (a restaurant manager) regularly received cheques drawn from wooden pallet Company B, as well as significant cash deposits. The account did not show any "normal" financial activity such as payment for food, travel, etc. The bank account of Company B also showed significant cash withdrawals of between EUR 500000 and EUR 1 million.

The bank where A's account was held became suspicious because of the inconsistency between Person A's profession and the nature of Company B's business and submitted a suspicious transaction report to the financial intelligence unit. FIU analysis revealed that the individuals concerned were linked to Salafist movements, and the case was referred to prosecutors for wider investigation.
Source: France

194 Financial Action Task Force, *Money Laundering & Terrorist Financing Typologies 2004-2005*, June 10, 2005, p. 1, online: Financial Action Task Force <http://www.fatf-gafi.org/dataoecd/16/8/35003256.pdf> (accessed February 17, 2009) [FATF 2004-05 Typologies].

195 FATF 2004-05 Typologies, p. 1.

Case study: Small, self-funding network plans attack

In July 2006, rail employees found two unattended suitcases on two German regional trains. Improvised explosive and incendiary devices were discovered in each suitable consisting of a propane tank, an alarm clock as a timer, batteries for energy supply, various detonating agents as well as a plastic bottle filled with petrol. The instructions for building an explosive device were taken from an al-Qaeda-linked website, with components purchased in ordinary shops, costing no more than EUR 250.

No suspicious funding from abroad was required, and the suspect's primary source of funding during this period was from family members to pay for his education. The only transactions that appear to have been linked to the planned attack were for plastic bottles, which when filled with petrol and linked to propane tanks would have made an improvised explosive device.
Source: Germany

Case study: Terrorist organisation extorts money from drug traffickers

An investigation and prosecution carried out by Turkish authorities revealed that drug trafficking is the principal source of funds for a terrorist organisation. Drugs are grown in Pakistan, Afghanistan and Iran; and sent from there to Europe, both through known members of the organisation, and through their associates and other non-designated militants.

In 2007, more than 10 members of the organisation terrorist group were arrested and large amounts of money seized. Investigation and testimony by these members revealed that the organisation extorts money from smugglers at points of entry in the North of Iraq in the form of "taxes" worth around 7% of the value of smuggled items. The groups also collect money for each person or each car crossing their 'customs points.' One such "customs point" earns USD 20,000 - 30 000 per week. One member of the group stated that the most important income for the group is the money collected from drug traffickers as 'taxation'.
Source: Turkey

Case study: Extortion of a commercial organisation

In September 2007, Company C was sentenced to pay a USD 25 million criminal fine, placed on five years of corporate probation and ordered to implement and maintain an effective compliance and ethics program. Earlier in the year, Company C pleaded guilty to one count of engaging in transactions with a Specially Designated Global Terrorist (SDGT) in that, from 1997 through 2004, the company made payments to a terrorist group. The payments, demanded by the group, were made nearly every month and totalled over USD 1.7 million. The group was designated as a Foreign Terrorist Organisation in September 2001, and listed as an SDGT in October 2001.
Source: United States

Case Study: Terrorist organization uses MVT mechanisms to move money

Person D, a leader of a terrorist organization based in Country C and once a resident in Country A, was in hiding in Country B. The FIU in Country A found out through investigations that persons in Country A were sending money through money transfers to D's friends in Country B to financially support him. The money flow was detected because the transfers were made by nationals of Country C — which was unusual in Country A. Person D was later arrested in Country B on suspicion of terrorism. Money transfers from Country A to Country B were presented in court as supporting evidence of terrorist financing.
Source: The Netherlands

The Egmont Group of Financial Intelligence Units (Egmont Group) has published a review of 100 "sanitized" cases relating to money laundering.[196] Relatively few deal with TF.[197]

1.4.3.3.1 The "Terrorism Operational Cycle"

In his testimony and in a related paper, Professor Rudner described his model of a "terrorism operational cycle." He developed the model by looking at case studies of terrorism and "…breaking terrorism down into its functional and enabling activities."

196 The Egmont Group, *FIU's in action: 100 cases from the Egmont Group*, online: The Egmont Group <http://www.egmontgroup.org/files/library_sanitized_cases/100casesgb.pdf> (accessed February 12, 2009).

197 These can be accessed online: The Egmont Group <http://www.egmontgroup.org/library_sanitized_cases.html> (accessed February 12, 2009).

Rudner identified 11 stages of the cycle. Each stage consisted of a set of activities which enabled terrorism to proceed.[198] Rudner testified that the model could apply to any terrorist phenomenon.[199]

Rudner described the 11 stages of the cycle as follows:[200]

- strategic planning;
- recruitment;
- training;
- communication;
- financing;
- procurement;
- infrastructure;
- tactical preparations;
- propaganda;
- reconnaissance; and
- terrorist assaults.[201]

It appears that money plays a role in most, if not all, of the 11 stages of the cycle, not merely in the "financing" and "procurement" stages. Rudner considered the financing and procurement stages as among the most sensitive in a democratic context because of the intrusive legal measures usually required to investigate the activities involved.[202]

1.4.3.3.2 The Schmidt "Terrorist Resourcing Model"

John Schmidt of ITAC testified about a model he had developed of the TF process – the "Terrorist Resourcing Model."[203] Schmidt started developing the model while at FINTRAC, and eventually enhanced it with information gathered after he was seconded to ITAC.[204] It appears to be the only model of its kind,[205] and has been well received by both domestic and international partners.[206] Professor Rudner's model of a "terrorism operational cycle," discussed above, breaks "terrorism" into its functional and enabling activities, including financing and procurement; the Schmidt model focuses solely on TF.

---

198 Testimony of Martin Rudner, vol. 92, December 10, 2007, p. 12211.
199 Testimony of Martin Rudner, vol. 92, December 10, 2007, pp. 12211-12240.
200 Rudner Paper on Building Counter-Terrorism Capacity, pp. 114-125. Rudner's testimony and paper differ slightly in the description of the stages. The Commission is using the description of the stages from his testimony.
201 In his paper, Rudner uses the term "penetrating sensitive government departments, agencies and institutions" as the 9th of 12 steps.
202 Testimony of Martin Rudner, vol. 92, December 10, 2007, pp. 12232-12233.
203 The model was first explained to Commission counsel when Schmidt presented it at a seminar on TF issues in Montreal.
204 Testimony of John Schmidt, vol. 53, September 27, 2007, p. 6651.
205 Testimony of John Schmidt, vol. 53, September 27, 2007, pp. 6661-6662.
206 Testimony of John Schmidt, vol. 53, September 27, 2007, p. 6663.

Schmidt named his model the "Terrorist Resourcing Model" rather than the "Terrorist Financing Model" because, in his view, TF does not necessarily involve money. It can consist of an exchange of goods and, even if money is used, it may not reach the operating cell if it is exchanged before then for goods.[207]

Both classified and open-source information were used to build Schmidt's model, and it was reviewed by several experts before its description was published.[208] One goal of the model is to inform those working on TF matters,[209] and it may also help to identify gaps in efforts to counter TF.[210] ITAC and FINTRAC are cooperating to find ways to test the model.[211]

The model identifies five stages of TF. The stages need not always occur in the same order and may not be present in every case. They are summarized below:[212]

First Stage: Acquisition

Acquisition activities are fundraising activities. Acquisition can also consist of the direct contribution or receipt of goods or services – for example, weapons, vehicles, explosives or food.

Second Stage: Aggregation

This stage consists of pooling resources, either in a few financial institutions (for money) or in a few physical locations (for goods). In some cases, the aggregation stage is bypassed completely.

Third Stage: Transmission to a Terrorist Organization

Here, the funds or goods are moved. Schmidt testified that this stage often involves at least one international movement of the funds or goods. The movement might occur in several steps.

Fourth Stage: Transmission to a Terrorist Cell (Allocation or Disaggregation)

The terrorist organization allocates funds or goods to the appropriate cell in charge of a given activity. In the model, "activity" means much more than attacks, and includes matters such as direct support, propaganda, intelligence gathering, recruitment and radicalization. If funds are allocated rather than converted into goods, this will be the last stage of the process.

---

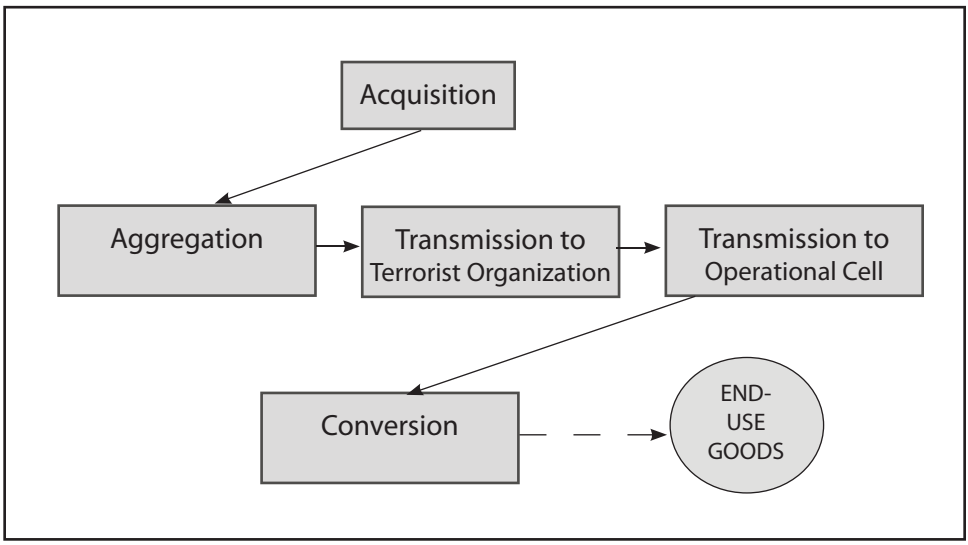
207 Testimony of John Schmidt, vol. 53, September 27, 2007, p. 6654. For consistency, this chapter continues to use the term "terrorist financing."
208 Testimony of John Schmidt, vol. 53, September 27, 2007, p. 6651.
209 Testimony of John Schmidt, vol. 53, September 27, 2007, pp. 6651-6652.
210 Testimony of John Schmidt, vol. 53, September 27, 2007, p. 6652.
211 Testimony of John Schmidt, vol. 53, September 27, 2007, p. 6661.
212 Testimony of John Schmidt, vol. 53, September 27, 2007, pp. 6657-6659.

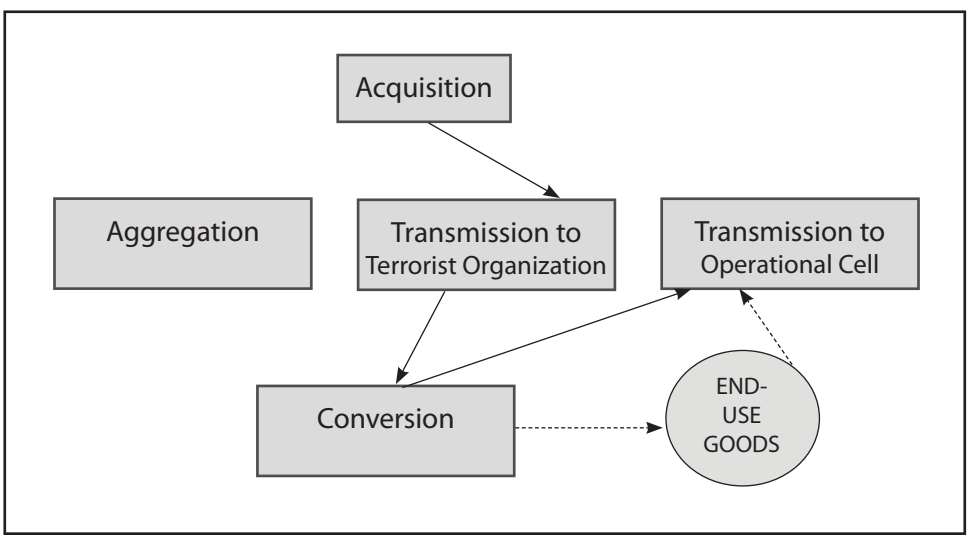
Fifth Stage: Conversion

This stage consists of exchanging funds or goods for end-use goods. For example, money may be used to buy a vehicle.[213]

1.4.3.3.3 Possible Sequences in the Terrorist Financing Process

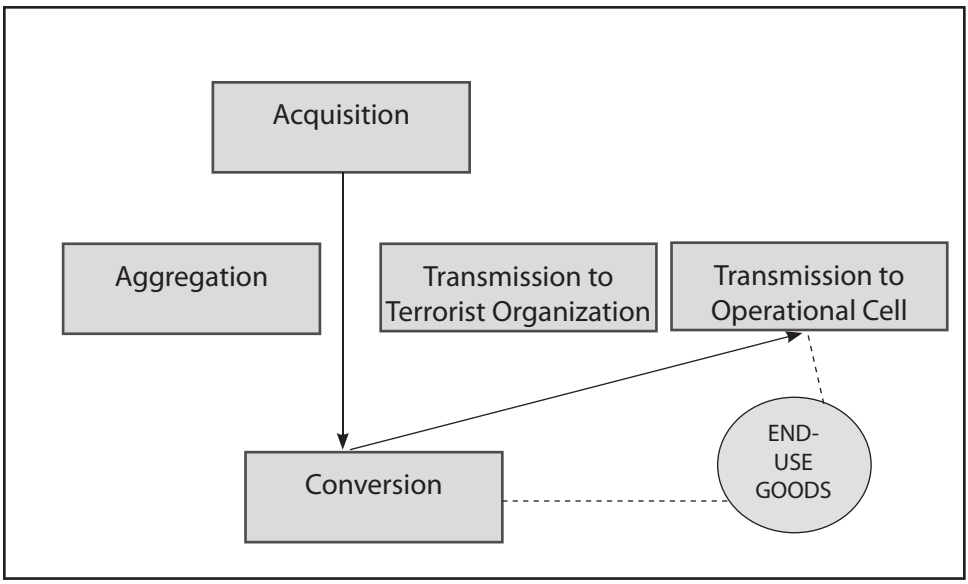
The order of the stages in Schmidt's model may vary and some stages may also be omitted. Below are examples of possible variations.[214]

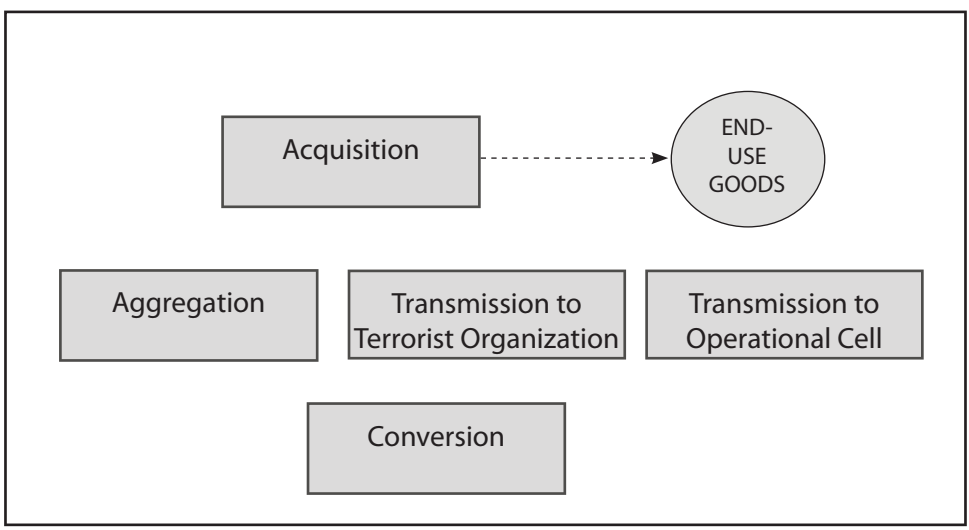




213 Testimony of John Schmidt, vol. 53, September 27, 2007, pp. 6657-6659.

214 Exhibit P-223, Tab 4: John Schmidt, "A Terrorist Financing/Resourcing Model," August 2007, pp. 18-21 [Schmidt Terrorist Financing Model].





1.4.3.3.4 Similarities between the Rudner and Schmidt Models

In Professor Rudner's model of a "terrorism operational cycle," which involved eleven stages, the fifth stage was "financing."[215] Financing involved the following:

215 Testimony of Martin Rudner, vol. 92, December 10, 2007, pp. 12211-12212.

- raising funds;
- remitting them to a safe place; and
- transferring them to their final destination.[216]

Rudner and Schmidt described the TF process in similar ways. Rudner spoke of raising funds, remitting them to a safe place and transferring them to their destination. Schmidt spoke of acquisition, aggregation and transmission.

1.4.3.4 Relationship between Terrorist Financing and Money Laundering

Up to this point, this chapter has discussed two models of how TF works in practice. It is also useful to understand the relationship between TF and money laundering to determine whether the techniques used to combat money laundering are suitable for pursuing TF.

1.4.3.4.1 Historically

The concept of money laundering was first introduced into the international community in the *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988*.[217] The Convention required parties to establish criminal offences relating to money laundering.

Immediately after 9/11, countries called for measures to fight TF. In an effort to respond quickly, the money laundering model was chosen.[218]

UN Security Council Resolution 1373 (2001) spoke of a connection between international terrorism and money laundering:

> [The Security Council] [n]otes with concern the close connection between *international terrorism* and transnational organized crime, illicit drugs, *money-laundering*, illegal arms-trafficking, and illegal movement of nuclear, chemical, biological and other potentially deadly materials, and in this regard *emphasizes* the need to enhance coordination of efforts on national, subregional, regional and international levels in order to strengthen a global response to this serious challenge and threat to international security."[219] [Emphasis added.]

Similarly, a 2006 ITAC intelligence assessment stated that "…[m]ost of the methods used by terrorist groups to 'process' their funds (that is, move them from the source to where they will be used) have also long been used by non-terrorist criminal groups to launder funds."[220]

---

216 Testimony of Martin Rudner, vol. 92, December 10, 2007, p. 12229.
217 Testimony of Keith Morrill, vol. 54, September 28, 2007, p. 6686.
218 Testimony of Nikos Passas, vol. 53, September 27, 2007, pp. 6568-6569.
219 S. 4, online: United Nations <http://daccessdds.un.org/doc/UNDOC/GEN/N01/557/43/PDF/N0155743.pdf?Open Element> (accessed February 13, 2009).
220 ITAC Intelligence Assessment on Terrorist Financing, para. 4.

The same international body, the FATF, oversees both anti-money laundering and anti-TF efforts. In October 2001, the FATF added special recommendations about TF to its existing recommendations about money laundering.[221]

As well, some of the techniques used to deter and detect money laundering operations (for example, those described in the FATF Forty Recommendations) have been applied by entities obliged to report to FINTRAC to combat TF.

The Department of Finance Memorandum of Evidence on Terrorist Financing states that, "…[t]o the extent that funds for financing terrorism are derived from illegal sources, the same anti-money laundering techniques and legal framework used to combat the financing of organized crime can be used to combat terrorist financing."[222] Professor Passas also testified that anti-money laundering methods can be effective in countering TF.[223] In addition, several officials and experts concluded that money can eventually be laundered in the TF process and that there is a convergence between the two activities.[224]

1.4.3.4.2 Differences between Money Laundering and Terrorist Financing

The main objectives of money laundering and TF differ. Money laundering generally involves organized criminal groups trying to disguise the origins of money obtained through crime.[225] The goal is to have the money appear "clean" so that it can be spent in the legal economy without drawing suspicion towards those spending it. In contrast, TF is not necessarily about laundering "dirty" money so that it can be spent in the legal economy.

Schmidt testified that money laundering and TF do "intersect" on many occasions and share many of the same techniques, but that TF is not the same as money laundering. As a result, the money laundering model does not effectively represent the TF process.[226]

TF may involve a complex web of activities that differ significantly from those used to launder money. Schmidt stated that, unlike TF, which generally occurs in five stages, money laundering occurs in three main stages – placement, layering

---

221 The FATF's Nine Special Recommendations on TF must be read in conjuncture with The Forty Recommendations to adequately understand the whole regime: "The revised Forty Recommendations now apply not only to money laundering but also to terrorist financing, and when combined with the Eight [now Nine] Special Recommendations, they provide a set of enhanced measures that will help countries to prevent terrorism.": Financial Action Task Force on Money Laundering, Annual Report 2002-2003, June 20, 2003, para. 20, online: Financial Action Task Force <http://www.fatf-gafi.org/dataoecd/13/0/34328221.pdf> (accessed February 18, 2009). See also Koh, *Suppressing Terrorist Financing and Money Laundering*, p. 125.

222 Department of Finance Memorandum of Evidence on Terrorist Financing, para. 2.3.

223 Testimony of Nikos Passas, vol. 53, September 27, 2007, p. 6575.

224 Testimony of John Schmidt, vol. 53, September 27, 2007, p. 6654; Schmidt Terrorist Financing Model; Testimony of Mark Potter, vol. 56, October 2, 2007, p. 7008; Department of Finance Memorandum of Evidence on Terrorist Financing, para. 2.5; Testimony of Nikos Passas, vol. 53, September 27, 2007, p. 6574.

225 Testimony of Keith Morrill, vol. 54, September 28, 2007, pp. 6685-6687.

226 Testimony of John Schmidt, vol. 53, September 27, 2007, p. 6653.

and integration. The placement stage is basically the movement of funds (the proceeds of crime) into banking or related systems. The layering stage is the "cover" stage, where the individual or organization tries to move the proceeds of crime, in whatever form they take at that point, to distance the funds from their origins. This second stage is often characterized by numerous movements of the funds. The third stage, integration, occurs when the funds are integrated into the legitimate marketplace.[227]

The money laundering model puts great emphasis on the "placement" stage (the movement of criminal proceeds into the financial system),[228] which is not the case in most TF activities, where the focus is more on how funds are transmitted to terrorists.

Detective Inspector Paul Newham, Deputy Head of the National Terrorist Financial Investigations Unit of the Metropolitan Police Service in the UK, testified that the TF and money laundering phenomena were very different in several ways:[229]

> With money laundering, you have a crime and then you have the proceeds of that crime flowing though a variety of sophisticated mechanisms. The situation you've described as placement, layering and then integration within the financial system to actually launder the money.
>
> In terms of terrorist financing, there is no predicate offence. This is – often there is no criminal money. It can be legitimate donations.
>
> Another distinction would be that in money laundering, you see large vast sums of money being moved in a variety of ways. In terms of terrorist financing, we see [in most cases] very small amounts or relatively small amounts compared to money laundering.
>
> So, in essence, the distinction with money laundering is we have a post-criminal act. In terms of terrorist financing, we have money, either a mixture of donations or potential low-level frauds, being used for an intended terrorist activity in the future which, again, brings its own problems when it comes to the actual prosecution of terrorist financing.[230]

---

227 Testimony of John Schmidt, vol. 53, September 27, 2007, p. 6652.
228 Testimony of John Schmidt, vol. 53, September 27, 2007, p. 6653.
229 Testimony of Paul Newham, vol. 58, October 4, 2007, p. 7232.
230 Testimony of Paul Newham, vol. 58, October 4, 2007, p. 7232.

As well, in money laundering operations, the money is "in hand" whereas in TF, the money must first be acquired.[231]

Keith Morrill of DFAIT stated that "…the impetus of the money laundering approach internationally" was recognition of the "huge" amounts of money involved.[232] Money laundering has been identified in Canada alone as "a multi-billion dollar problem."[233] The large sums known to be involved in money laundering cases – for example, laundering the proceeds of drug crimes – dwarf the amounts involved in financing even major terrorist attacks or in sustaining operating cells, or even larger organizations, such as Al Qaida. Techniques that might help to identify money laundering, such as a focus on cash transactions over $10,000, might completely miss many transactions related to TF.

1.4.4 The Need for an Anti-Terrorist Financing Program in Canada

Professor Passas asked this important question in his testimony:

> …[C]an terrorist finance be stopped? And it is more or less a rhetorical question. Unless you seriously disrupt legitimate trade or you have a police state, you can't do it.[234]

Like the crimes of murder or fraud, TF cannot be completely eradicated. RCMP Superintendent Reynolds testified, however, that authorities can try to make it more difficult.[235]

The alleged cost of the actual bombing of Air India flight 182 was under $10,000.[236] That excludes the cost of maintaining the organization and individuals involved in its planning and execution. Money was likely not a factor in the decision to proceed with the bombing. Still, several reasons have been advanced for Canada to have an anti-TF program.

1.4.4.1 The Reality of Terrorism

Canadians have their own interests at stake in international efforts to combat terrorism and terrorism financing.[237] In addition, as Keith Morrill of DFAIT testified, the international community would not go through the difficult process of adopting treaties and resolutions if an issue were not sufficiently serious.[238]

---

231 Schmidt Terrorist Financing Model, p. 7.
232 Testimony of Keith Morrill, vol. 54, September 28, 2007, p. 6690.
233 *Royal Canadian Mounted Police Departmental Performance Report for the period ending March 31, 2007*, p. 76, online: Treasury Board of Canada Secretariat <http://www.tbs-sct.gc.ca/dpr-rmr/2006-2007/inst/rcm/rcm-eng.pdf> (accessed May 13, 2009).
234 Testimony of Nikos Passas, vol. 53, September 27, 2007, p. 6567.
235 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6878.
236 Passas Paper on Terrorism Financing, p. 55.
237 Keith Morrill of DFAIT appeared to hold a similar view: Testimony of Keith Morrill, vol. 54, September 28, 2007, p. 6681.
238 Testimony of Keith Morrill, vol. 54, September 28, 2007, p. 6719.

RCMP Superintendent Reynolds testified that Canada had long been considered fertile ground for TF and for the procurement of terrorism-related materials, but it was not seen as a country from which terrorist attacks themselves were being launched. However, the situation has evolved.[239] Canada is not immune to direct terrorist attacks, and terrorist groups operate in Canada.[240]

The RCMP Departmental Performance Report for the period ending March 31, 2006 noted that, "…[i]f the RCMP is unable to address terrorist financing issues in an appropriate manner, Canadians and our allies would be in an environment of elevated risk."[241] Terrorist financiers could focus on Canada as an operating base, which could undermine the integrity of Canada's financial system[242] and its reputation abroad.[243] Failure to pursue TF might also put members of some communities at greater risk of being exploited.

1.4.4.2 Canada's International Obligations

Morrill testified that Canada has now signed several international instruments aimed at combatting TF, and that it must follow through domestically and internationally on its commitments.[244] Like many other countries, Canada is bound by UN Security Council Resolutions 1373 and 1267 and by the *International Convention for the Suppression of the Financing of Terrorism*. Morrill stated that Canada takes its international obligations "very, very seriously."[245]

Canada also is under strong pressure to honour the FATF Recommendations.[246] As a founding member, Canada committed itself to their implementation.[247] As well, Recommendation 26 requires member states to have a functioning FIU, and Special Recommendations I and II require ratifying and implementing the Convention and criminalizing TF.

Countries that do not follow the "40+9" Recommendations face the real possibility of being blacklisted by the FATF.[248] Until recently, the FATF maintained a list of countries identified as Non-Cooperative Countries and Territories (NCCT). In 2006, the FATF introduced a new surveillance process – the International Co-

---

239 Testimony of Rick Reynolds, vol. 55, October 1, 2007, pp. 6826-6827.
240 Testimony of Rick Reynolds, vol. 55, October 1, 2007, pp. 6828-6829.
241 *Royal Canadian Mounted Police Departmental Performance Report for the period ending March 31, 2006*, p. 62, online: Treasury Board of Canada Secretariat <http://www.tbs-sct.gc.ca/dpr-rmr/2005-2006/rcmp-grc/rcmp-grc-eng.pdf> (accessed May 13, 2009) [2005-06 RCMP Departmental Performance Report].
242 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6773; 2005-06 RCMP Departmental Performance Report, p. 62.
243 One can imagine the outcry if a terrorist attack occurring elsewhere were financed from Canada while Canada had failed to put TF measures in place. Keith Morrill believed Canada would hear criticism from the international community if it were not meeting its commitments in this regard: Testimony of Keith Morrill, vol. 54, September 28, 2007, p. 6721.
244 Testimony of Keith Morrill, vol. 54, September 28, 2007, pp. 6697-6698.
245 Testimony of Keith Morrill, vol. 54, September 28, 2007, p. 6711.
246 Testimony of Keith Morrill, vol. 54, September 28, 2007, pp. 6701-6702.
247 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6767.
248 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6774.

operation Review Group – "to identify, examine and engage with vulnerable jurisdictions that are failing to implement effective AML/CFT systems."[249]

1.4.4.3 Role of Anti-Terrorist Financing Efforts in Combatting Terrorism

John Schmidt of ITAC testified that financial intelligence was a useful component of the fight against terrorism as a whole: "...[T]he financial intelligence can and does go a long way to help identify criminal or terrorist networks and relationships and is very important in the overall process.…[U]nderstanding terrorist resourcing goes a long way to helping us understand, anticipate, the overall terrorist activity; how they work together, how their networks operate and…the [change] that is going on in the nature of many terrorist organizations and their activities."[250]

Financial intelligence can often help law enforcement and related agencies understand the networks and relationships much better than can other sources of information.[251] Terrorism financing prosecutions have the potential to disrupt groups that may be accumulating funds for terrorist purposes but have not yet decided to commit any terrorist act.

In his testimony, Passas gave several reasons why financial controls were a vital part of all counterterrorism efforts:

- If the would-be terrorists have less money, the harm might be reduced. Passas cited the example of those involved in the first World Trade Centre attacks who complained that they didn't have more than $19,000 to pack explosives into the rental truck that they exploded in the parking garage: "They didn't have more money so when you limit the resources the harm is reduced";
- The intelligence that can be gathered in anti-TF operations is essential to make links and reconstruct events: "Monitoring what the militant groups are doing is much more important than seizing and freezing their assets"; and
- If terrorists believe that they are being tracked, it forces them to "… speak to each other, to communicate, to change methods, to move things around, to move to low-tech hand-carried kinds of options, and that generates additional intelligence-gathering opportunities."[252]

Passas warned, however, that controls may produce negative results. Among his examples were the following:

---

249 FATF Revised Mandate 2008-2012, para. 8.
250 Testimony of John Schmidt, vol. 53, September 27, 2007, pp. 6660-6662.
251 Testimony of John Schmidt, vol. 53, September 27, 2007, pp. 6663-6664.
252 Testimony of Nikos Passas, vol. 53, September 27, 2007, p. 6623.

- The controls may drive terrorists networks underground and create organizations that are more difficult to monitor and detect;
- Innocent parties could suffer "significant collateral damage";
- Legitimate trade could be disrupted;
- Ethnic groups that otherwise would serve as allies in counterterrorism matters might be alienated; and
- Other countries that are forced to implement measures that they do not support may simply pass laws that are not enforced. This "window dressing" would give the appearance of progress even though none was occurring.[253]

Detective Inspector Newham of the Metropolitan Police Service in the UK estimated in his testimony that there was more information and intelligence on individuals within the financial systems of developed Western economies than in any other database.[254] He spoke of the value of this information:

> It's one of the tools where we can quickly locate individuals; we can quickly identify trouble patterns; we can identify spending, procurement activity associations, and we use a number of covert and overt techniques to actually model behaviours of individuals and what connectivity they have, again, abroad.[255]

1.5 Conclusion

It is impossible to obtain a clear picture of the extent of TF. It is clear, however, that the TF phenomenon is complex. TF can take on innumerable forms[256] and can span many borders.

Several witnesses spoke of the importance in combatting terrorism of the financial intelligence acquired through anti-TF programs. Fighting TF can generate leads and serve as an investigative or intelligence-gathering tool. Anti-TF efforts are therefore one element of a larger process: preventing terrorist incidents.

---

253 Testimony of Nikos Passas, vol. 53, September 27, 2007, pp. 6623-6624.

254 Testimony of Paul Newham, vol. 58, October 4, 2007, p. 7228. The Egmont Group also stated that "… [i]t became apparent over the years that banks and other financial institutions were an important source for information about money laundering and other financial crimes being investigated by law enforcement.": "Financial Intelligence Units (FIUs)," online: The Egmont Group <http://www.egmontgroup.org/about_egmont.pdf> (accessed February 20, 2009).

255 Testimony of Paul Newham, vol. 58, October 4, 2007, p. 7238.

256 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6842, agreeing with a description by the Commissioner.

VOLUME FIVE
TERRORIST FINANCING

CHAPTER II: CANADIAN LEGISLATION GOVERNING TERRORIST FINANCING

2.1 Introduction

Canadian legislation relating to TF consists of criminal and regulatory provisions. In a paper prepared for the Commission, Professor Anita Anand summarized the current Canadian legislative framework dealing with TF:

> Although anti-terrorist financing law did not exist in 1985 when Air India Flight 182 was bombed, today's legal regime appears to be comprehensive.… These legislative initiatives cover significant regulatory ground in terms of substantive law, and, generally speaking, they also accord with private and public international law on terrorist financing.[1]

2.2 The *Anti-terrorism Act* (*ATA*)

Within a few months of the events of September 11, 2001, Canada followed the example of several other countries and enacted anti-terrorism legislation – in Canada's case, the *Anti-terrorism Act*[2] (*ATA*). Parliament included several TF offences in the *ATA*, to comply with the *Financing of Terrorism Convention* and UN Security Council Resolution 1373. The *ATA* also introduced various means to combat TF.

In its Memorandum of Evidence on Terrorist Financing, the Department of Finance described the *ATA* as "…designed to strengthen the ability to identify, prosecute and convict terrorists, in part by providing new investigative tools to law enforcement and national security agencies."[3] The *ATA* amended the following acts:

- the *Criminal Code*;[4]

---

1 Anita Indira Anand, "An Assessment of the Legal Regime Governing the Financing of Terrorist Activities in Canada" in Vol. 2 of Research Studies: Terrorism Financing Charities and Aviation Security, p. 121 [Anand Paper on Legal Regime Governing Terrorist Financing].

2 S.C. 2001, c. 41.

3 Exhibit P-227, Tab 3: Department of Finance Memorandum of Evidence on Terrorist Financing, February 28, 2007, para. 1.6 [Department of Finance Memorandum of Evidence on Terrorist Financing].

4 R.S.C. 1985, c. C-46.

- the *Proceeds of Crime (Money Laundering) Act*, and renaming it *the Proceeds of Crime (Money Laundering) and Terrorist Financing Act*[5] (*PCMLTFA*);
- the *Security of Information Act*;[6]
- the *Canada Evidence Act*;[7] and
- the *National Defence Act*.[8]

The *ATA* also created the *Charities Registration (Security Information) Act*[9] (*CRSIA*).

The *ATA* introduced three TF offences into the *Criminal Code*. They cover (i) providing or collecting property for certain activities, including terrorist activities, (ii) providing property or services for terrorist purposes, and (iii) using or possessing property for terrorist purposes. The full text of these offences reads as follows:

Providing or collecting property for certain activities

Section 83.02 Every one who, directly or indirectly, wilfully and without lawful justification or excuse, provides or collects property intending that it be used or knowing that it will be used, in whole or in part, in order to carry out

> (a) an act or omission that constitutes an offence referred to in subparagraphs (a)(i) to (ix) of the definition of "terrorist activity" in subsection 83.01(1),[10] or
>
> (b) any other act or omission intended to cause death or serious bodily harm to a civilian or to any other person not taking an active part in the hostilities in a situation of armed conflict, if the purpose of that act or omission, by its nature or context, is to intimidate the public, or to compel a government or an international organization to do or refrain from doing any act,

is guilty of an indictable offence and is liable to imprisonment for a term of not more than 10 years.

---

5 S.C. 2000, c. 17.
6 R.S.C. 1985, c. O-5, which replaced the *Officials Secret Act*.
7 R.S.C. 1985, c. C-5.
8 R.S.C. 1985, c. N-5.
9 S.C. 2001, c. 41, s. 113. The Act was created by the *Anti-terrorism Act*.
10 These subparagraphs contain references to various treaties and the related offences under the *Criminal Code* that give effect to the treaties in Canadian domestic law. For example, offences under s. 7(2) implement the *Convention for the Suppression of Unlawful Seizure of Aircraft*. See the earlier section on the Canadian definition of "terrorism."

Providing, making available, etc., property or services for terrorist purposes

Section 83.03 Every one who, directly or indirectly, collects property, provides or invites a person to provide, or makes available property or financial or other related services

> (a) intending that they be used, or knowing that they will be used, in whole or in part, for the purpose of facilitating or carrying out any terrorist activity, or for the purpose of benefiting any person who is facilitating or carrying out such an activity, or
>
> (b) knowing that, in whole or part, they will be used by or will benefit a terrorist group,

is guilty of an indictable offence and is liable to imprisonment for a term of not more than 10 years.

Using or possessing property for terrorist purposes

Section 83.04 Every one who

> (a) uses property, directly or indirectly, in whole or in part, for the purpose of facilitating or carrying out a terrorist activity, or
>
> (b) possesses property intending that it be used 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,

is guilty of an indictable offence and is liable to imprisonment for a term of not more than 10 years.

Sections 83.18 and 83.19 of the *Criminal Code* create offences for participating in or contributing to the activities of a terrorist group to facilitate terrorist activity. Section 83.2 makes it an offence under the *Criminal Code* to commit an indictable offence under any Act of Parliament for a terrorist group, and section 83.21 creates an offence for instructing any person to carry out activities in support of a terrorist group. TF activities may violate these provisions.

The *ATA* also created a process in the *Criminal Code* for designating ("listing") entities that, once listed, are considered "terrorist groups" under the Code. The listing process and related Code provisions are discussed more fully below.

Besides renaming the *Proceeds of Crime (Money Laundering) Act* as the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (*PCMLTFA*), the *ATA* amended the act to give the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) the added mandate to collect and analyze financial data relating to TF. The *PCMLTFA* is now the central law in combatting TF in Canada. Its main provisions are explored later in this volume as they apply to FINTRAC and other agencies. The 2008 FINTRAC Annual Report summarizes the general thrust and evolution of the *PCMLTFA*:

> This statute establishes FINTRAC to collect, analyze, assess and disclose financial information with respect to money laundering and terrorist activity financing. Other parts of the Act require financial institutions and intermediaries to take prescribed customer due diligence, record keeping, transaction reporting and compliance program requirements and establish Canada's cross-border currency reporting system. Originally enacted as the *Proceeds of Crime (Money Laundering) Act* in June 2000, it was amended in December 2001, to add combating terrorist activity financing to FINTRAC's mandate. In December 2006, the Act was substantially amended to bring it in line with international standards by expanding its coverage, strengthening its deterrence provisions and broadening the range of information that FINTRAC may include in its financial intelligence disclosures.[11]

In her paper, Professor Anand explained the relationship between the *Criminal Code* provisions and those under the *PCMLTFA*:

> While the *Criminal Code* addresses a variety of activities that relate to terrorist financing (from providing property, to assist in terrorist financing, to money laundering) and criminalizes such activity, the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* deals with reporting requirements, cross-border movement of currency, and the creation of an agency to administer the Act.[12]

When the *ATA* created the *Charities Registration (Security Information) Act* (*CRSIA*), the purpose was to allow the use of secret evidence in decisions to deny or revoke charitable status in order to reduce the possibility of groups using their charitable status to facilitate TF.[13]

---

11 Financial Transactions and Reports Analysis Centre of Canada, *FINTRAC 2008 Annual Report*, p. 26, online: Financial Transactions and Reports Analysis Centre of Canada <http://www.fintrac.gc.ca/publications/ar/2008/ar-eng.pdf> (accessed May 13, 2009).

12 Anand Paper on Legal Regime Governing Terrorist Financing, p. 127.

13 The *CRSIA* is discussed in greater detail in Chapter VI.

Section 145 of the *ATA* requires a comprehensive review of the *ATA* within three years of the Act receiving Royal Assent, which occurred on December 18, 2001.[14] The PCMLTFA requires a review of that Act every five years.[15]

2.3 Bill C-25

On December 14, 2006, Bill C-25 received Royal Assent, becoming *An Act to amend the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and the Income Tax Act and to make a consequential amendment to another Act*.[16] The Department of Finance Memorandum of Evidence on Terrorist Financing stated that the Act would "…bring Canada's regime in line with FATF international standards, responding to changing domestic risks and addressing the recommendations of the Auditor General of Canada, Treasury Board and the Standing Senate Committee on Banking, Trade and Commerce."[17]

Bill C-25 created a registration requirement for money services businesses.[18] It strengthened the identification requirements for wire transfers.[19] It also strengthened the regime to confront the misuse of charitable organizations for TF purposes by providing authority to the Canada Revenue Agency (CRA) to disclose more extensive information to CSIS, the RCMP and FINTRAC.[20]

Bill C-25 amended the *PCMLTFA* to allow FINTRAC, when certain conditions are met, to disclose information to the CRA for purposes related to determining charitable status.[21] It added to the *PCMLTFA* the obligation for a reporting entity to report an "attempted" transaction where the entity suspects that the attempt was related to the commission or attempted commission of a money

---

14 See also House of Commons Canada, Final Report of the Standing Committee on Public Safety and National Security, Subcommittee on the Review of the *Anti-terrorism Act, Rights, Limits, Security: A Comprehensive Review of the Anti-terrorism Act and Related Issues*, March 2007, online: Parliament of Canada <http://www2.parl.gc.ca/content/hoc/Committee/391/SECU/Reports/RP2798914/sterrp07/sterrp07-e.pdf> (accessed May 25, 2009); The Senate of Canada, *Fundamental Justice in Extraordinary Times: Main Report of the Special Senate Committee on the Anti-terrorism Act*, February 2007, online: Parliament of Canada <http://www.parl.gc.ca/39/1/parlbus/commbus/senate/Com-e/anti-e/rep-e/rep02feb07-e.pdf> (accessed February 17, 2009).

15 *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, S.C. 2000, c. 17, s. 72 [*PCMLTFA*].

16 S.C. 2006, c. 12. Even though Bill C-25 has received Royal Assent, and thus has officially become a law, it is commonly referred to as Bill C-25 and not by it proper name, *An Act to amend the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and the Income Tax Act and to make a consequential amendment to another Act*.

17 Department of Finance Memorandum of Evidence on Terrorist Financing, para. 1.9.

18 A money services business is defined as "a person or entity that is engaged in the business of remitting funds or transmitting funds by any means or through any person, entity or electronic funds transfer network, or of issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments. It includes a financial entity when it carries out one of those activities with a person or entity that is not an account holder.": Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, S.O.R./2002-184), s. 1; *Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations*, S.O.R./2001-317), s. 1.

19 Bill C-25, s. 8, adding s. 9.5 to the *PCMLTFA*.

20 Bill C-25, s. 45.

21 Bill C-25, s. 26(4), introducing s. 55(3)(c) to the PCMLTFA.

laundering or terrorist activity financing offence.[22] Bill C-25 also required the Privacy Commissioner of Canada to review the measures taken by FINTRAC to protect the privacy of the information it receives or collects under the *PCMLTFA*. This review is to occur every two years.[23]

Later chapters explore in greater detail the changes that Bill C-25 brought to Canada's anti-TF program.

The changes brought by Bill C-25 came into force progressively. The Act was fully in force in December 2008, and further changes can occur through regulation. For example, Bill C-25 introduced the concept of "politically exposed persons" to the *PCMLTFA*,[24] and the concept may be further defined by regulation.

2.4 The Listing Processes

2.4.1 The *United Nations Al-Qaida and Taliban Regulations* (UNAQTR)[25]

UN Security Council Resolution 1267 established the Al-Qaida and Taliban Sanctions Committee (the "1267 Committee"[26]) and made it responsible for designating individuals associated or involved with the Taliban, Al-Qaida and associates of Usama bin Laden. Bin Laden was also designated. The main purpose of putting individuals on the Committee's list was to facilitate the freezing of money and property used for terrorism purposes:

---

22 Bill C-25, s. 5, replacing s. 7 of the *PCMLTFA*.

23 Bill C-25, s. 38, replacing s. 72(2) of the *PCMLTFA*. For comments on the *PCMLTFA* from a privacy standpoint, see the submission by Jennifer Stoddart, Privacy Commissioner of Canada, to the Standing Senate Committee on Banking, Trade and Commerce, June 21, 2006, online: Office of the Privacy Commissioner of Canada <http://www.privcom.gc.ca/information/pub/sub_ml_060621_e.asp> (accessed February 18, 2009). For the Privacy Commissioner's comments specifically on Bill C-25, see her opening statement and submission to the Standing Senate Committee on Banking, Trade and Commerce, December 13, 2006, online: Office of the Privacy Commissioner of Canada <http://www.privcom.gc.ca/parl/2006/parl_061213_e.asp> and <http://www.privcom.gc.ca/parl/2006/sub_061213_e.asp> (accessed February 18, 2009).

24 Bill C-25, s. 8, introducing s. 9.3(3) to the *PCMLTFA*. A politically exposed person is defined as "…a person who holds or has held one of the following offices or positions in or on behalf of a foreign state: (a) head of state or head of government; (b) member of the executive council of government or member of a legislature; (c) deputy minister or equivalent rank; (d) ambassador or attaché or counsellor of an ambassador; (e) military officer with a rank of general or above; (f) president of a state-owned company or a state-owned bank; (g) head of a government agency; (h) judge; (i) leader or president of a political party represented in a legislature; or (j) holder of any prescribed office or position. It includes any prescribed family member of such a person."

25 Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (Ottawa: Public Works and Government Services Canada, 2006) [*A New Review Mechanism for the RCMP's National Security Activities*] describes these regulations as the *United Nations Afghanistan Regulations*: p. 238, note 411. The Regulations themselves use both names. The title of the Regulations is *United Nations Al-Qaida and Taliban Regulations*. The preamble to the Regulations states, "Her Excellency the Governor General in Council . . . hereby makes the annexed *United Nations Afghanistan Regulations*." For consistency, this volume refers to the regulations as the *United Nations Al-Qaida and Taliban Regulations* and uses the acronym UNAQTR.

26 Also known as the "Al-Qaida and Taliban Sanctions Committee": see online: United Nations <http://www.un.org/sc/committees/1267/information.shtml> (accessed February 17, 2009).

> The 1267 Committee lists entities and individuals upon the request of a member state. Therefore, an individual or entity listed as a terrorist by the United Nations may have their assets seized or frozen in any or all UN member states that incorporate the listings into their domestic laws.[27]

> The 1267 Committee advises states to submit names as soon as they gather the supporting evidence of association with Al-Qaida and/or the Taliban. A criminal charge or conviction is not necessary for inclusion on the 1267 list as the sanctions are intended to be preventive in nature.[28]

Canada has incorporated the listing process under Resolution 1267 into Canadian law by way of the *United Nations Al-Qaida and Taliban Regulations* (UNAQTR),[29] made under the *United Nations Act*.[30] Any individual or entity added to the 1267 list by the 1267 Committee is automatically subject to the provisions of Canada's UNAQTR.[31]

Among other restrictions, sections 3, 4 and 5 of the UNAQTR prohibit any person in Canada or any Canadian outside Canada from dealing with property or providing financial services to the Taliban, Usama bin Laden or any of their associates, as designated by the 1267 list.

Section 5.1 provides that specific Canadian entities,[32] including banks, trust companies and insurance companies, have a "duty to determine" on a continuing basis whether they are in possession of, or in control of, money or property that belongs to the Taliban, Usama bin Laden or any of their associates. The entities must report periodically to their regulators whether or not they are in possession of such property.

Section 5.2 imposes a "duty to disclose." Every person in Canada and every Canadian outside Canada must disclose to the Commissioner of the RCMP and to the Director of CSIS the existence of property in their possession or control that they have reason to believe is owned or controlled by, or on behalf of, the Taliban, a person associated with the Taliban, Usama bin Laden or his associates.

---

27 *A New Review Mechanism for the RCMP's National Security Activities*, pp. 192-193.

28 Exhibit P-383, Tab 1: DFAIT Modifications to *A New Review Mechanism for the RCMP's National Security Activities.*

29 S.O.R./99-444.

30 R.S.C. 1985, c. U-2.

31 *Response of the Government of Canada to the Final Report of the Standing Committee on Public Safety and National Security, Subcommittee on the Review of the Ant-terrorism Act, Rights, Limits, Security: A Comprehensive Review of the Anti-terrorism Act and Related Issues*, pp. 9-10, online: Parliament of Canada <http://cmte.parl.gc.ca/Content/HOC/committee/391/secu/govresponse/rp3066235/391_SECU_Rpt07_GR/391_SECU_Rpt07_GR-e.pdf> (accessed May 25, 2009) [Canada Response to House of Commons Report on the *ATA*].

32 S. 5.1(1) indicates that the entities are those referred to in ss. 83.11(1)(a) to (g) of the *Criminal Code*.

They must also disclose information about any transaction or proposed transaction in respect of that property.

The Minister of Foreign Affairs is the Minister responsible for the UNAQTR,[33] while the 1267 Committee is responsible for the actual listing.

The UNAQTR also allow individuals to petition the Minister of Foreign Affairs to be removed from the list.[34] The delisting process may involve Canada making representations to the 1267 Committee.

2.4.2 *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism* (RIUNRST)

A second listing process was established under UN Security Council Resolution 1373. It was incorporated into Canadian law by the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism* (RIUNRST)[35] under the *United Nations Act*.

Resolution 1373 created a framework for each country to develop its own list. This list is not "…restricted in geographic and affiliative [*sic*] scope as are the UNAQTR."[36] In essence, Resolution 1373 provides that countries must criminalize persons who wilfully commit TF, and allow for the quick freezing of the following:

> …funds and other financial assets or economic resources of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds derived or generated from property owned or controlled directly or indirectly by such persons and associated persons and entities.[37]

The response of the Government of Canada to a 2007 review of the *ATA* observed that, in the absence of an international consensus as to the identification or designation of the entities involved, the Security Council left the decision as to which entities should be listed to member states.[38] This was because there was often no consensus about whether a group was a terrorist group. The LTTE is one example. Canada did not list it until 2006, several years later than some other countries.

---

33 No specific provision in the UNAQTR states this, but the Minister of Foreign Affairs is the only minister mentioned in the regulations.
34 S.O.R./99-444, s. 5.3(1).
35 S.O.R./2001-360.
36 Canada Response to House of Commons Report on the *ATA*, p. 10.
37 S. 1(c), online: United Nations <http://daccessdds.un.org/doc/UNDOC/GEN/N01/557/43/PDF/N0155743.pdf?Open Element> (accessed February 13, 2009).
38 Canada Response to House of Commons Report on the *ATA*, p. 10.

Each country designates entities for listing under Resolution 1373 (for instance, by way of the RIUNRST in Canada). Peer pressure among countries often leads recalcitrant countries to list certain entities. Under the RIUNRST, the Governor in Council may, on the recommendation of the Minister of Foreign Affairs, list an individual or an entity if the Governor in Council is satisfied that there are reasonable grounds to believe that they may have been involved in certain terrorist activities specified in the RIUNRST.[39] The Department of Foreign Affairs and International Trade (DFAIT) is the lead department in the RIUNRST listing process.

The consequences of listing consist primarily of the freezing of assets and a prohibition on fundraising.[40] Sections 3 and 4 of the RIUNRST impose requirements to freeze assets similar to requirements in the UNAQTR. Among other restrictions, the RIUNRST prohibit any person in Canada and any Canadian outside Canada from dealing with property or providing financial services to a listed person. Also, like the UNAQTR, the RIUNRST impose a "duty to determine" (section 7) and a "duty to disclose" (section 8).[41] In short, these provisions in the RIUNRST operate in a way that is almost identical to these provisions of the UNAQTR.

2.4.3. *Criminal Code* Listing Process

The *ATA* introduced a third, exclusively Canadian, listing process – in this case, through the *Criminal Code*. This third listing process is considered to fulfill an important part of Canada's obligation to implement both Security Council Resolution 1373 and the *Convention on the Suppression of Terrorism Financing*. The *Criminal Code* provides for consequences beyond freezing assets and prohibiting fundraising.

Section 83.05 of the *Criminal Code* provides for the Governor in Council to create a list of entities on the recommendation of the Minister of Public Safety[42] – rather than the Minister of Foreign Affairs, as is the case with the RIUNRST. For an entity to be included on the *Criminal Code* list, the Governor in Council must have reasonable grounds to believe that the entity "…has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity" or that the "…entity is knowingly acting on behalf of, at the direction of or in association with" such an entity.

---

39 S.O.R./2001-360, s. 2(1).

40 Canada Response to House of Commons Report on the *ATA*, p. 11.

41 An amendment to the *PCMLTFA* contained in Bill C-25 requires that a report also be provided to FINTRAC if the person or entity is subject to the *PCMLTFA*: see Bill C-25, s. 6, amending s. 7.1(1) of the *PCMLTFA*.

42 The Minister of Public Safety and Emergency Preparedness identified in the *Criminal Code* was renamed the Minister of Public Safety. The Department, Public Safety and Emergency Preparedness Canada (PSEPC), was renamed Public Safety Canada (PSC). All references to PSEPC in this document should be read as a reference to Public Safety Canada (PS). Prior to this change, PSEPC had incorporated the "core activities of the former Department of the Solicitor General of Canada with those of the Office of Critical Infrastructure Protection and Emergency Preparedness, and the National Crime Prevention Centre": Public Safety and Emergency Preparedness Canada, *Report on Plans and Priorities 2004-2005*, online: Public Safety Canada <http://ww2.ps-sp.gc.ca/publications/corporate/rpp_2004_e.asp> (accessed February 18, 2009).

The Government of Canada states that "…the *Criminal Code* listing regime carries a higher standard, that is, the belief that the subject has knowingly been involved in a terrorist activity or acted on behalf of a terrorist entity. In contrast, the standard for the RIUNRST mechanism is based on the requirements of Resolution 1373."[43]

Section 83.01(1) of the *Criminal Code* defines the term "listed entity" as "…an entity on a list established by the Governor in Council under section 83.05." Section 83.01(1) defines "terrorist group" to include a listed entity. Hence, an entity listed under section 83.05 is by definition a terrorist group under the *Criminal Code*. There were 41 listed groups as of February 2009.[44] These definitions help Canadian prosecutors since they do not have to prove independently that the entity is a terrorist group. If the entity is listed under the *Criminal Code* listing process, the entity is considered a terrorist group.

Section 83.08 forbids any person in Canada, and any Canadian anywhere, from knowingly dealing with property or providing financial or other related services to terrorist groups. Offenders face a fine, incarceration, or both. Section 83.11 requires a number of reporting entities to determine on a continuing basis whether they are in possession of such property. The entities must make monthly reports to their supervisory agencies – for example, the Office of the Superintendent of Financial Institutions (OSFI). The reporting entities described in section 83.11 have similar reporting obligations under the *PCMLTFA* (the obligations under the *PCMLTFA* are examined in Chapter III). The main difference between the reporting obligations imposed under the *PCMLTFA* and those imposed by section 83.11 of the *Criminal Code* is that the *Criminal Code* obligations apply mainly to institutions taking deposits.

Section 83.1 also creates an obligation for every person in Canada to disclose to the Commissioner of the RCMP and to the Director of CSIS the existence of property in their possession that they know is owned or controlled by or for a terrorist group. In addition, every person or entity obliged to make a disclosure under section 83.1 must also report to FINTRAC if that person or entity is also subject to the *PCMLTFA*.[45]

To ensure compliance with the *Charter*,[46] the Code provides procedures for listed entities to apply to be de-listed. Under section 83.05(2) of the Code, the entity can request the Minister of Public Safety to consider recommending de-listing within 60 days. A similar process is available under section 83.07 in cases of mistaken identity. Under section 83.06, the entity can seek judicial review of the listing, albeit in a manner that allows the judge to consider intelligence that is not disclosed to the entity on the grounds that disclosure would injure national security or endanger the safety of other people.[47] The *Criminal Code*

43 Canada Response to House of Commons Report on the *ATA*, p. 12.
44 *Regulations Establishing a List of Entities*, SOR/2002-284.
45 *PCMLTFA*, s. 7.1.
46 *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11.
47 Security-cleared special advocates might play a useful role in such proceedings. They could challenge the intelligence used to support the listing while not risking the further disclosure of the intelligence, some of which might have been shared with Canada by allies on condition that it not be disclosed.

also requires that the Minister of Public Safety review the list every two years.[48]

The following chart, prepared by Public Safety Canada, illustrates the process for listing entities under the *Criminal Code* listing scheme:[49]

Procedure For Listing Entities Under the *Criminal Code*

Identification of Case

- CSIC or RCMP identifies, develops, evaluates, and assesses the case of listing.

Consultation

- CSIC and the RCMP to consult and share information to the extent possible related to potential listing.

Preparation of Security Intelligence Report (SIR)

- CSIS and RCMP internal approval, including internal legal review.
- Independent legal verification or case by Department of Justice.
- SIR prepared for sign off by the Director, CSIS or the Commissioner of the RCMP.
- Following sign off, SIR delivered to Deputy Minister (DM) of Public Safety

Notification of Interdepartmental Community

- DM of Public Safety convenes meeting of DM -level interdepartmental coordinating committee on listings.
- DMs are provided with copies of the Explanatory Note, identification of the entity and aliases, and the proposed web page summary.

Advising the Minister of Public Safety

- Department of Public Safety advances the SIR and other relevant documents of the Minister.
- Minister of Public Safety decides whether to make a recommendation to the Governor in Council (GIC)

GIC Decision

- Recommendation provided to the GIC
- GIC deliberates and approves/declines proposal for regulation to list the entity.
- Regulation is in force upon registration with PCO.
- Published in the Canada Gazette.

48 R.S.C. 1985, c. C-46, s. 83.05(9).

49 Exhibit P-383, Tab 11: Public Safety Canada's Submission to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, October 24, 2007, p. 3.

To help publicize the entities listed under the *Criminal Code*, RIUNRST and UNAQTR, the Office of the Superintendent of Financial Institutions regularly updates a consolidation of the lists on its website.[50]

Because countries develop their own listing processes in accordance with Resolution 1373, and possibly under their own domestic legislation (such as the *Criminal Code* listing process in Canada), listings among countries may not match, except for listings made under Security Council Resolution 1267.

2.5 Conclusion

Before 2001, like most other countries, Canada did not expressly prohibit TF. The 2001 *Anti-terrorism Act* introduced new crimes dealing with TF, a procedure for "listing" terrorist groups, new obligations to report financial transactions and provisions that allowed charities involved in terrorism to have their charitable status revoked or denied. These new provisions provide a weapon in combatting the complex phenomenon of TF and in ensuring that Canada complies with its international obligations to suppress TF. As subsequent chapters discuss, efforts against TF involve cooperation among many government agencies and private sector entities.

50 Online: Office of the Superintendent of Financial Institutions Canada <http://www.osfi-bsif.gc.ca/osfi/index_e.aspx?DetailID=525> (accessed February 17, 2009).

VOLUME FIVE
TERRORIST FINANCING

CHAPTER III: THE ROLES OF FEDERAL DEPARTMENTS AND AGENCIES IN EFFORTS TO SUPPRESS TERRORIST FINANCING

Many federal departments and agencies[1] are involved in national security matters:

- Canada Border Services Agency (CBSA);
- Canada Revenue Agency (CRA);
- Canadian Security Intelligence Service (CSIS);
- Communications Security Establishment (CSE)[2];
- Department of Finance (Finance Canada);
- Financial Transactions and Reports Analysis Centre of Canada (FINTRAC);
- Department of Fisheries and Oceans/Canadian Coast Guard;
- Department of Foreign Affairs and International Trade (DFAIT);
- Department of Justice (DOJ);
- Department of National Defence (DND) and the Canadian Forces (CF);
- Integrated Threat Assessment Centre (ITAC);
- Office of the Superintendent of Financial Institutions (OSFI);
- Privy Council Office (PCO);
- Public Safety Canada (PS); and
- Royal Canadian Mounted Police (RCMP).[3]

The focus of this chapter is on the roles of many of these agencies in attempts to suppress terrorist financing (TF). The role of the Canada Revenue Agency (CRA) is examined separately in Chapter VI.

---

1 To simplify the narrative in this chapter, the terms "department" and "agency" are used interchangeably. The use of one term includes the other where the context requires.

2 The official acronym is now CSEC, but the acronym CSE is still commonly used.

3 The agencies are not necessarily listed in order of the importance of their role in TF matters. Other documents and reports describe the inner workings of these agencies; see, for example, the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (Ottawa: Public Works and Government Services Canada, 2006) [*A New Review Mechanism for the RCMP's National Security Activities*].

3.1 The Department of Finance (Finance Canada)

Finance Canada is the lead department in the federal government's overall initiative to combat money laundering (ML) and TF.[4] It was placed in charge of the National Initiative to Combat Money Laundering in 2000, and remained at the helm when the Initiative was renamed the Anti-money Laundering and Anti-terrorist Financing Initiative (AML/ATF Initiative) after the enactment of the *Anti-terrorism Act*[5](ATA) in 2001. Two sections of Finance – Financial Crimes Domestic and Financial Crimes International – are responsible for money laundering and TF matters. Both sections are located in the Financial Sector Division of Finance.[6]

The Minister of Finance is responsible to Parliament for FINTRAC and for the Office of the Superintendent of Financial Institutions (OSFI).[7]

Canada is not unique in having a department such as Finance Canada in a lead policy and coordination role for TF matters.[8] Finance Canada has a broad range of responsibilities in regulating and overseeing the financial sector and in policy development. It assesses proposed security initiatives to evaluate their financial cost, efficiency and potential impact on the economy.[9] As part of this function, the Department is responsible for developing policy relating to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*[10] (*PCMLTFA*) and its regulations[11]. The *PCMLTFA* and its regulations provide the framework for Canadian initiatives against TF and money laundering.[12]

Finance Canada is also responsible for coordinating the activities of the AML/ATF Initiative, including consultations with stakeholders.[13] Its specific goal in the AML/ATF Initiative is to protect Canada's financial sector from illicit uses, thus protecting its integrity.[14]

The AML/ATF initiative is "horizontal," meaning that Finance Canada works with other agencies, many of which are funded by the Initiative for their work on money laundering and TF matters. The funding arrangements do not earmark funds specifically for money laundering or for TF.[15] As a result, agencies can

4 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6752.
5 S.C. 2001, c. 41.
6 Testimony of Diane Lafleur, vol. 54, September 28, 2007, pp. 6750-6751.
7 *Proceeds of Crime (Money Laundering) and Terrorist Financing Act,* ss. 2, 42(1) [*PCMLTFA*]*; Office of the Superintendent of Financial Institutions Act*, R.S.C. 1985, c. 18 (3rd Supp.), Part I, ss. 3, 4(1) [OSFI Act].
8 Testimony of Diane Lafleur, vol. 54, p. 6752. For examples in the US and the UK, see Michael Jacobson, "Extremism's Deep Pockets: The growing challenge of fighting terrorist financing," online: The Politic <http://thepolitic.org/content/view/91> (accessed June 3, 2009).
9 *A New Review Mechanism for the RCMP's National Security Activities*, p. 210.
10 S.C. 2000, c. 17.
11 *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations*, SOR/2002-184 [PCMLTFR].
12 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6752.
13 Exhibit P-227, Tab 3: Department of Finance Memorandum of Evidence on Terrorist Financing, February 28, 2007, para. 4.25 [Department of Finance Memorandum of Evidence on Terrorist Financing].
14 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6753.
15 Testimony of Diane Lafleur, vol. 54, September 28, 2007, pp. 6754-6755.

direct funds to either activity. With no specific allocation of funds for TF, there is a danger that agencies will use the funds primarily for anti-money laundering efforts, leaving anti-TF efforts under funded. The following chart[16] shows the agencies funded by the Initiative:

Anti- Money Laundering/Anti-Terrorist Financing (AML/ATF) Initiative

Funded Partners	Annual Funding (thousands)			
	2006-07	2007-08	2008-09	2009-10
Department of Finance	$1,800	$1,800	$1,800	$1,800
Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)	$37,500	$38,600	$37,400	$37,500
Royal Canadian Mounted Police (RCMP)	$15,600	$12,000	$12,000	$12,000
Canada Border Services Agency (CBSA)	$7,800	$7,700	$7,700	$7,700
Canada Revenue Agency (CRA)	$2,200	$2,200	$2,200	$2,200
Department of Justice & Public Prosecution Services of Canada	$2,300	$2,300	$2,300	$2,300

Other agencies participate in the Initiative but are not funded by it. These include DFAIT, Public Safety Canada, CSIS and OSFI.[17] FINTRAC, DFAIT and Public Safety receive funding through a separate program – the Public Security and Anti-Terrorism (PSAT) initiative. CSIS also receives funding to deal with its expanded anti-TF activities.[18]

The activities of the Financial Action Task Force (FATF) and Finance Canada are intertwined. Member countries follow the FATF recommendations on money laundering and TF. For its part, Finance Canada assesses financial sectors to determine if there is a sufficient vulnerability to money laundering or TF to warrant applying anti-TF laws to them.

Finance Canada has no intelligence-gathering role, but it uses information from law enforcement and intelligence agencies for these assessments.[19] It conducts regular media scans about TF activities around the world and obtains

16 Exhibit P-227, Tab 2: Department of Finance Presentation, slide 2 [Department of Finance Presentation].
17 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6755.
18 Exhibit P-439: Department of Finance Response to Supplementary Questions of the Commission, Question 1(c) [Department of Finance Response to Supplementary Questions of the Commission].
19 Testimony of Diane Lafleur, vol. 54, September 28, 2007, pp. 6788-6789.

information on TF through its connection with the FATF.[20] The Department has no investigative powers.[21]

In developing policy, Finance Canada conducts outreach to private sector reporting entities and refers to them as "partners." Diane Lafleur, Director of the Financial Sector Division at Finance Canada, testified that these entities, as front line players, had a key role in the anti-TF program.[22] She stated that the program could not be effective without their commitment and that Finance Canada works closely with them to develop policies that make sense in given business environments. This was to ensure that "… we are not creating wonderful rules that actually can't be administered and therefore have no results and can't be effective."[23] Ms. Lafleur also saw FINTRAC as a key partner of Finance in policy development.[24]

Finance Canada was responsible in 2004 for the coordination and response to reviews of the AML/ATF Initiative by EKOS, a social research body, and by the Auditor General. Following those reviews, Finance published a consultation paper on the future of the Initiative and on proposed legislative changes. It also consulted private sector reporting entities. With the help of other agencies, Finance headed the government's participation in the five-year parliamentary review of the Initiative and guided the policy development process leading to the enactment of Bill C-25[25] in 2006.

The Department led the government's efforts to have the FATF revise its initial 2008 criticisms of Canada's anti-TF efforts as well as Canada's response to the final conclusions and recommendations of the 2008 FATF Mutual Evaluation of Canada.

In short, Finance Canada has the lead in developing policy regarding Canada's anti-TF program. As the lead in anti-TF and anti-money laundering policy development, Finance Canada is responsible for two interdepartmental committees that have mandates in those matters, and a Finance representative chairs both committees.[26] Finance Canada is also responsible for work on a "performance management framework" for the Initiative.

Finance Canada also has numerous international responsibilities. It is the lead department for the Canadian delegation to the FATF, the Caribbean Financial Action Task Force and the Asia/Pacific Group on Money Laundering. It is also responsible for the anti-TF issues of concern to other international bodies, including the G-7, G-8, G-20, the International Monetary Fund, the World Bank,

---

20 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6788.
21 Testimony of Diane Lafleur, vol. 54, September 28, 2007, pp. 6751, 6785.
22 Testimony of Diane Lafleur, vol. 54, September 28, 2007, pp. 6752-6753.
23 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6756.
24 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6786.
25 *An Act to amend the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and the Income Tax Act and to make a consequential amendment to another Act*, S.C. 2006, c. 12 [Bill C-25].
26 The committees are the Financial Crimes Interdepartmental Coordinating Committee (ICC) and the Financial Crimes Interdepartmental Steering Committee (ADM Steering Committee).

the United Nations, the Organization of American States, the Inter-American Drug Abuse Control Commission, the Commonwealth Secretariat, all FATF-style regional bodies and organizations, and other international AML/ATF organizations.[27]

3.2 Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)

3.2.1 Role, Goals, Structure and Overview

The Financial Transactions and Reports Analysis Centre (FINTRAC) is Canada's Financial Intelligence Unit (FIU).[28] FIUs have three main functions:

- to serve as a centralized repository for financial information;
- to analyze the information; and
- to facilitate the dissemination of the results.[29]

FIUs can also monitor compliance by AML/ATF programs with FATF requirements, block transactions and freeze bank accounts, and train those in the financial sector, research and public education.[30]

FINTRAC is an intelligence agency that receives financial information from private sector entities and government agencies and then produces financial intelligence.[31] FINTRAC is the product of Canada's attempt to comply with Recommendation 26 of the FATF's "40 Recommendations" on Money Laundering:

> Countries should establish a FIU that serves as a national centre for the receiving (and, as permitted, requesting), analysis and dissemination of [Suspicious Transaction Reports] and other information regarding potential money laundering or terrorist financing.[32]

FINTRAC is one of many federal agencies that Parliament has established to fight TF. FINTRAC's evidence of success is that it has produced valuable information

---

27 Department of Finance Memorandum of Evidence on Terrorist Financing, para. 4.27.

28 Much of Canada's legislation dealing with terrorist financing was examined earlier in this volume, but an important part of this legislation, specifically the *PCMLTFA*, is reserved for FINTRAC's work. The finer points of the *PCMLTFA* are therefore discussed in this section.

29 Jae-myong Koh, *Suppressing Terrorist Financing and Money Laundering* (Berlin: Springer, 2006), p. 54 [Koh, *Suppressing Terrorist Financing and Money Laundering*].

30 Koh, *Suppressing Terrorist Financing and Money Laundering*, p. 54.

31 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6950.

32 FATF's "40 Recommendations" can be found online: Financial Action Task Force <http://www.fatf-gafi.org/document/28/0,3343,en_32250379_32236930_33658140_1_1_1_1,00.html> (accessed September 14, 2009).

and identified links between individuals, organizations and transactions that help law enforcement and security intelligence agencies further their investigations.[33] FINTRAC believes that its activities help to create a hostile environment and a deterrent for those who want to use legitimate financial channels to launder money or finance terrorism[34] and that, without FINTRAC, the RCMP and CSIS would face greater difficulties in obtaining information and financial intelligence.[35]

In 1997, a FATF evaluation criticized Canada's anti-money laundering program, in part due to the absence of an FIU. In response to the evaluation and to the FATF's "40 Recommendations," Canada established FINTRAC in July 2000 through the *Proceeds of Crime (Money Laundering) Act*. FINTRAC's initial operations were targeted solely at money laundering. In 2001, the ATA added TF to FINTRAC's mandate. The Act regulating FINTRAC was accordingly renamed the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.

FINTRAC began operating in October 2001.[36] It is a young agency.[37] FINTRAC's TF work is even more recent. In addition, the implementation of its roles and responsibilities, both legal and operational, has occurred in stages.

FINTRAC's mission is to assist in combatting financial crime, whether generated by money laundering or TF. It is often involved in reviews of Canada's anti-TF program, including the 2008 FATF Mutual Evaluation of Canada. FINTRAC receives significantly more than half of the federal funds dedicated each year to the AML/ATF Initiative.

In general terms, FINTRAC's role is as follows:

> …as Canada's financial intelligence unit (FIU)…to safeguard Canada's financial system by contributing to the creation of a more hostile environment for money laundering and terrorist activity financing in Canada; by supporting the public safety and national security of Canadians; and by upholding personal privacy.[38]

---

33 Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, p. 6957.

34 Financial Transactions and Reports Analysis Centre of Canada, *Report on Plans and Priorities For the years 2007-2008 to 2009-2010*, p. 7, online: Treasury Board of Canada Secretariat <http://www.tbs-sct.gc.ca/rpp/0708/fintrac-canafe/fintrac-canafe-eng.pdf> (accessed June 3, 2009) [FINTRAC Report on Plans and Priorities for 2007-08 to 2009-10]; Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6952.

35 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6979.

36 UN CTC Report Submitted by Canada pursuant to Security Council resolution 1373 (2001), S/2004/132, p. 3, online: United Nations Security Council Counter-Terrorism Committee <http://daccessdds.un.org/doc/UNDOC/GEN/N06/297/90/PDF/N0629790.pdf?OpenElement> (accessed September 17, 2009).

37 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6967.

38 Financial Transactions and Reports Analysis Centre of Canada, *Departmental Performance Report For the Period ending March 31, 2007*, p. 6, online: Financial Transactions and Reports Analysis Centre of Canada <http://www.fintrac.gc.ca/publications/DPR/2007/DPR-eng.pdf> (accessed September 14, 2009) [FINTRAC 2006-07 Departmental Performance Report].

The *PCMLTFA* sets out the objects of FINTRAC, calling it an independent agency that does the following:

> (a) acts at arm's length from law enforcement agencies and other entities to which it is authorized to disclose information;
>
> (b) collects, analyses, assesses and discloses information in order to assist in the detection, prevention and deterrence of money laundering and of the financing of terrorist activities;
>
> (c) ensures that personal information under its control is protected from unauthorized disclosure;
>
> (d) operates to enhance public awareness and understanding of matters related to money laundering; and
>
> (e) ensures compliance with Part 1 of the *PCMLTFA* [which sets out the obligations of the reporting entities].[39]

The FINTRAC 2008 Annual Report describes the activities of the agency as follows:

- Receiving financial transaction reports in accordance with the legislation and regulations and safeguarding personal information under our control.
- Ensuring compliance of reporting entities with the legislation and regulations.
- Producing financial intelligence on suspected money laundering, terrorist activity financing and other threats to the security of Canada.
- Researching and analyzing data from a variety of information sources that shed light on trends and patterns in financial crime.
- Enhancing public awareness and understanding of money laundering and terrorist activity financing.[40]

The Department of Finance Memorandum of Evidence on Terrorist Financing offers a slightly fuller description of FINTRAC's responsibilities. They are to:

- receive and analyze financial transaction reports submitted by reporting entities in accordance with the *PCMLTFA* and its regulations, reports on the cross-border movement of currency

---

39 *PCMLTFA*, s. 40.

40 Financial Transactions and Reports Analysis Centre of Canada, *FINTRAC 2008 Annual Report*, page following cover page, online: Financial Transactions and Reports Analysis Centre of Canada <http://www.fintrac.gc.ca/publications/ar/2008/ar-eng.pdf> (accessed February 24, 2009) [FINTRAC 2008 Annual Report].

or monetary instruments, and information from international and domestic partners and from the general public;

- provide domestic police forces and foreign financial intelligence units (FIUs) (with which it has concluded an agreement to exchange information) with financial intelligence that it suspects would be relevant to the investigation or prosecution of money laundering and terrorist activity financing offences;
- provide the Canadian Security Intelligence Service (CSIS) with financial intelligence that it suspects would be relevant to threats to the security of Canada, including information on suspected terrorist activity financing;
- provide information to the CRA on suspected cases of terrorist financing involving charities, pursuant to an amendment made to the *PCMLTFA*;[41] and
- help fulfill Canada's international commitments to participate in the fight against transnational crime, particularly money laundering and terrorist financing.[42]

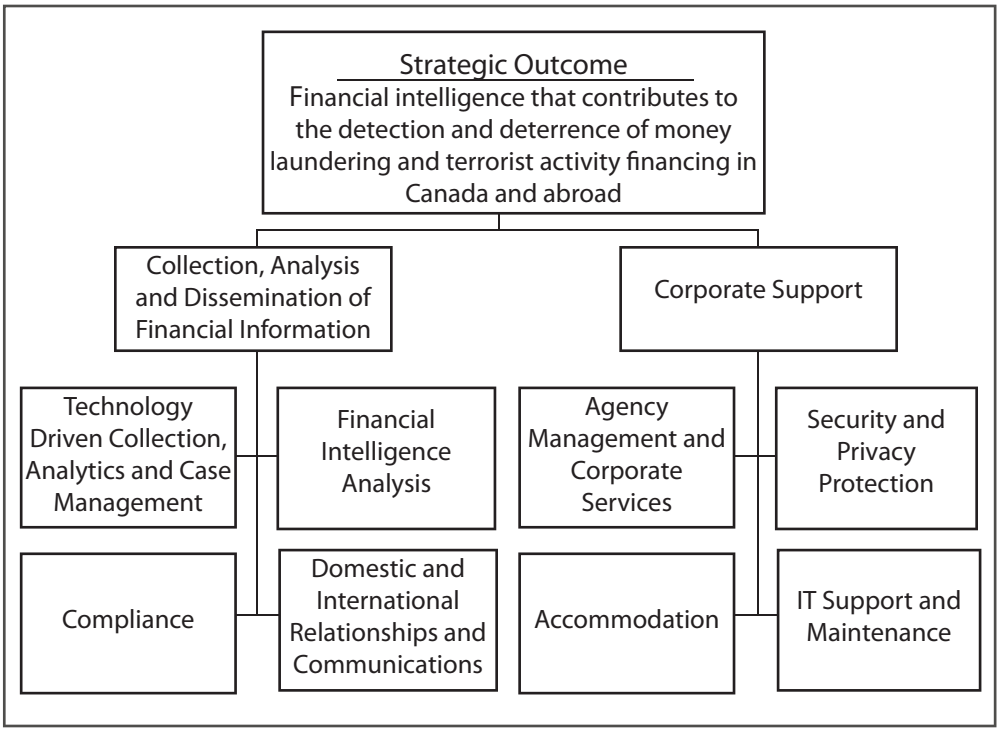
FINTRAC identified its three key priorities in its *Report on Plans and Priorities for the years 2007-2008 to 2009-2010*:

- deliver timely and high quality financial intelligence to law enforcement, security and intelligence agencies, and foreign financial intelligence units;
- ensure compliance with the *PCMLTFA*; and
- disseminate strategic information on money laundering and terrorist activity financing to partners, stakeholders, and the general public.[43]

FINTRAC's work products are (i) disclosures of information (based on its analysis of the information it holds or receives about financial transactions) to agencies such as the RCMP, CSIS, CRA, CSE and CBSA and (ii) the production of macro-analyses and research documents on money laundering and TF. FINTRAC's "program activity architecture" is illustrated below:[44]

---

41 This was an amendment introduced by Bill C-25.
42 Department of Finance Memorandum of Evidence on Terrorist Financing, para. 4.29.
43 FINTRAC Report on Plans and Priorities for 2007-08 to 2009-10, p. 6.
44 FINTRAC Report on Plans and Priorities for 2007-08 to 2009-10, p. 26.



The Minister of Finance is responsible for FINTRAC and reports to Parliament on its activities.[45] It might have made sense to put FINTRAC, the central agency under the *PCMLTFA*, under the umbrella of Public Safety Canada since other agencies under that umbrella have significant responsibilities in terrorism matters. However, Finance Canada, with its regulatory responsibility for many parts of the financial sector, is better suited for dealing with reporting entities from the financial world.

FINTRAC operates as an agent of the Crown[46] and acts "…at arm's length from law enforcement agencies and other entities to which it is authorized to disclose information."[47] At least part of the rationale for having Finance take on oversight was to avoid real or perceived conflicts of interest that might arise if FINTRAC were housed in a department or agency that might benefit from FINTRAC disclosures. Under Finance's umbrella, FINTRAC stands at arm's length from law enforcement.[48]

Besides reporting to Parliament through the Minister of Finance, FINTRAC maintains a close working relationship with the Department of Finance itself.[49]

45 *PCMLTFA*, ss. 2, 42(1).
46 *PCMLTFA*, s. 41(2).
47 *PCMLTFA*, s. 40(a).
48 Testimony of Diane Lafleur, vol. 54, September 28, 2007, pp. 6760-6761.
49 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6786.

However, Finance officials are not involved in FINTRAC operations, and have no access to data provided to FINTRAC by reporting entities.[50]

FINTRAC also maintains relationships with several branches of the federal and provincial governments,[51] as well as with international organizations and foreign agencies.[52]

FINTRAC is an "administrative" FIU – the most common FIU model internationally.[53] Among other things, this means that it is separate from law enforcement and intelligence agencies and from other bodies that receive information from it. It also means that FINTRAC is a stand-alone administrative and regulatory agency responsible for ensuring that reporting entities comply with the *PCMLTFA* and for analyzing the information received from them. Other, less common FIU models are the "law enforcement" model, where the FIU is part of a larger law enforcement apparatus, and the "prosecutorial" model, where the FIU falls under the jurisdiction of a public prosecutor's office.

Each model has merits. Some argue that the administrative model is more trusted by private sector reporting entities, since the FIU acts as a buffer between the entities and law enforcement agencies, and it permits more efficient information exchanges with foreign FIUs. However, an administrative model FIU does not have the same range of powers as the other two models, and may not be able to get information into the hands of law enforcement agencies as efficiently as an FIU where the law enforcement function is an integral part of the FIU itself.[54]

Mark Potter, Assistant Director for Government Relationships at FINTRAC, testified about the importance of FINTRAC's international connections in anti-TF matters:

> I think we all recognize we're part of a global network and that money launderers, terrorist financiers, will seek the weakest link. So to the extent we can cooperate, both at a policy and standard-setting level, through groups like the FATF and at an operational level, through groups like [the Egmont Group of

---

50 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6787; Testimony of Mark Potter, vol. 56, October 2, 2007, p. 7003.

51 These include national and provincial financial regulators, the RCMP and provincial and municipal police forces, CBSA, CRA, Department of Finance, Department of Justice, PSEPC, DFAIT, PCO and Treasury Board: Financial Transactions and Reports Analysis Centre of Canada, *FINTRAC 2006 Annual Report*, p. 7, online: Financial Transactions and Reports Analysis Centre of Canada <http://www.fintrac.gc.ca/publications/ar/2006/ar-eng.pdf> (accessed June 3, 2009) [FINTRAC 2006 Annual Report].

52 Including foreign financial intelligence units (FIUs), The Egmont Group of FIUs, FATF, the World Bank, the International Monetary Fund and the United Nations Global Programme against Money Laundering (UNGPML): FINTRAC 2006 Annual Report, p. 7.

53 Testimony of Mark Potter, vol. 56, October 2, 2007, pp. 7006-7007.

54 For the pros and cons of the various models, see International Money Fund and World Bank, *Financial Intelligence Units: An Overview*, pp. 9-17, online: International Monetary Fund <http://www.imf.org/external/pubs/ft/FIU/fiu.pdf> (accessed August 8, 2008) [IMF and World Bank Overview of FIUs]. See also Koh, *Suppressing Terrorist Financing and Money Laundering*, pp. 54-55.

> Financial Intelligence Units], in being able to share information efficiently, in sharing best practices with respect to training, with respect to information technology, helps us all reach a similar level of capacity to be able to – to combat global money laundering and terrorist financing.[55]

Since June 2002, FINTRAC has been a member of the Egmont Group of Financial Intelligence Units (the Egmont Group), an international organization founded in 1995 to foster communication and improve the exchange of information, intelligence and expertise, with a worldwide membership of more than 100 FIUs. The Egmont Group's purpose is to "…enhance cooperation and information exchange in support of member countries' anti-money laundering and terrorist financing regimes."[56] FINTRAC saw joining the Egmont Group as a milestone since it "…allows us to strengthen relationships with FIUs from around the globe and will facilitate the establishment of bi-lateral information exchange agreements that will assist domestic and global efforts to detect, deter and prevent money laundering and terrorist financing."[57]

FINTRAC collaborates with foreign FIUs individually in addition to relying on formal cooperation channels. For example, in 2006-07, FINTRAC worked with its Australian counterpart, AUSTRAC,[58] on technology upgrades and to improve data capture and data analysis capabilities.[59]

3.2.2 Reporting Entities and Their Obligations

The *PCMLTFA* imposes reporting obligations on entities from many sectors of the financial world.[60] Reporting entities are required to provide FINTRAC with information on certain financial transactions involving them. These entities include federally-regulated banks, provincially-regulated *caisses populaires* and credit unions, Money Services Businesses (MSBs) and securities dealers.

---

55 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 7006.

56 Financial Transactions and Reports Analysis Centre of Canada, "FINTRAC is a member of the Egmont Group," online: Financial Transactions and Reports Analysis Centre of Canada <http://www.fintrac.gc.ca/publications/inter/egmont-eng.asp> (accessed December 7, 2007).

57 FINTRAC's then Director was the chair of the Transition Sub-committee of Egmont in 2005-06 to "lead the group towards becoming a more sustainable and permanent institution": FINTRAC 2006 Annual Report, p. 5.

58 Prof. Martin Rudner has stated that "the Australian Financial Intelligence Unit is regarded as the gold standard, much more robust and much more capable in the prosecution, in both senses of the word, of people engaged in terrorism finance": Testimony of Martin Rudner, vol. 92, December 10, 2007, p. 12232.

59 Financial Transactions and Reports Analysis Centre of Canada, *FINTRAC 2007 Annual Report*, pp. 2, 25, online: Financial Transactions and Reports Analysis Centre of Canada <http://www.fintrac.gc.ca/publications/ar/2007/ar-eng.pdf> (accessed June 3, 2009) [FINTRAC 2007 Annual Report]; FINTRAC 2006-07 Departmental Performance Report, p. 14.

60 Although reporting entities are mostly from the private sector, s. 5(l) of the *PCMLTFA* also requires "departments and agents of Her Majesty in right of Canada or of a province that are engaged in the business of accepting deposit liabilities, that sell money orders to the public or that sell prescribed precious metals, while carrying out the activities described in regulations made under paragraph 73(1)(c)" to report.

Reporting entities are not a part of FINTRAC but critically aid its work. They provide most of the information received by FINTRAC[61] and have become the "eyes and ears" of the Centre.

Section 5 of the *PCMLTFA* identifies the entities required to report:

> (a) authorized foreign banks within the meaning of section 2 of the *Bank Act* in respect of their business in Canada, or banks to which that Act applies;
>
> (b) cooperative credit societies, savings and credit unions and caisses populaires regulated by a provincial Act and associations regulated by the *Cooperative Credit Associations Act*;
>
> (c) life companies or foreign life companies to which the *Insurance Companies Act* applies or life insurance companies regulated by a provincial Act;
>
> (d) companies to which the *Trust and Loan Companies Act* applies;
>
> (e) trust companies regulated by a provincial Act;
>
> (f) loan companies regulated by a provincial Act;
>
> (g) persons and entities authorized under provincial legislation to engage in the business of dealing in securities, or to provide portfolio management or investment counselling services;
>
> (h) persons and entities engaged in the business of foreign exchange dealing;
>
> (i) persons and entities engaged in a business, profession or activity described in regulations…;
>
> (j) persons and entities engaged in a business or profession described in regulations...while carrying out the activities described in the regulations;
>
> (k) casinos, as defined in the regulations, including those owned or controlled by Her Majesty;
>
> (l) departments and agents of Her Majesty in right of Canada or of a province that are engaged in the business of accepting deposit liabilities or that sell money orders to the public, while carrying out the activities described in regulations…; and

61 *PCMLTFA*, s. 54.

> (m) for the purposes of section 7 [which sets out the obligation to report certain transactions], employees of a person or entity referred to in any of paragraphs (a) to (l).

Sections 5(i) and 5(j) make it possible to add new reporting entities by way of regulation. The following organizations have been added: legal counsel and legal firms,[62] British Columbia notaries public and notary corporations, accountants and accounting firms, dealers in precious metals and stones, and real estate developers.

FINTRAC monitors reporting sectors to identify appropriate additions to the list of reporting entities. For example, in its 2007 Annual Report, FINTRAC stated that it had noticed a stronger presence of Internet payment systems and "white label" ATMs in its disclosures of financial intelligence to other agencies.[63] The ability to add new financial sectors is particularly important if those who finance terrorism shift their fundraising activities to sectors that may still not be subject to reporting requirements.

3.2.3 Collection or Receipt of Information

FINTRAC receives information from three main sources: (i) private sector reporting entities, (ii) foreign FIUs and (iii) federal government agencies such as the RCMP, CSIS and the CBSA.[64] It must retain any reports received or information collected for a minimum of 10 years.[65] Identifying information contained in a report must be destroyed after 15 years if, during that time, the report has not been disclosed to certain bodies (for example, CSIS or the RCMP) identified in the *PCMLTFA*.[66]

3.2.3.1 The Arm's-Length Arrangement

FINTRAC does not have the legal authority to compel other agencies to provide information to it.[67] Nor can other agencies compel FINTRAC to provide information to them, except by obtaining a production order, discussed below. This is because FINTRAC stands at arm's length from other agencies.

---

62 However, the obligation to report contained in ss. 7 and 9 of the *PCMLTFA* does not apply to legal counsel or legal firms when they are providing legal services: *PCMLTFA*, s. 10.1. Furthermore, s. 11 of the *PCMLTFA* states that nothing in Part 1 of the Act (which deals with record keeping, verifying identity, reporting of suspicious transactions and registration) requires a legal counsel to disclose any communication that is subject to solicitor-client privilege.

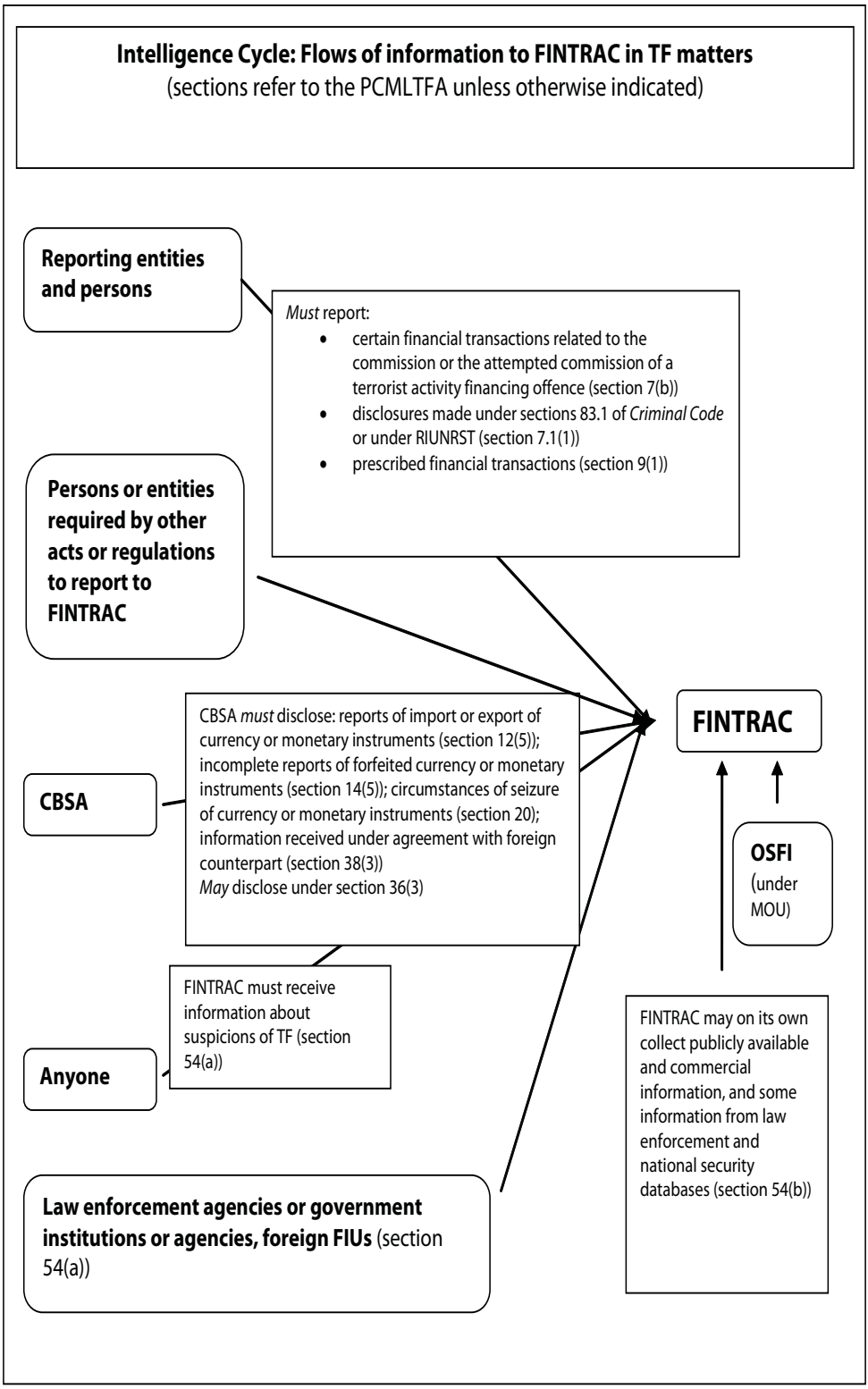
63 FINTRAC 2007 Annual Report, p. 24. "White label" ATMs dispense cash, but are not affiliated with a bank.

64 Department of Finance Memorandum of Evidence on Terrorist Financing, para. 4.31.

65 *PCMLTFA*, s. 54(d). The retention requirement is subject to s. 6 of the *Privacy Act*, R.S.C. 1985, c. P-21, which sets out requirements for the retention and disposal of personal information collected by federal government institutions.

66 *PCMLTFA*, s. 54(e).

67 Exhibit P-382: Dossier 4: Terrorist Financing, December 13, 2007, p. 40 [Terrorist Financing Dossier].


Intelligence Cycle: Flows of information to FINTRAC in TF matters
(sections refer to the PCMLTFA unless otherwise indicated)
Reporting entities and persons
Must report:
certain financial transactions related to the commission or the attempted commission of a terrorist activity financing offence (section 7(b))
disclosures made under sections 83.1 of Criminal Code or under RIUNRST (section 7.1(1))
prescribed financial transactions (section 9(1))
Persons or entities required by other acts or regulations to report to FINTRAC
CBSA
CBSA must disclose: reports of import or export of currency or monetary instruments (section 12(5)); incomplete reports of forfeited currency or monetary instruments (section 14(5)); circumstances of seizure of currency or monetary instruments (section 20); information received under agreement with foreign counterpart (section 38(3))
May disclose under section 36(3)
FINTRAC
OSFI (under MOU)
Anyone
FINTRAC must receive information about suspicions of TF (section 54(a))
FINTRAC may on its own collect publicly available and commercial information, and some information from law enforcement and national security databases (section 54(b))
Law enforcement agencies or government institutions or agencies, foreign FIUs (section 54(a))

3.2.3.2 Information Received from Reporting Entities

Under the *PCMLTFA*, reporting entities must do more than simply report certain transactions to FINTRAC. They have specific obligations about record-keeping, verifying clients' identities, complying with other legislation besides the *PCMLTFA*, and reporting suspicious and other transactions.[68]

Reporting entities must provide information to FINTRAC about the following:

- suspicious transactions (through Suspicious Transaction Reports (STRs)) related to the possible commission of a money laundering or terrorist activity financing offence;[69]
- the possession or control of property by listed entities (Terrorist Property Reports (TPRs));[70]
- cash transactions of $10,000 or more,[71] or two or more cash transactions within 24 hours that amount to $10,000 or more (Large Cash Transaction Reports),[72] other than withdrawals;[73] and
- electronic funds transfers of $10,000 or more, or two or more transactions within 24 hours that amount to $10,000 or more, where the sender or the recipient is located outside Canada (Electronic Funds Transfer Reports (EFTRs)).[74]

All the reports described above are submitted to FINTRAC on standardized forms. Reports are typically made using FINTRAC's electronic online system, known as F2R.[75]

Reporting entities have no specific legal authorization to report any transactions that could be considered a threat to the security of Canada.[76] Still, reporting entities, unsurprisingly, are not prohibited from reporting these types of transactions.

---

68 *PCMLTFA*, ss. 6-11.1.

69 *PCMLTFA*, s. 7.

70 Section 7.1 was added to the *PCMLTFA* in 2001 as part of the *Anti-terrorism Act*, S.C. 2001, c. 41 [*Anti-terrorism Act*] and requires a person or entity who is required to make a disclosure under s. 83.1 of the *Criminal Code*, R.S.C. 1985, c. C-46 [*Criminal Code*] to file a report with FINTRAC if that person or entity is subject to the *PCMLTFA*. Bill C-25 amended the provision by adding the obligation for a person or entity who is required to report under the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism*, S.O.R./2001-360 [RIUNRST] and who is subject to the *PCMLTFA*.

71 PCMLTFR, s. 12(1)(a).

72 PCMLTFR, s. 3(1).

73 PCMLTFR, s. 12(1)(a).

74 PCMLTFR, ss. 12(1)(b), 12(1)(c), 3(1).

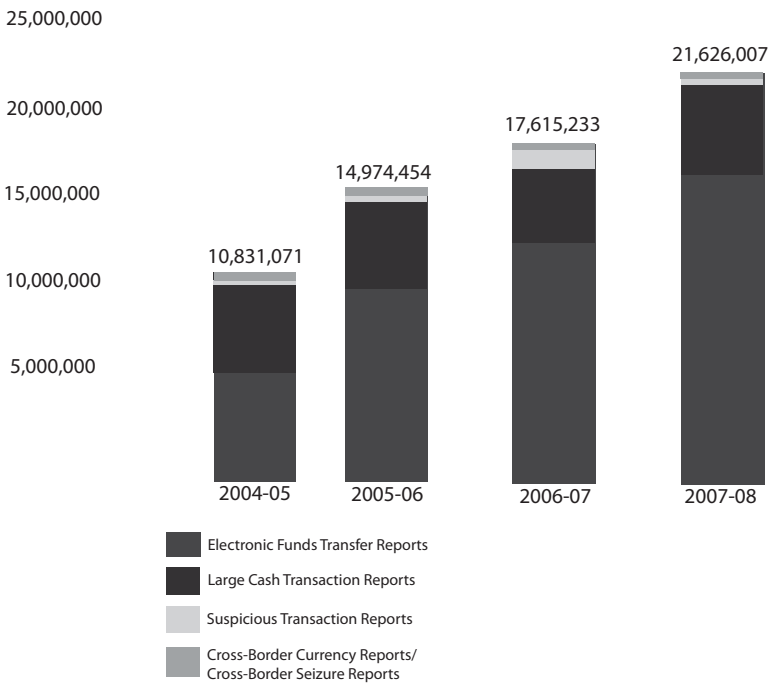
75 FINTRAC presented a demonstration of the F2R system to Commission Counsel during the course of the Inquiry.

76 A document prepared by FINTRAC also mentions this: see Exhibit P-233, Tab 11: Reasonable Grounds to Suspect, p. 1 [FINTRAC Response on Reasonable Grounds to Suspect].

Amendments to section 7 of the *PCMLTFA* came into force in June 2008. They require a reporting entity to report to FINTRAC when it has reasonable grounds to suspect that a transaction or attempted transaction is related to the commission or the attempted commission of a money laundering or terrorist activity financing offence.[77] Before, there was no obligation to report attempted transactions.

In fiscal year 2007-08, FINTRAC received slightly more than 21.6 million reports, a substantial increase over the previous year, and about twice as many reports as it received in 2004-05. However, only a very small percentage of reports to FINTRAC in recent years have been Suspicious Transaction Reports. The vast majority have been Electronic Funds Transfer Reports, followed by Large Cash Transaction Reports. The following chart[78] illustrates the breakdown of the reports received by FINTRAC, by fiscal year and type:

REPORTS RECEIVED BY FISCAL YEAR AND TYPE



Although FINTRAC has over the years received relatively few STRs as a proportion of the total reports, STRs are particularly important because reporting entities have applied their financial experience to flag these transactions as problematic. Mark Potter testified that the STR is "…often one of the richest and most useful types of reports for getting at particularly the terrorist financing side of things."[79]

77 The amendments were introduced by Bill C-25, s. 5.
78 FINTRAC 2008 Annual Report, p. 17.
79 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 7029.

Unlike STRs, other reports are triggered mechanically, without analysis by the reporting entity, when an objective threshold is met – cash transactions of $10,000 or more, for example.

"Objective threshold" reports also supply useful information.[80] For example, FINTRAC documents state that 93 per cent of its disclosures of information to other agencies about TF or threats to the security of Canada contained at least one EFTR, based on objective thresholds.[81] Even so, FINTRAC's own statistics show that Voluntary Information Records[82] (VIRs) provided by government agencies, along with STRs, are the most common sources of information leading to investigations.[83]

Section 7 of the *PCMLTFA* requires "…every person or entity [to] report to [FINTRAC] … every financial transaction that occurs or that is attempted in the course of their activities and in respect of which there are reasonable grounds to suspect that the transaction is related to…" the commission, or the attempted commission, of a money laundering offence or a terrorist activity financing offence. There is no definition in the *PCMLTFA* of "suspicious transaction," but FINTRAC has issued a guideline.[84] According to FINTRAC, the omission of a definition from the Act was deliberate, thereby leaving it up to the reporting entities, which were in the best position to make the determination.[85] There is no monetary limit below which STRs are not required.[86] The guideline indicates that "reasonable grounds to suspect" is "…determined by what is reasonable in your circumstances, including normal business practices and systems within your industry."[87] Furthermore, the guideline offers broad parameters for determining when a transaction might qualify as suspicious:

> As a general guide, a transaction may be connected to money laundering or terrorist activity financing when you think that it (or a group of transactions) raises questions or gives rise to discomfort, apprehension or mistrust.

---

80 Exhibit P-438: FINTRAC Response to Supplementary Questions of the Commission, January 9, 2008, Question 3(a) [First FINTRAC Response to Supplementary Questions of the Commission].

81 First FINTRAC Response to Supplementary Questions of the Commission, Question 3(b). This is consistent with the international nature of terrorism. See also Financial Action Task Force, *Third Mutual Evaluation on Anti-Money Laundering and Combating the Financing of Terrorism*, *Canada*, February 29, 2008, para. 101, online: Financial Action Task Force <http://www.fatf-gafi.org/dataoecd/5/3/40323928.pdf> (accessed April 1, 2009) [2008 FATF Mutual Evaluation of Canada].

82 As discussed below, the RCMP and other government agencies can voluntarily provide information to FINTRAC through Voluntary Information Records.

83 Exhibit P-233, Tab 14: FINTRAC Originators Chart [FINTRAC Originators Chart].

84 Financial Transactions and Reports Analysis Centre of Canada, "Guideline 2: Suspicious Transactions" (December 2008), online: Financial Transactions and Reports Analysis Centre of Canada <http://www.fintrac.gc.ca/publications/guide/Guide2/2-eng.asp> (accessed July 10, 2007) [FINTRAC Guideline on Suspicious Transactions].

85 FINTRAC Response on Reasonable Grounds to Suspect, p. 1.

86 FINTRAC Guideline on Suspicious Transactions, para. 6.1.

87 FINTRAC Guideline on Suspicious Transactions, para. 3.1.

> The context in which the transaction occurs or is attempted is a significant factor in assessing suspicion. This will vary from business to business, and from one client to another. You should evaluate transactions in terms of what seems appropriate and is within normal practices in your particular line of business, and based on your knowledge of your client. The fact that transactions do not appear to be in keeping with normal industry practices may be a relevant factor for determining whether there are reasonable grounds to suspect that the transactions are related to money laundering or terrorist activity financing.[88]

The guideline also identifies indicators of suspicious transactions relating to TF,[89] stating that these indicators resemble and complement indicators of suspicious transactions in money laundering cases. The guideline states that it can be difficult to distinguish between a suspicion of money laundering activity and a suspicion of TF activity.[90] For FINTRAC, the important point is whether the entity has suspicions, not whether the suspicions relate to money laundering or TF.[91] FINTRAC stated that most STRs that form the basis of disclosures to other agencies about possible TF were originally brought to FINTRAC's attention for their suspected relation to money laundering.[92]

The guideline notes that TF often involves smaller amounts than money laundering cases.[93] Entities are urged to provide as many details as possible, "… including anything that made you suspect that it might be related to terrorist financing, money laundering, or both."[94]

The guideline identifies more than 100 indicators that, alone or together, might point to suspicious activity.[95] Many are general, while others relate to specific activities or industries. Specific indicators are provided for financial sector entities, securities dealers, real estate brokers, non-profit organizations (NPOs) and Money Service Businesses (MSBs), among others. Below are several examples of indicators contained in the guideline:

---

88 FINTRAC Guideline on Suspicious Transactions, para. 6.1.
89 FINTRAC Guideline on Suspicious Transactions, paras. 7, 8.
90 FINTRAC Guideline on Suspicious Transactions, para. 6.2.
91 FINTRAC Guideline on Suspicious Transactions, para. 6.2.
92 Exhibit P-440: FINTRAC Response to Supplementary Questions of the Commission, February 5, 2008, Question 2(m)(i) [Second FINTRAC Response to Supplementary Questions of the Commission].
93 Janet DiFrancesco also testified that TF transactions are more difficult to identify than money laundering transactions because they involve "much smaller amounts of money": Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, p. 6956.
94 FINTRAC Guideline on Suspicious Transactions, para. 6.2.
95 The guideline clearly states that: "These indicators were compiled in consultation with reporting entities, law enforcement agencies and international financial intelligence organizations. They are not intended to cover every possible situation and are not to be viewed in isolation.": FINTRAC Guideline on Suspicious Transactions, para. 6.3.

- Client appears to have accounts with several financial institutions in one area for no apparent reason.
- Client conducts transactions at different physical locations in an apparent attempt to avoid detection.
- Client is accompanied and watched.
- Client shows uncommon curiosity about internal systems, controls and policies.
- Client uses aliases and a variety of similar but different addresses.
- Client spells his or her name differently from one transaction to another.
- Client makes inquiries that would indicate a desire to avoid reporting.
- Client has unusual knowledge of the law in relation to suspicious transaction reporting.
- Client is quick to volunteer that funds are "clean" or "not being laundered."
- Client appears to be structuring amounts to avoid record keeping, client identification or reporting thresholds.
- Client refuses to produce personal identification documents.
- All identification documents presented appear new or have recent issue dates.
- Client presents uncounted funds for a transaction. Upon counting, the client reduces the transaction to an amount just below that which could trigger reporting requirements.
- Stated occupation of the client is not in keeping with the level or type of activity (for example a student or an unemployed individual makes daily maximum cash withdrawals at multiple locations over a wide geographic area).
- Cash is transported by a cash courier.
- Transaction is unnecessarily complex for its stated purpose.
- Activity is inconsistent with what would be expected from declared business.
- Account with a large number of small cash deposits and a small number of large cash withdrawals.
- Establishment of multiple accounts, some of which appear to remain dormant for extended periods.
- Unusually large cash deposits by a client with personal or business links to an area associated with drug trafficking.

- Multiple personal and business accounts are used to collect and then funnel funds to a small number of foreign beneficiaries, particularly when they are in locations of concern, such as countries known or suspected to facilitate money laundering activities.
- Client and other parties to the transaction have no apparent ties to Canada.
- Transaction crosses many international lines.
- Transactions involving high-volume international transfers to third party accounts in countries that are not usual remittance corridors.
- Client visits the safety deposit box area immediately before making cash deposits.
- Client makes large cash withdrawals from a business account not normally associated with cash transactions.
- The non-profit organization appears to have little or no staff, no suitable offices or no telephone number, which is incompatible with their stated purpose and financial flows.
- The non-profit organization has operations in, or transactions to or from, high-risk jurisdictions.
- Sudden increase in the frequency and amounts of financial transactions for the organization, or the inverse, that is, the organization seems to hold funds in its account for a very long period.[96]

FINTRAC has compiled some of the most common reasons for sending STRs to FINTRAC:

- Customer known to authorities;
- Unusual business activity;
- Unable to ascertain source of funds;
- Multiple deposits at different branches;
- Many third party deposits, appears to be operating MSB through the account.[97]

Below is a chart[98] showing the number of STRs, by sector, that FINTRAC received in TF matters between 2001 and mid-2007.

---

96 FINTRAC Guideline on Suspicious Transactions, paras. 7, 8.

97 These and other reasons are found at Exhibit P-233, Tab 22: FINTRAC, "Tactical Financial Intelligence," pp. 18-20 [FINTRAC Presentation on Tactical Financial Intelligence].

98 Exhibit P-233, Tab 6: STRs Received by Sector, 2001-07.

FINTRAC'S RESPONSE TO AI INQUIRY
REQUEST FOR DISCLOSURE OF DOCUMENTS
TRANCHE 1

Q. Statistics regarding "suspicious transactions" reports linked to TF that FINTRAC has received from all financial institutions.

A. See chart below.

STRs Received by Sector

	2001-2002	2002-2003	2003-2004	2004-2005	2005-2006	2006-2007*
Accountant	7	20	20	40	20	12
Bank	576	3623	4077	5665	12084	5174
Caisse Populaire	1045	3357	1946	3151	4918	5185
Canada Post	87	127	73	19	35	249
Casino	143	498	360	390	420	223
Co-op Credit Society	20	29		1	6	0
Foreign Exchange Dealer	938	6188	3221	2109	963	429
Legal Counsel	5	2	3	0	0	0
Life Insurance Broker or Agent	1	1	11	2	4	0
Life Insurance Company	10	30	52	29	32	78
Money Services Business	182	647	1871	4048	7092	5148
Provincial Savings Office	5	61	17	202	336	114
Real Estate Broker/Sales Representative	2	8	6	6	12	42
Savings & Credit Unions	639	2415	2767	2905	2837	1336
Securities Dealer	42	169	80	74	83	48
Trust & Loan Company	31	37	64	214	438	388
Unknown	39	146	226	258	87	5

Note: statistics for 2006-07 are for the first two quarters only.

Potter testified that banks provide a preponderance of the financial transaction reports submitted to FINTRAC,[99] including the most STRs, but that MSBs also contribute a significant number. The relatively large number from MSBs is surprising because of the small size of the MSB sector in Canada and the absence, until Bill C-25 was enacted, of requirements for such entities to register with FINTRAC. The new registration requirements for MSBs should produce more and better reports from that sector.[100]

---

99 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6975. In fact, banks were the first institutions to be subjected to the reporting obligations under the FATF's original 40 Recommendations. Although non-bank financial institutions were also included in principle, no list of such institutions was provided: IMF and World Bank Overview of FIUs, p. 35.

100 Testimony of Mark Potter, vol. 56, October 2, 2007, pp. 6973-6974.

Several detailed guidance documents are also available to reporting entities to help them report properly.[101] These documents are updated as circumstances and legislation change.

The 2008 FATF Mutual Evaluation of Canada explained that federal officials felt that asking for further information would violate section 8 of the *Charter*,[102] although no court has yet made such a finding. Nonetheless, FINTRAC officials indicated that FINTRAC does go back to reporting entities to ask for additional information about an individual or a transaction.[103]

Many private sector reporting entities see the reporting system as complex and as imposing considerable responsibilities on them, especially because of the numerous reporting obligations, including client identification rules (also sometimes referred to as "customer due diligence"). The inherent complexity of the financial world and its myriad types of transactions further complicate matters. Some reporting entities complain in particular about the one-way flow of information that leaves them wondering whether their reporting efforts were at all useful.

3.2.3.3 Other Sources of Information for FINTRAC

The CBSA must send a Cross-Border Currency Report (CBCR) to FINTRAC for any cross-border movement of currency or monetary instruments of $10,000 or more.[104] CBSA also reports seizures of currency or monetary instruments via a Cross-Border Seizure Report (CBSR).[105] In addition, CBSA may provide information to FINTRAC if it has reasonable grounds to suspect that such information would be of assistance in the detection, prevention or deterrence of money laundering or financing of terrorist activities.[106]

The RCMP and other municipal or provincial police forces, CSIS, CSE, ITAC, CBSA, CRA, DFAIT and other agencies can all (if their governing legislation permits) provide information to FINTRAC by way of a form entitled a Voluntary Information Record (VIR). FINTRAC must also receive reports that are made to it by foreign

---

101 These guidelines are more technical than substantive. They include Guideline 3A: Submitting Suspicious Transaction Reports to FINTRAC Electronically, Guideline 3B: Submitting Suspicious Transaction Reports to FINTRAC by Paper, Guideline 5: Submitting Terrorist Property Reports, Guideline 7A: Submitting Large Cash Transaction Reports to FINTRAC Electronically, Guideline 7B: Submitting Large Cash Transaction Reports to FINTRAC by Paper, Guideline 8A: Submitting Non-SWIFT Electronic Funds Transfer Reports to FINTRAC Electronically, Guideline 8B: Submitting SWIFT Electronic Funds Transfer Reports to FINTRAC and Guideline 8C: Submitting Non-SWIFT Electronic Funds Transfer Reports to FINTRAC by Paper: see Financial Transactions and Reports Analysis Centre of Canada, "FINTRAC Guidelines," online: Financial Transactions and Reports Analysis Centre of Canada <http://www.fintrac.gc.ca/publications/guide/guide-eng.asp> (accessed July 10, 2008).

102 2008 FATF Mutual Evaluation of Canada, para. 402.

103 Testimony of Mark Potter, vol. 56, October 2, 2007, pp. 6987-6989.

104 *A New Review Mechanism for the RCMP's National Security Activities*, p. 186; *PCMLTFA*, ss. 12(1), 12(5); *Cross-border Currency and Monetary Instruments Reporting Regulations*, S.O.R./2002-412, s. 2(1) [*Cross-border Currency and Monetary Instruments Reporting Regulations*].

105 *PCMLTFA*, ss. 18, 20.

106 *PCMLTFA*, s. 36(3).

FIUs as well as other information voluntarily provided to it about suspicions of TF.[107] In addition, FINTRAC can collect information stored in databases maintained by the federal and provincial governments for law enforcement or national security purposes, such as the Canadian Police Information Centre (CPIC).[108] FINTRAC also relies on open source information – information available in the public domain, such as corporate registries. FINTRAC expressed concern, however, that it could not obtain access to CSIS databases.[109]

Media scans concerning money laundering, TF and possible threats to the security of Canada are reviewed daily by FINTRAC analysts. This open source information is then matched against FINTRAC's database. Such a process was used in the recent case of the "Toronto 18."[110]

FINTRAC also reviews past and present TF cases around the world to enhance its own research and analysis.[111]

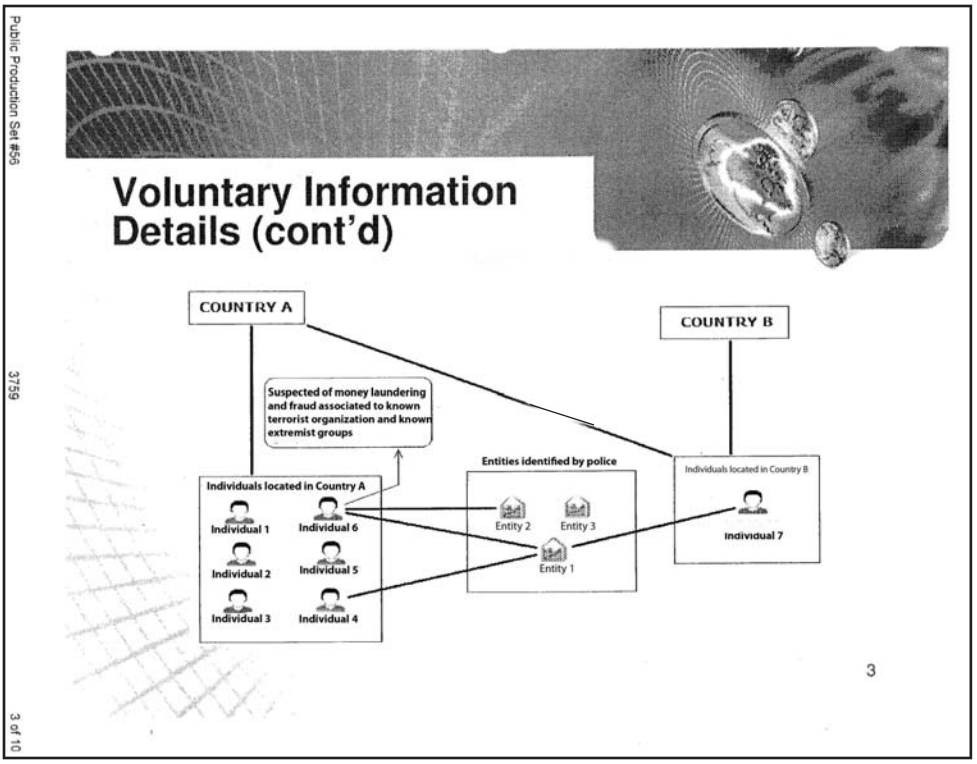
3.2.3.4 The Voluntary Information Record (VIR) Process

VIRs may relate to investigations of money laundering or TF offences.[112] Federal officials spoke of their importance. For example, James Galt of CSIS testified that his first reflex on handling a new TF file would be to determine whether FINTRAC had been consulted. He stated that he could not think of a reason why the information in a file should not be sent to FINTRAC.[113] RCMP Superintendent Rick Reynolds testified that, in TF matters, "…we provide…as many voluntary information reports as we feel appropriate and our resources allow."[114] Once it receives a VIR, FINTRAC's TF Unit assesses the information to determine if it can produce an analysis for the agency that submitted the VIR.[115]

As noted, the VIR is usually sent to FINTRAC using a standardized form.[116] Potter stated that the form was developed because the information FINTRAC was receiving before then was of "mixed quality."[117] The form, developed with FINTRAC's partners, speeds up the analysis process within FINTRAC.[118] During testimony, FINTRAC officials showed the Commission a "sanitized" case of actual TF activity. They also explained the content of the VIR in that case.

---

107 *PCMLTFA* s. 54(a).
108 *PCMLTFA* s. 54(b); Terrorist Financing Dossier, p. 39.
109 Exhibit P-442: Summary of Meeting between Commission Counsel and FINTRAC, April 10, 2008, p. 3 [Summary of Meeting with FINTRAC].
110 Exhibit P-233, Tab 20: FINTRAC Response to Various Questions of the Commission, p. 1. The informal name of the case has changed several times, as charges were dropped against some of the defendants. The term "Toronto 18" is used here.
111 Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, pp. 7009-7010.
112 Department of Finance Memorandum of Evidence on Terrorist Financing, p. 37.
113 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6941.
114 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6886.
115 Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, p. 6957.
116 English and French versions of a VIR form were entered into evidence: see Exhibit P-233, Tab 9.
117 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6960.
118 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6961.



[Exhibit P-233, Tab 21, p.3 (Public Production 3759)]

The preparation of VIRs in agencies such as the RCMP and CSIS is centralized, with at least one senior staff member tasked with overseeing the information provided in the VIRs.[119] There is no coordination between the RCMP and CSIS in preparing VIRs.

FINTRAC documents indicate that if a VIR is received from an agency such as CSIS, and if FINTRAC concludes that it meets the threshold for disclosing the information to law enforcement as suspected TF activity, it would seek permission from CSIS before such disclosure. Similarly, it would seek permission from a law enforcement agency before disclosing information to CSIS.[120] James Galt of CSIS stated that VIRs prepared by CSIS often contain an authorization to release the information to another agency.[121] CSIS documents indicate that this is done with about half of VIRs. For the remainder, FINTRAC would need to seek permission and CSIS would decide on a case-by-case basis.[122]

This arrangement whereby FINTRAC must seek permission from CSIS potentially conflicts with FINTRAC's legal obligation under the *PCMLTFA* to

119 Testimony of Jim Galt, vol. 55, October 1, p. 6917;
120 Second FINTRAC Response to Supplementary Questions of the Commission, Question 1(d).
121 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6920.
122 Exhibit P-441: CSIS Response to Supplementary Questions of the Commission, March 5, 2008, Question 2 [CSIS Response to Supplementary Questions of the Commission].

disclose designated information to a relevant agency when the threshold for disclosure is met. For example, section 55(3) of the *PCMLTFA* obliges FINTRAC to disclose information to "the appropriate police force" if FINTRAC has reasonable grounds to suspect that designated information would be relevant to investigating a terrorist activity financing offence. Even if CSIS had provided information in confidence, FINTRAC would be obliged to disclose it to the police if the information, combined with other information, gave FINTRAC "reasonable grounds to suspect." Thus, the conflict arises between FINTRAC'S agreement with CSIS and its obligations under the *PCMLTFA*.

FINTRAC officials have stated that, in most cases where they have not received prior authorization, they do receive it after they approach the agency that submitted the VIR. The two principal situations where the agency refuses permission are when the VIR contains information from a foreign FIU or information about undercover sources.[123]

FINTRAC gives priority to possible TF cases, regardless of the size of the operation.[124] Responding to VIRs submitted in TF matters is important to FINTRAC because of the possibility of loss of life from terrorist incidents.[125]

The amounts of money at issue in TF, typically smaller than in money laundering cases, make it more difficult for FINTRAC to generate TF leads on its own. Janet DiFrancesco, Assistant Director for Macro-Analysis and Integration within the Operations Sector at FINTRAC, gave evidence that the smaller number of independent TF investigations generated by FINTRAC was primarily due to the nature of TF cases: "…[T]ypically we're dealing with much smaller amounts of money moving."[126]

Unlike money laundering, where the large sums involved may arouse FINTRAC's suspicion, the small amounts sometimes involved in TF may give FINTRAC no reason to become suspicious. As a result, FINTRAC has difficulty identifying possible TF by relying solely on its internal analysis. Galt testified that FINTRAC had identified cases on its own three times in the last few years.[127] In most cases, it must rely on others – reporting entities or agencies such as the RCMP or CSIS – who are reporting their own suspicions to FINTRAC. FINTRAC can then add value through its analysis of the information that comes into its possession.

About 90 per cent[128] of the possible TF cases that come to FINTRAC's attention do so because FINTRAC has received law enforcement or CSIS VIRs. FINTRAC then responds to these VIRs, which can be viewed as unofficial requests for

123 Summary of Meeting with FINTRAC, p. 1.
124 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6962; Second FINTRAC Response to Supplementary Questions of the Commission, Question 2(b).
125 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6962.
126 Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, p. 6956.
127 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6920.
128 Testimony of Janet DiFrancesco, vol. 56, October 2, 2007 at p. 6956. Mark Potter could not give a number for the operations of FIUs in other countries: see Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6965.

information from FINTRAC – requests made by way of VIRs – by searching its own databases, analyzing the combined information and, if the legal criteria for disclosure are met, disclosing designated information to the appropriate agency.

Ms. DiFrancesco testified that FINTRAC identifies additional links, entities, individuals or accounts in regard to a particular investigation or matter. As well, to further advance the investigation, FINTRAC verifies links that law enforcement agencies have already made.[129] Because FINTRAC has information about electronic funds transfers (EFTs), information that law enforcement agencies usually do not hold, FINTRAC is well-positioned to identify links with foreign countries.[130] Potter testified that the VIR process also helped to maintain an appropriate relationship with other agencies:

> …[P]articularly with law enforcement and CSIS, it allows us to balance two things: on the one hand being able to respond to the investigative priorities of those agencies by receiving VIRs from them on targets and entities of interest to them, and on the other hand to balance the need to maintain an arm's-length relationship and not have direct access to our database by those agencies and ensure that any cases we do ultimately disclose in which a VIR is a factor, reach our threshold of reasonable grounds to suspect. So there is a balance that is achieved through the use of that mechanism and that piece of information.[131]

During 2005-06, FINTRAC received 47 VIRs that it classified as relating to national security. This represented nine per cent of the total VIRs received. During the same period, FINTRAC made 33 disclosures to other agencies relating to TF or threats to national security. Recipients made seven follow-up requests and FINTRAC responded by providing additional information for six of the seven. The 33 disclosures were not necessarily the product of the 47 VIRs received during 2005-06 because some disclosures could have been the result of VIRs from previous years.[132]

The 2008 FATF Mutual Evaluation of Canada spoke of FINTRAC's excessive reliance on VIRs for its TF work, stating that "…[t]his raises serious concern with respect to the capability of FINTRAC to generate new ML/TF cases independent from existing investigations."[133] The number of FINTRAC disclosures on TF matters which could lead to new investigations by other agencies should

---

129 Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, p. 6957.
130 Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, p. 6957. In fact, FINTRAC is one of several FIUs in the world to receive EFTs, which puts it in a good position in Canada's fight against TF and ML: FINTRAC 2007 Annual Report, p. 24.
131 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6959.
132 Exhibit P-233, Tab 10: FINTRAC Response on Voluntary Information Record Statistics, p. 1.
133 2008 FATF Mutual Evaluation of Canada, para. 21.

increase in coming years because the FINTRAC database is becoming more fully populated. Potter gave an example of a possible lead initiated by a FINTRAC review of media reports about terrorist activities. That information would then be combined with information in FINTRAC's database and analyzed.[134]

3.2.4 Analysis of Information Received by FINTRAC

Section 54(c) of the *PCMLTFA* provides that FINTRAC must analyze and assess the reports and information it receives. The analysis process consists of assembling all relevant information from various sources, trying to identify connections between various parties and, finally, trying to identify transactions that could be linked to either TF or money laundering.[135]

FINTRAC's 2008 Annual Report described the two general categories of financial intelligence that FINTRAC produces: "The first is information about specific suspicious transactions, that is, those that suggest movements of illicit money. The second is information showing overall patterns and trends as they emerge in the ever-evolving world of money laundering and terrorist financing."[136]

Each of FINTRAC's four Tactical Financial Intelligence Units, part of its Operations section, plays a role in the analysis process:

- One unit deals with VIRs, performing a general triage function and handling less complicated cases, as needed;
- One unit deals with money laundering;
- One unit deals with TF and queries from foreign FIUs; and
- One unit deals with STRs and open source information which might feed into the money laundering and TF units.[137]

Ms. DiFrancesco testified in 2007 that the TF unit at that time had a staff of approximately ten.[138] (The 2007 FINTRAC Annual Report stated that FINTRAC had 264 employees in total).[139] Employees in other units may also work on TF matters. FINTRAC's 2008 Annual Report stated that staffing increased to 329 employees during that year, but did not indicate how many devoted their time wholly or partly to TF matters.[140] The 2008 Annual Report spoke of how the efficiency of its electronic systems avoided the need to hire many more employees:

---

134 Testimony of Mark Potter, vol. 56, October 2, 2007, pp. 6963-6964.
135 FINTRAC Presentation on Tactical Financial Intelligence, p. 8.
136 FINTRAC 2008 Annual Report, p. 7.
137 Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, pp. 6953-6955.
138 Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, pp. 6955-6956.
139 FINTRAC 2007 Annual Report, p. 30.
140 FINTRAC 2008 Annual Report, p. 21.

> Annually, [FINTRAC's] powerful systems collect, capture, cleanse, and move 20 million reports into appropriate databases, all within two hours of receipt. Because of this, we have been able to cut down our use of paper files drastically, and we are saving immeasurable amounts of staff time. (Indeed, if we had to key in these reports manually, we would need another thousand employees.) We then scan these huge volumes of reports – using analytical tools designed specifically for FINTRAC's unique requirements – and quickly zero in on patterns of possible suspicious transactions.[141]

The 2008 Annual Report stressed the utility of these systems:

> …FINTRAC benefits from being one of the few FIUs that has developed electronic systems that permit the automated receipt of high volumes of financial reports and the rapid and precise mining of information from the millions of reports of various types in our databases.
>
> …
>
> We receive more than twenty million reports annually. Thirty years ago, the processing of this data would have required an army of sorters, filers and compilers to collect and analyze such volumes, as well as an airplane hangar in which to store the records. Today however, FINTRAC is up to the task at hand thanks to the advanced technological infrastructure – electronic systems that we constantly revamp and upgrade – that lies at the core of our operations.[142]

The Annual Report claimed that FINTRAC's technology and analysis provided considerable benefits for police and other recipients of FINTRAC disclosures:

> FINTRAC's sophisticated data mining techniques are able, for example, to look for links among transaction reports received from a multiplicity of different reporting entities. In so doing they can uncover the trail left by money launderers who typically use several banks – sometimes more than a dozen in widely dispersed locations – to try to evade detection…. [H]alf of our case disclosures this past year were based on reports from six or more reporting entities.
>
> …

141 FINTRAC 2008 Annual Report, p. 21.
142 FINTRAC 2008 Annual Report, p. 7.

> [T]he financial intelligence that FINTRAC discloses takes a variety of forms and is derived through many different methods. Often information provided to us by law enforcement and intelligence agencies leads us to comb through our databases to find connections that would otherwise elude investigators. What we are then able to disclose gives the investigators a valuable return on that initial lead.
>
> In other instances, our automated technology will find suspicious patterns of financial transactions, and these enable our analysts to construct a case that is wholly new to police and other disclosure recipients. Common to all cases, however, is the scope and detail of the intelligence that FINTRAC is able to provide.[143]

In analyzing the information it holds, FINTRAC looks at a broad array of indicators of TF. The following are examples:[144]

- Sending or receiving funds by international transfers from and/or to locations of specific concern;
- Atypical business/account behaviour;
- Charity/relief organization linked to transactions;
- Media coverage of account holder's activities;
- Ongoing investigation; and
- Large and/or rapid movement of funds;

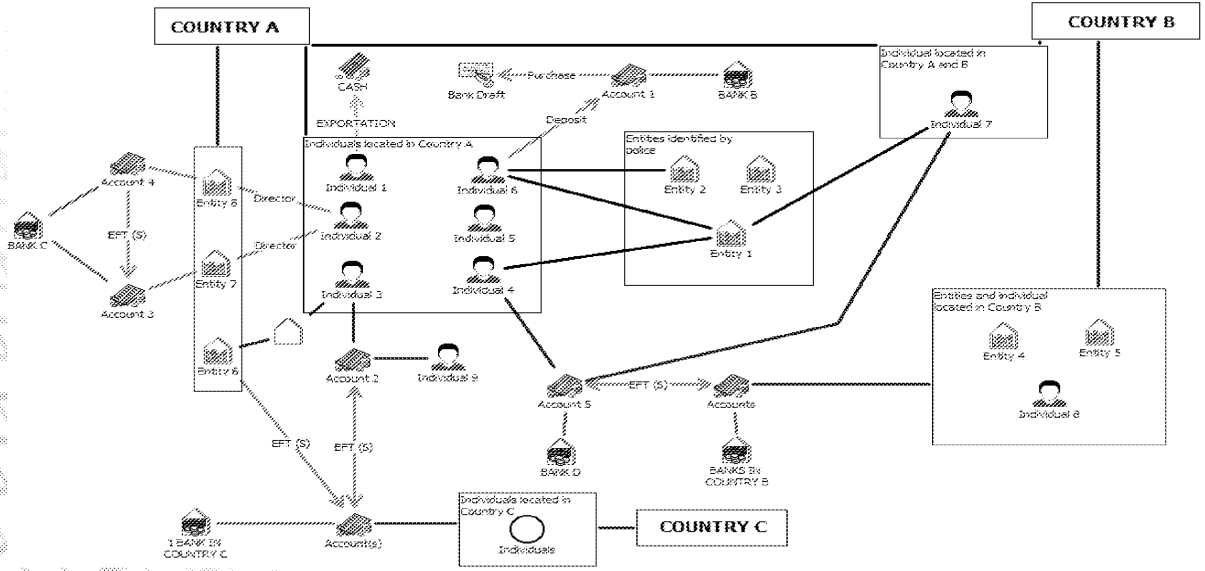
The 2008 FATF Mutual Evaluation of Canada criticized FINTRAC because of the indicators it used to determine whether a transaction was related to TF. The FATF concluded that the indicators were solely based on FATF typologies (examples of trends and methods) and indicators, as well as those of the Egmont Group and other FIUs, rather than developed by FINTRAC. The FATF concluded that, the list based on TF trends identified by FINTRAC itself spots "relatively basic and unsophisticated indicators."[145]

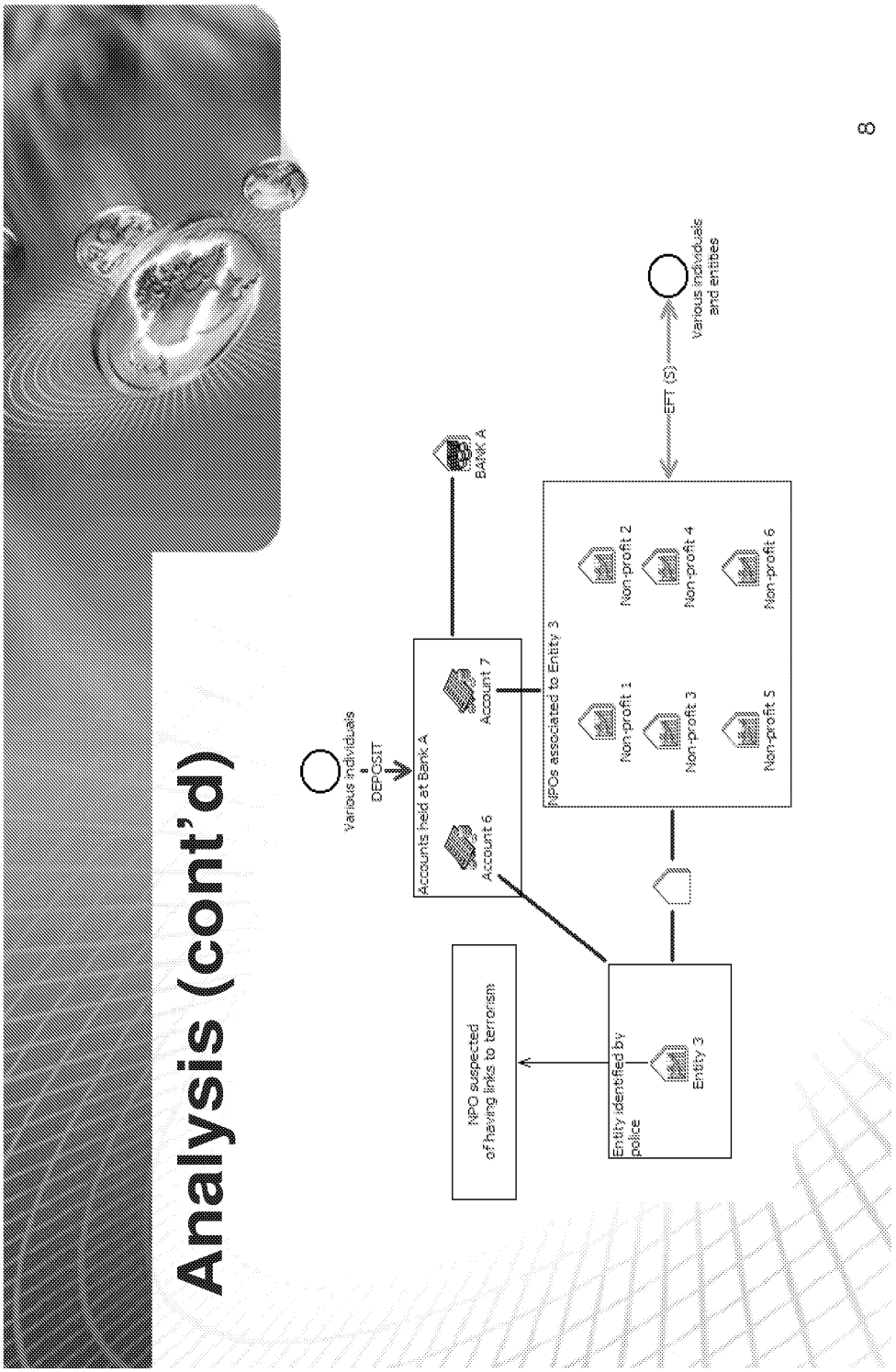
FINTRAC officials presented to the Commission a "sanitized" TF scheme. The scheme is complex, as the diagrams below show. This and other cases of such complexity may require FINTRAC to perform a very sophisticated analysis.[146]

---

143 FINTRAC 2008 Annual Report, p. 11.
144 The FINTRAC Presentation on Tactical Financial Intelligence includes a more complete list: see pp. 21-24.
145 2008 FATF Mutual Evaluation of Canada, para. 378.
146 Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, pp. 6989-6995.

Analysis (cont'd)



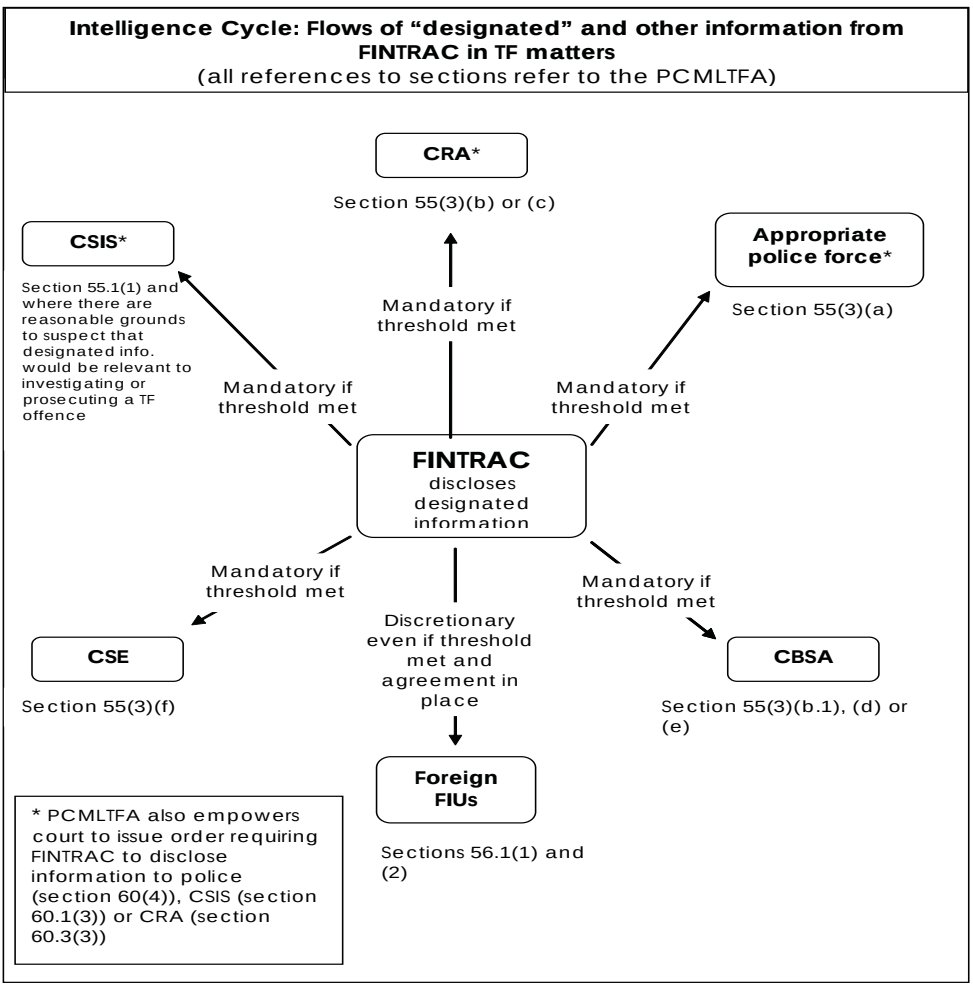


[Exhibit P-233, Tab 21 pp. 6 and 8 (Public Production # 3759)]

3.2.5 Disclosure of Information

3.2.5.1 Conditions for FINTRAC Disclosures

After completing its analysis,[147] FINTRAC must or may, if the legal threshold is met, disclose "designated information" to specific agencies. The following chart[148] explains the different tests for disclosure by FINTRAC:



147 *PCMLTFA*, s. 54(c).

148 Some provisions were in place before the *Anti-terrorism Act* – for example, in the *Proceeds of Crime (Money Laundering) Act* in regard to money laundering. The purpose of this chart is to differentiate between the provisions contained in Bill C-25 and those in place before in regard to TF. Anything which preceded Bill C-25 is labelled "ATA." Likewise, since agencies such as the Canada Customs and Revenue Agency and the Department of Citizenship and Immigration have changed, disclosure rules that may have been modified to apply to different recipients were not identified as "new" in the chart. For example, the previous s. 55(3)(b) was been amended and disclosure can now be made to two agencies instead of one because of organizational changes. As such, the "new" provisions are still labelled as originating in the *Anti-terrorism Act*.

1st Test	2nd Test	Recipient	PCMLTFA	Since
If FINTRAC has reasonable grounds to suspect that designated information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence;	None.	Police	55(3)(a)	ATA
If FINTRAC has reasonable grounds to suspect that designated information would be relevant to threats to the security of Canada;	None.	CSIS	55.1(1)	ATA
If FINTRAC has reasonable grounds to suspect that designated information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence;	If FINTRAC also determines that the information is relevant to an offence of obtaining or attempting to obtain a rebate, refund or credit to which a person or entity is not entitled, or of evading or attempting to evade paying taxes or duties imposed under an Act of Parliament administered by the Minister of National Revenue;	CRA	55(3)(b)	ATA
If FINTRAC has reasonable grounds to suspect that designated information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence;	If FINTRAC also has reasonable grounds to suspect that the information is relevant to determining whether a registered charity, as defined in subsection 248(1) of the *Income Tax Act*, has ceased to comply with the requirements of that Act for its registration as such;	CRA	55(3)(c)(i)	C-25
If FINTRAC has reasonable grounds to suspect that designated information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence;	If FINTRAC also has reasonable grounds to suspect that the information is relevant to determining whether a person or entity that the Centre has reasonable grounds to suspect has applied to be a registered charity, as defined in subsection 248(1) of the *Income Tax Act*, is eligible to be registered as such;	CRA	55(3)(c)(ii)	C-25
If FINTRAC has reasonable grounds to suspect that designated information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence;	If FINTRAC also determines that the information is relevant to an offence of evading or attempting to evade paying taxes or duties imposed under an Act of Parliament administered by the Agency;	CBSA	55(3)(b.1)	ATA
If FINTRAC has reasonable grounds to suspect that designated information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence;	If FINTRAC also determines that the information is relevant to determining whether a person is a person described in sections 34 to 42 of the *Immigration and Refugee Protection Act* or is relevant to an offence under any of sections 117 to 119, 126 or 127 of that Act;	CBSA	55(3)(d)	ATA
If FINTRAC has reasonable grounds to suspect that designated information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence;	If FINTRAC also determines that the information is relevant to investigating or prosecuting an offence of smuggling or attempting to smuggle goods subject to duties or an offence related to the importation of goods that are prohibited, controlled or regulated under the *Customs Act* or under any other Act of Parliament;	CBSA	55(3)(e)	C-25
If FINTRAC has reasonable grounds to suspect that designated information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence;	If FINTRAC also determines that the information is relevant to the mandate of the Communications Security Establishment referred to in paragraph 273.64(1)(a) of the *National Defence Act*.	CSE	55(3)(f)	C-25
If FINTRAC has reasonable grounds to suspect that the information would be relevant to the investigation or prosecution of a money laundering offence or a terrorist activity financing offence, or an offence that is substantially similar to either offence [and has a MOU in place];	In response to a request made by the institution or agency [FIU].	Foreign FIU	56.1(1) or (2) and 56.1 (2.1)	ATA
If FINTRAC has reasonable grounds to suspect that the information would be relevant to the investigation or prosecution of a money laundering offence or a terrorist activity financing offence, or an offence that is substantially similar to either offence [and has a MOU in place];	In order to perform its functions, FINTRAC may direct queries to an institution or agency [FIU] and in doing so it may disclose designated information.	Foreign FIU	56.1(1) or (2) and 56.1 (3)	ATA

Using an example from the chart, FINTRAC is required to disclose designated information to a law enforcement agency or CSIS if it meets the first test described in the chart – that FINTRAC has "…reasonable grounds to suspect that designated information *would be* relevant…." The conditions for disclosing to agencies other than CSIS and the RCMP are stricter. FINTRAC must satisfy not only the first test, but a second test as well. For example, the *PCMLTFA* requires FINTRAC to disclose designated information to the CRA under section 55(3)(b) of the *PCMLTFA*, but only if FINTRAC satisfies two tests:

- It has reasonable grounds to suspect that designated information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence, and
- It determines that the information is relevant to an offence of obtaining or attempting to obtain a rebate, refund or credit to which a person or entity is not entitled, or of evading or attempting to evade paying taxes or duties imposed under an Act of Parliament administered by the Minister of National Revenue.

Potter explained the reason for a more stringent test when FINTRAC deals with the CRA:

> I think the intent of the original legislation and the way we were put together was, we're a money laundering/terrorist financing financial intelligence unit, so that's our core focus. There are other agencies, like CRA that deal with tax evasion most directly. So I think there was a concern that might – at a minimum, there would be the perception that somehow this new agency was created and was going to be looking at your taxes.[149]

There is no definition of "reasonable grounds to suspect" in the *PCMLTFA* and no case law about its interpretation in the context of that legislation.[150] FINTRAC therefore relies on the case law interpreting the expression in other contexts:[151]

> Based on [various courts' interpretations of similar phrases], it would appear clear that FINTRAC would have "reasonable grounds to suspect" that information it would be disclosing would be relevant to investigating or prosecuting a terrorist

149 Testimony of Mark Potter, vol. 56, October 2, 2007, pp. 6970-6971.
150 FINTRAC Response on Reasonable Grounds to Suspect, p. 3.
151 FINTRAC Response on Reasonable Grounds to Suspect, p. 3. See pp. 4-5 of the same document for jurisprudence on this subject.

> activity financing offence when police provide FINTRAC with voluntary information regarding individuals and businesses of interest to them in the context of a particular investigation.[152]

The *PCMLTFA* requires FINTRAC to disclose designated information to CSIS if FINTRAC has reasonable grounds to suspect that designated information would be relevant to threats to the security of Canada.[153] One FINTRAC document provided to the Commission states that any "terrorist activity financing offence," as defined in the *PCMLTFA*, would constitute a "threat to the security of Canada" as defined in the *Canadian Security Intelligence Service Act (CSIS Act)*.[154] Accordingly, if the FINTRAC interpretation is accurate, when FINTRAC has reasonable grounds to suspect that financial intelligence would be relevant to investigating a terrorist activity financing offence, this would also constitute reasonable grounds to suspect that the intelligence would be relevant to "threats to the security of Canada." FINTRAC would be obliged to disclose the information to CSIS as well as whichever other agency to which the *PCMLTFA* requires disclosure. In short, if FINTRAC finds information that could be relevant to investigating or prosecuting a TF offence – barring possible limits on disclosure contained in VIRs sent to FINTRAC – FINTRAC must disclose information to CSIS as well as to other recipients.

However, the converse is not necessarily true. "Threats to the security of Canada" can take many forms that do not involve TF. If FINTRAC has reasonable grounds to suspect that designated information would be relevant to a threat to the security of Canada that does not involve TF – espionage, for example – FINTRAC must disclose the information only to CSIS.

FINTRAC has the discretion to disclose information to foreign FIUs with which it has a memorandum of understanding (MOU) on grounds similar to those for which it is obliged to disclose information to Canadian law enforcement agencies.[155] These MOUs must be approved by the Minister of Finance[156] and are limited in scope.[157] Before entering into an MOU with a foreign FIU, FINTRAC assesses the country's legal regime, relying on input from local partners.[158] FINTRAC seeks assurances that the country has adequate privacy measures to

---

152 FINTRAC Response on Reasonable Grounds to Suspect, p. 5. This does not appear to be far removed from direct access by recipients of FINTRAC information to FINTRAC's database, notwithstanding the prohibition to do so.

153 *PCMLTFA*, s. 55.1.

154 Second FINTRAC Response to Supplementary Questions of the Commission, Question 1(d).

155 *PCMLTFA*, s. 56.1(2); Testimony of Mark Potter, vol. 56, October 2, 2007, pp. 7010-7012. The Terrorist Financing Dossier notes that, "When FINTRAC decides whether to enter into an information-sharing agreement with a foreign financial intelligence agency, it considers the country's willingness and ability to protect the information that FINTRAC provides and to honour the restrictions that FINTRAC places on the information": p. 41, note 188. For a list of FINTRAC's MOU Partners as of July 2007, with the name of each FIU and the date of signature, see Exhibit P-233, Tab 18: FINTRAC MOU Partners.

156 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 7010; *PCMLTFA*, s. 56(2). The Minister may also enter into MOU agreements: see *PCMLTFA*, s. 56(1).

157 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 7011.

158 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 7011.

protect the information sent to its FIU.[159] Privacy concerns are one reason for FINTRAC's reluctance to sign MOUs with some foreign FIUs:

> Ideally, FINTRAC would be able to exchange information with every FIU in the world in pursuit of the money trail, without reservations, wherever that trail may lead. Practically, however, this desire to obtain information must be balanced with the need to ensure that FINTRAC is exchanging information with partners who will safeguard that information from unauthorized disclosure.[160]

In its 2007 Annual Report, FINTRAC stated that it had agreements with FIUs from 45 countries.[161] The 2008 Annual Report stated that FINTRAC signed agreements with two new FIU partners in Sweden and the island of St. Kitts and Nevis.[162]

When asked why none of the FIUs with whom FINTRAC had signed MOUs are located in countries that are "hotspots" of terrorism, FINTRAC offered two main explanations:

- FINTRAC's selection of MOU partners does not exclusively focus on TF, but also on money laundering. The MOU may be directed at money laundering alone and reflect the fact that a country is a money laundering "hotspot," but not a significant source of terrorism or TF; and
- Many jurisdictions that could be considered terrorism "hotspot" may have FIUs, but the FIUs may be in the early stages of development and they may not yet be members of the Egmont Group. All Egmont members undergo an operational evaluation before admission to ensure that they are able to maintain an agreed level of standards and practices. [The implication of this response by FINTRAC is that FINTRAC is reluctant to make an agreement with an FIU that has not passed the Egmont evaluation.][163]

FINTRAC did note, however, that it had MOUs with countries that have been targets of terrorist acts, including Spain, France, Israel, Indonesia, Colombia, the US and the UK.[164] After MOUs are in place, FINTRAC continues to monitor foreign countries' legal frameworks.[165]

159 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 7011.
160 Second FINTRAC Response to Supplementary Questions of the Commission, Question 6(a)(i).
161 FINTRAC 2007 Annual Report, p. 27. FINTRAC had MOUs with 30 FIUs in 2006 and 20 in 2005: see FINTRAC 2007 Annual Report, "FINTRAC Highlights 2005-2007," on the page following the report cover.
162 FINTRAC 2008 Annual Report, p. 20.
163 Second FINTRAC Response to Supplementary Questions of the Commission, Question 6(a).
164 Second FINTRAC Response to Supplementary Questions of the Commission, Question 6(a).
165 Testimony of Mark Potter, vol. 56, October 2, 2007, pp. 7011-7012. As of January 2008, FINTRAC had conducted outreach visits to the FIUs of Australia, Bahamas, Barbados, Belgium, Cayman Islands, Hong Kong, Israel, Italy, Mexico, Netherlands, Spain and the United States: Second FINTRAC Response to Supplementary Questions of the Commission, Question 6(d).

3.2.5.2 What FINTRAC Discloses

FINTRAC discloses only "designated information." The *PCMLTFA* defines "designated information" in three places,[166] and the applicable definition depends on the identity of the proposed recipient. Before the changes introduced by Bill C-25, only limited information – basically raw data[167] – could be disclosed, limiting the potential value of FINTRAC disclosures. As a result, recipients often had to do their own analysis of the information they received, causing delay and wasting resources.

Bill C-25 added new categories of information to what constituted "designated information" in the *PCMLTFA*. FINTRAC's 2008 Annual Report spoke of how this enhanced the value of FINTRAC's disclosures to other agencies:

> With the new provisions, our case disclosures can include a greater range of information relating to financial transactions, and the number of agencies to which we are authorized to make them has increased. Consequently, because our financial intelligence is enriched, its value in investigations is enhanced. Feedback from the law enforcement and intelligence communities already reflects this enhancement. [168]

The same report spoke of the more general "products" of FINTRAC's analysis that it discloses:

> In 2007-08, we produced and disseminated a wide range of well-received strategic analysis products to our partners. Among these were "The Watch", an environmental scan focused on money laundering and terrorist activity financing issues; "Backgrounders", which present a general overview of emerging trends and typologies; and financial intelligence "Briefs" which provide a more in-depth assessment of our reports and disclosures. As in the past, "Perspectives" were also produced to offer a retrospective of our disclosures and reports, and to identify typologies and patterns of transactions in relation to a particular subject or theme.[169]

The chart below shows the expanded categories of information included in the definition of "designated information" (the definitions in sections 55(7), 55.1 and 56.1 are identical at present).

---

166 *PCMLTFA*, ss. 55(7), 55.1(3), 56.1(5).
167 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6918.
168 FINTRAC 2008 Annual Report, p. 4.
169 FINTRAC 2008 Annual Report, p. 8.

	PCMLTFA on December 1st, 2006 Section 55(7)	PCMLTFA on June 13th, 2008 Section 55(7)
(a)	the name of the client or of the importer or exporter, or any person acting on their behalf;	the name of any person or entity that is involved in the transaction, attempted transaction, importation or exportation, or any person or entity acting on their behalf;
(b)	the name and address of the place of business where the transaction occurred or the address of the customs office where the importation or exportation occurred, and the date the transaction, importation or exportation occurred;	the name and address of the place of business where the transaction occurred or the address of the customs office where the importation or exportation occurred, and the date the transaction, importation or exportation occurred;
(c)	the amount and type of currency or monetary instruments involved or, in the case of a transaction, if no currency or monetary instruments are involved, the value of the transaction or the value of the funds that are the subject of the transaction;	the amount and type of currency or monetary instruments involved or, in the case of a transaction, if no currency or monetary instruments are involved, the value of the transaction or the value of the funds that are the subject of the transaction;
(d)	in the case of a transaction, the transaction number and the account number, if any;	in the case of a transaction, the transaction number and the account number, if any;
(e)*	any other similar identifying information that may be prescribed for the purposes of this section.	**similar section is now at (f) in the current PCMLTFA**
(e)*		the name, address, electronic mail address and telephone number of each partner, director or officer of an entity referred to in paragraph (a), and the address and telephone number of its principal place of business;
(f)		any other similar identifying information that may be prescribed for the purposes of this section;
(g)		the details of the criminal record of a person or entity referred to in paragraph (a) and any criminal charges laid against them that the Centre considers relevant in the circumstances;
(h)		the relationships suspected by the Centre on reasonable grounds to exist between any persons or entities referred to in paragraph (a) and any other persons or entities;
(i)		the financial interest that a person or entity referred to in paragraph (a) has in the entity on whose behalf the transaction was made or attempted, or on whose behalf the importation or exportation was made;
(j)		the name of the person or entity referred to in paragraph (a) suspected by the Centre on reasonable grounds to direct, either directly or indirectly, the transaction, attempted transaction, importation or exportation;
(k)		the grounds on which a person or entity made a report under section 7 about the transaction or attempted transaction and that the Centre considers relevant in the circumstances;
(l)		the number and types of reports on which a disclosure is based;
(m)		the number and categories of persons or entities that made those reports;
(n)		indicators of a money laundering offence or a terrorist activity financing offence related to the transaction, attempted transaction, importation or exportation.

As the chart shows, Bill C-25 brought a significant increase in the information qualified as designated information. FINTRAC now discloses links between the various parties identified in the disclosures, as well as the indicators of suspicious activity and the original grounds for an STR. Still, FINTRAC cannot of its own accord disclose its analysis in a specific case or the written justification for its disclosures.[170] FINTRAC explained that "…[t]he decision to allow disclosure of strictly factual information was, once again, a deliberate one to counterbalance the fact that FINTRAC would be making its disclosures based on the 'reasonable grounds to suspect' threshold, which is the least onerous legal standard possible that is not entirely subjective."[171]

Although Bill C-25 added new categories to the information that FINTRAC discloses, law enforcement agencies or CSIS may still need to analyze the information – in essence, repeating the analysis that FINTRAC has already done. Law enforcement agencies, CRA and CSIS can obtain a FINTRAC analysis (as opposed to designated information) only by obtaining a production order.[172]

The 2008 FATF Mutual Evaluation of Canada stated that 14 production orders had been sought to that point by law enforcement.[173] It is not known whether any of these orders related to TF, but the main point is the relatively small number of orders, even if all had related to TF.

3.2.5.3 How FINTRAC Discloses

FINTRAC has a rigorous internal case approval process that aims to ensure that the required threshold for disclosures is met.[174] The final decision to disclose rests with FINTRAC's Disclosure Committee, chaired by the Director of FINTRAC. If the disclosure package is approved, it is provided to recipients. The process can extend over a few weeks in a money laundering case, a period which may be reasonable since such an investigation is essentially reactive and the circumstances of the case do not generally threaten lives. In TF cases, however, lives can be at immediate risk and there may be a need to disclose information promptly. FINTRAC assured the Commission that the turnaround time in TF cases from receipt of a VIR to disclosure to an agency can be as fast as 24 hours and that FINTRAC gives TF disclosures priority.[175]

FINTRAC disclosures are made without any caveat on the use of the information. It is expected that the recipient will use the information to further its investigations.[176] The information disclosed by FINTRAC could potentially become public if a prosecution proceeds or if the recipients decide for any other reason to make the information public.

---

170 FINTRAC Response on Reasonable Grounds to Suspect, p. 2.
171 FINTRAC Response on Reasonable Grounds to Suspect, p. 2.
172 Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, p. 7016; *PCMLTFA*, ss. 60, 60.1, 60.3.
173 These numbers are probably current as of the time of the FATF on-site visit, which occurred early in 2007.
174 See Testimony of Mark Potter, vol. 56, October 2, 2007, pp. 6983-6984 for an explanation of the process.
175 Second FINTRAC Response to Supplementary Questions of the Commission, Question 4(a). See also 2008 FATF Mutual Evaluation of Canada, para. 375.
176 Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, p. 6994.

FINTRAC's 2008 Annual Report stated that FINTRAC made 210 disclosures of cases during the year under review. Of this total, 171 were associated with money laundering, 29 with TF and other "threats to Canada's safety," and 10 with both money laundering and TF.[177] The 2008 Annual Report did not state the value of the disclosures. However, the 2007 Annual Report indicated that there were roughly $10 billion in suspicious transactions,[178] of which about $208 million related to suspected TF or threats to the security of Canada.[179]

The amounts involved in individual disclosures are generally much smaller in TF cases than in money laundering cases. In 2005-06, the biggest single disclosure in a TF case involved about $98 million, with the average being $919,000 and the smallest being under $10,000. In contrast, the amounts involved in money laundering disclosures were at least $10,000, with the largest being $886 million.[180] The following chart shows the range in value of FINTRAC disclosures related to suspected TF:[181]

Threats and/or Terrorist Financing (Number of Cases)		
	2005-06	2006-07
0 - $1M	17	18
$1M - $10M	13	10
$10M - $50M	1	4
$50M - $100M	2	1
$100M - $500M	0	0
$500M - $1B	0	0
$1B +	0	0
Total Number of Disclosures	33	33

177 FINTRAC 2008 Annual Report, p. 9.
178 FINTRAC 2007 Annual Report, p. 8.
179 Second FINTRAC Response to Supplementary Questions of the Commission, Question 2(e); FINTRAC 2007 Annual Report, p. 8. In 2005-06, FINTRAC made 168 case disclosures involving slightly more than $5 billion in suspect financial transactions. Of these disclosures, 33 were for suspected terrorist activity financing and/or other threats to the security of Canada. One disclosure involved both suspected money laundering and suspected terrorist activity financing and/or threats to the security of Canada. Of the roughly $5 billion in suspicious transactions, approximately $256 million related to suspected terrorist activity financing and other threats to the security of Canada: FINTRAC 2006 Annual Report, p. 8.
180 Exhibit P-233, Tab 13: FINTRAC Disclosure Value Chart, p. 1.
181 Second FINTRAC Response to Supplementary Questions of the Commission, Question 2(i).

The number and dollar value of FINTRAC disclosures has steadily increased over the years for both TF and money laundering. According to FINTRAC, the increase in the value of disclosures flows from its strategy of focusing on large cases, its deeper knowledge of trends, more experienced staff, improved computer systems, and its growing database.[182]

In its 2007 Annual Report FINTRAC stated that the demand for its intelligence attested to its quality. The report also stated that feedback from law enforcement offered a clear indication of the value of the financial intelligence it provided.[183] As noted above, however, the 2008 Annual Report provided no indication of the dollar value of FINTRAC's disclosures for the period covered by the report.

FINTRAC officials explained that the dollar value of disclosures did not indicate the actual amount of TF taking place. This was because FINTRAC only needs to *suspect* that certain transactions are relevant to investigating a TF offence for it to disclose information. Even so, it included the value of these transactions in the total value of its disclosures.

One FINTRAC document stated that the value of a particular transaction is "…not necessarily the most relevant piece of the intelligence puzzle," adding that, for example, names of individuals and account numbers may have more intelligence value.[184]

3.2.6. Relationships between FINTRAC and Other Agencies

3.2.6.1 In General

As noted earlier, FINTRAC stands at arm's length from other agencies.[185] The arm's-length relationship is intended to address privacy concerns. A central issue is how to achieve a workable compromise between investigative efficiency and privacy rights. The objects of the *PCMLTFA* are relevant in searching for this compromise, since they include responding to the needs of law enforcement "…while ensuring that appropriate safeguards are put in place to protect the privacy of persons with respect to personal information about themselves."[186]

The 2008 FATF Mutual Evaluation of Canada described the justification advanced for the arm's-length relationship:

> The decision to provide police and other recipients with designated information only when FINTRAC reaches its threshold, rather than to provide unrestricted access to FINTRAC's data holdings, reflects the fact that FINTRAC receives

182 FINTRAC 2007 Annual Report, p. 9.
183 FINTRAC 2007 Annual Report, pp. 4, 10.
184 Second FINTRAC Response to Supplementary Questions of the Commission, Question 1(b).
185 The term "arm's length" is used in the *PCMLTFA*: see s. 40(a).
186 *PCMLTFA*, s. 3(b).

> a large amount of varied financial information on persons and entities, the vast majority of which is legitimate and not relevant to any investigation or prosecution.[187]

Janet DiFrancesco of FINTRAC testified that standing at arm's length from other bodies is an advantage:

> [O]ur regime…was created to be consistent with the *Charter of Rights*, and it does of course consider privacy laws but I think one of the advantages that FINTRAC does have, having been created at arm's length, is that we are also able to collect what we call more objective reports, prescribed transactions in terms of international wire transfers and large cash transaction reports.[188]

The relationship between FINTRAC and Finance Canada was described earlier in this chapter. Potter testified that FINTRAC's relationship with both CSIS and the RCMP, the most typical recipients of its disclosures, was "positive."[189] He described the relationship as follows:

> We would work with them…in a number of [areas other than disclosures], whether it be policy and legal development, whether it be research on new methods being used, typologies work; so there are a number of ways in which we would interact with the RCMP and CSIS beyond just the core relationship of providing disclosures.[190]

Potter described FINTRAC's relationship with CBSA as less close, since CBSA is a recipient of FINTRAC disclosures under different conditions from those that exist for the RCMP and CSIS.[191] FINTRAC continues to work on understanding and clarifying the conditions for disclosure to CBSA.

In 2004, the Auditor General[192] reported reluctance among law enforcement agencies to share information with FINTRAC. However, Ms. DiFrancesco testified that there was no longer any reluctance to share.[193]

FINTRAC also gives its partners macro-analyses (not to be confused with its analyses in individual cases, which it cannot disclose unless compelled by a

---

187 2008 FATF Mutual Evaluation of Canada, para. 382.
188 Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, pp. 6967-6968.
189 Testimony of Mark Potter, vol. 56, October 2, 2007, pp. 7004-7005.
190 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 7004.
191 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 7005.
192 *Report of the Auditor General of Canada to the House of Commons*, November 2004, Chapter 2: "Implementation of the National Initiative to Combat Money Laundering," para. 2.25, online: Office of the Auditor General of Canada <http://www.oag-bvg.gc.ca/internet/docs/20041102ce.pdf> (accessed January 16, 2009) [2004 Auditor General Report on Money Laundering].
193 Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, pp. 7018-7019.

production order) and research documents on money laundering and TF. In 2006-07, it provided macro-analyses to ITAC and to the Criminal Intelligence Service Ontario.[194] FINTRAC also contributed to assessments and studies by the RCMP and CSIS.[195] One FINTRAC document provided to the Commission stated that, during recent years, "…strategic information has been provided on FINTRAC's drug, fraud, and FIU query related disclosures and on the use of NPOs and internet payment systems."[196]

FINTRAC has specialized staff – Law Enforcement Liaison Officers – responsible for delivering disclosure packages to and obtaining feedback from law enforcement agencies. These officers also assist law enforcement agencies when they provide VIRs to FINTRAC.

Privacy concerns may arise from using secondments between FINTRAC and other agencies because of a fear that employees seconded from FINTRAC may use their FINTRAC connections to obtain information for the agency to which they are seconded, even if FINTRAC is not legally allowed or required to disclose the information.

3.2.6.2 Feedback to FINTRAC from Recipients of Disclosures

FINTRAC was criticized in the past for not disclosing sufficient information. Bill C-25 expanded the types of information that FINTRAC can or must disclose.

The Auditor General's November 2004 report found that police forces did not "give much weight" to unsolicited disclosures by FINTRAC.[197] RCMP Superintendent Reynolds assured the Commission that this was not the case, at least for the TF portion of the RCMP's work.[198]

FINTRAC provides voluntary Disclosure Feedback Forms with all of its disclosures. It has been encouraging disclosure recipients to complete the form and to identify leads that the FINTRAC information may have produced. FINTRAC receives some, though not regular, feedback. FINTRAC does not view such feedback as a necessity, but admits that it is useful to learn about the impact of its work.[199] In some cases, FINTRAC does receive follow-up information from law enforcement agencies about ongoing investigations.

FINTRAC officials indicated that the issue of feedback from disclosure recipients will be addressed in the "performance management framework" that is being developed under Finance Canada's leadership. This framework will involve all of the partners in the federal government's AML/ATF Initiative.

---

194 FINTRAC 2007 Annual Report, p. 24.
195 Second FINTRAC Response to Supplementary Questions of the Commission, Question 2(d).
196 Second FINTRAC Response to Supplementary Questions of the Commission, Question 2(d).
197 2004 Auditor General Report on Money Laundering, para. 2.25.
198 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6885.
199 Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, pp. 6994-6995.

Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) *Protected B* when completed

FINTRAC DISCLOSURE FEEDBACK FORM

* Please complete and submit this form within 30 days of receipt of a FINTRAC disclosure.

Originator (Disclosure Recipient) Information:

Agency Name:	FINTRAC Disclosure (DC#):	Type of Feedback ☐ Initial ☐ Follow-up
Lead Investigator:	Investigator Telephone:	
Date of this feedback (dd/mm/yyyy):	Date Disclosure Received (dd/mm/yyyy):	
Level of security (if other than Protected B) once form is completed:	Agency File #:	

1. Did this information (check all that apply):

- ☐ A) Relate to persons or business / entities of interest
- ☐ B) Provide a major contribution to your ongoing investigation
- ☐ C) Provide a minor contribution to your ongoing investigation
- ☐ D) Trigger a new investigation
- ☐ E) Contribute to a case that is expected to be prosecuted
- ☐ F) Provide you with names of, or leads on, previously unknown persons or businesses / entities
- ☐ G) Assist you in gathering sufficient evidence for a warrant
- ☐ H) Provide information useful for intelligence purposes
- ☐ I) Provide very limited or no value
- ☐ J) Other (please comment below):

If the information provided very limited or no value, it was because (check all that apply):

- ☐ K) The substantive offence was unknown
- ☐ L) Persons or businesses / entities unknown
- ☐ M) Contained no new intelligence
- ☐ N) Investigation was already concluded
- ☐ O) Already under investigation by another agency
- ☐ P) Not timely / not currently relevant
- ☐ Q) Other (please comment below):

2. Was the information forwarded to another section or agency?

☐ YES ☐ NO If YES, please specify:

3. What was the most useful aspect of this disclosure? (please comment):

4. Do you anticipate seeking a production order relating to this disclosure?

☐ YES ☐ NO ☐ Unknown at this time

5. General Feedback (quality and timeliness of the disclosure, relevance to your priorities, met expectations or not, how can we improve this product - substantive, format or process changes) please comment below:

As of January 2007, feedback to FINTRAC about the value of its disclosures produced the following results.[200] The disclosures:

- related to persons/business/entity of interest: 79%
- were useful for intelligence purposes: 75%
- provided names/leads on previous unknowns: 62%
- were a major contribution: 24%
- were a minor contribution: 23%[201]

Ms. DiFrancesco agreed with one counsel that feedback has a double benefit. If it is negative, it forces FINTRAC to make the appropriate changes. If it is positive, it can act as a morale booster.[202]

In addition to the voluntary feedback form, and in compliance with the Auditor General's recommendation encouraging FINTRAC to expand exchanges of information with other agencies, FINTRAC has initiated more frequent meetings with disclosure recipients. Meetings with the RCMP provide an opportunity to meet with RCMP investigators at both senior and working levels.[203]

Obtaining feedback through meetings and feedback forms is an ad hoc approach to evaluating the usefulness of FINTRAC. It is not required by law. As a result, meetings and feedback forms do not help to measure FINTRAC's performance systematically.

3.2.7 Interaction between FINTRAC and the Private Sector

Ms. Lafleur testified that FINTRAC and the anti-TF program are dependent on reporting entities.[204] Millions of transaction reports are sent to FINTRAC every year, producing an ever-growing database.[205] The FINTRAC *Report on Plans and Priorities For the years 2007-2008 to 2009-2010* noted that "…[t]he production of timely, high quality financial intelligence is dependant on reporting entities fulfilling their obligations to report and ensuring that the reported data is of high quality."[206] In short, if FINTRAC does not receive reports of sufficient quality, its own analysis suffers.[207] This in turn impedes the work of those to whom it discloses information.

---

200 See FINTRAC Disclosure Feedback Form, section 1, for the various categories. Disclosure recipients can select more than one answer.
201 Exhibit P-233, Tab 17: FINTRAC Disclosure Feedback Statistics.
202 Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, pp. 7014-7015.
203 Testimony of Mark Potter, vol. 56, October 2, 2007, pp. 6997-6998.
204 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6756.
205 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6950. At the time of the Commission's hearings, the database was said to contain around 60 million reports: see Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, p. 6957.
206 FINTRAC Report on Plans and Priorities for 2007-08 to 2009-10, p. 9.
207 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6985.

3.2.7.1 FINTRAC Measures to Ensure Compliance by Private Sector Reporting Entities

FINTRAC has the obligation to ensure that reporting entities comply with the *PCMLTFA* and its regulations.[208] A budget of $16.2 million was designated for FINTRAC's compliance efforts during the 2007-08 fiscal year.[209] FINTRAC's compliance examinations continue to demonstrate that the vast majority of reporting entities want to, and do in fact, comply with their legislative obligations.[210]

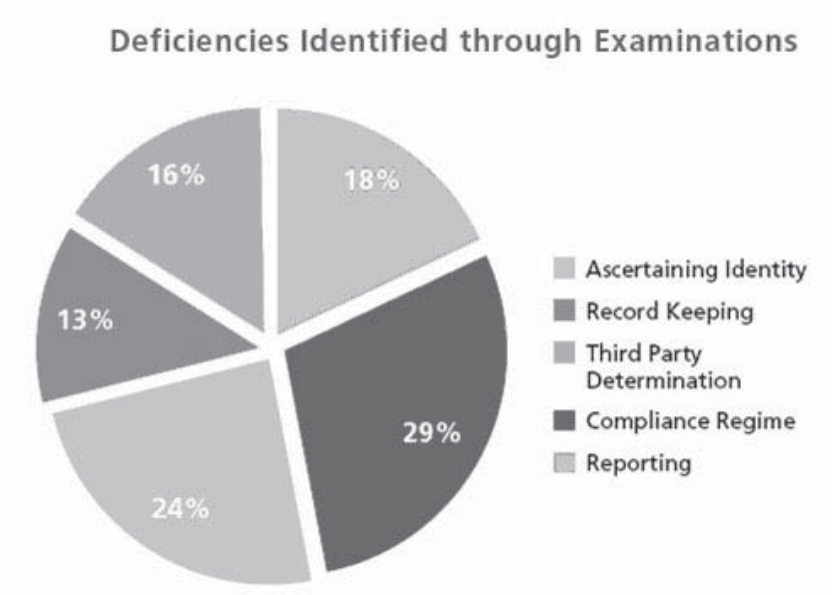
FINTRAC cannot oversee compliance by all reporting entities because of their numbers. Instead, compliance focuses "…primarily [on] those sectors and entities that are most at risk for non-compliance."[211] Compliance efforts consist of the following: awareness activities; monitoring data quality; questionnaires; on-site examinations; and taking appropriate remedial action when non-compliance is detected.[212]

FINTRAC has begun to refocus its compliance activities to invest more resources in examining reporting entities. Entities are selected using a risk-based approach, focusing on reporting entities at highest risk of non-compliance.[213] The FINTRAC 2008 Annual Report stated that, in 2007-08, FINTRAC conducted 277 examinations, and the national and provincial regulatory agencies with which FINTRAC had a memorandum of understanding conducted 257 examinations. FINTRAC disclosed five cases of suspected non-compliance with reporting obligations to law enforcement for investigation and prosecution.[214]

The FINTRAC 2008 Annual Report did not identify the deficiencies that examinations revealed. However, the 2007 Annual Report, covering 2006-07, identified the deficiencies found during that period:[215]

---

208 *PCMLTFA*, s. 62.
209 FINTRAC Report on Plans and Priorities for 2007-08 to 2009-10, p. 13.
210 FINTRAC Report on Plans and Priorities for 2007-08 to 2009-10, p. 15.
211 Exhibit P-233, Tab 7: FINTRAC's Risk-Based Approach, p. 1 [FINTRAC's Risk-Based Approach].
212 FINTRAC Report on Plans and Priorities for 2007-08 to 2009-10, p. 13; Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6986; FINTRAC's Risk-Based Approach.
213 FINTRAC Report on Plans and Priorities for 2007-08 to 2009-10, p. 14.
214 FINTRAC 2008 Annual Report, p. 17.
215 FINTRAC 2007 Annual Report, p. 19.



In performing compliance work, FINTRAC considers a wide range of factors, such as "…open source information, reporting volumes, observations gleaned from outreach activities, voluntary information which FINTRAC has received on non-compliance, results from compliance questionnaires completed by reporting entities, information received from regulators, quality and quantity assurance reviews, and the results of compliance examinations."[216] FINTRAC assigns a general risk level to reporting sectors based on these factors, although risk-based assessments of individual entities within the various reporting sectors are also done.[217]

Compliance questionnaires, which FINTRAC considers an effective tool for monitoring compliance, are widely used. As a result, FINTRAC can cover many reporting entities at low cost.[218] In 2007-08, more than 6,000 questionnaires were sent to reporting entities.[219]

Bill C-25 introduced a requirement for reporting entities to establish and implement a compliance program in addition to their reporting duties. The program is "risk-based," since it must include "…the development and application of policies and procedures for the person or entity to assess, in the course of their activities, the risk of a money laundering offence or a terrorist activity

---

216 FINTRAC's Risk-Based Approach, pp. 1-2.
217 FINTRAC's Risk-Based Approach, p. 2.
218 Questionnaires assess compliance by reporting entities by asking about several subjects, such as the size and scope of the reporting entity's operation, the entity's business lines, the implementation of a compliance regime, compliance policies and procedures, review of compliance policies and procedures, and ongoing compliance training: see FINTRAC's Risk-Based Approach, p. 2.
219 FINTRAC 2008 Annual Report, p. 17.

financing offence."[220] This risk-based approach is not designed to replace an approach based on simply complying with rules that require reporting (a "rules-based" approach). FINTRAC provides guidance on its website about setting up programs.[221]

FINTRAC documents describe the risk-based approach for reporting entities in their compliance programs as consisting of the following elements:

- risk assessment of its business activities, using certain factors;
- risk-mitigation to implement controls to handle identified risks;
- keeping client identification and, if required for its sector, beneficial ownership information up to date; and
- ongoing monitoring of financial transactions that pose higher risks.[222]

One submission on behalf of the Indian Nationals proposed greater reliance on a risk-based approach.[223]

FINTRAC also consults with other agencies that have responsibility for regulating entities covered under the *PCMLTFA*.[224] FINTRAC states that this facilitates its compliance work and can help minimize duplication of effort and the burden imposed upon reporting entities. As of March 2007, FINTRAC had MOUs with the following agencies:

- Office of the Superintendent of Financial Institutions (OSFI);
- Investment Dealers Association of Canada (IDA);
- Alberta Gaming and Liquor Commission (AGLC);
- Financial Institutions Commission of British Columbia (FICOM);
- Gaming Policy and Enforcement Branch (BC)(GPEB);
- Credit Union Deposit Guarantee Corporation of Manitoba (CUDGC);
- Brunswick Credit Union Federation Stabilization Board Limited ("Risk Management Agency" (RMA));
- New Brunswick Department of Justice and Consumer Affairs, Insurance Branch;

---

220 *PCMLTFA*, ss. 9.6(1), 9.6(2).

221 Financial Transactions and Reports Analysis Centre of Canada, "Guideline 4: Implementation of a Compliance Regime" (December 2008), online: Financial Transactions and Reports Analysis Centre of Canada <http://www.fintrac.gc.ca/publications/guide/Guide4/4-eng.asp> (accessed July 18, 2008).

222 Financial Transactions and Reports Analysis Centre of Canada, "Guideline 4: Implementation of a Compliance Regime" (December 2008), Chapter 6: "Risk-Based Approach," online: Financial Transactions and Reports Analysis Centre of Canada <http://www.fintrac.gc.ca/publications/guide/Guide4/4-eng.asp#66> (accessed August 6, 2008).

223 Submissions of the Family Members of the Crew Victims of Air India Flight 182 and Indian Nationals, Air India Cabin Crew Association, Sanjay Lazar and Aleen Quraishi, p. 45.

224 FINTRAC's Risk-Based Approach, p. 2; *PCMLTFA*, s. 65(2).

- Office de stabilisation de la Fédération des caisses populaires acadiennes;
- Credit Union Deposit Guarantee Corporation of Newfoundland and Labrador (CUDGC);
- Nova Scotia Environment and Labour, Alcohol and Gaming Division;
- Nova Scotia Credit Union Deposit Insurance Corporation (NSCUDIC);
- Alcohol and Gaming Commission of Ontario (AGCO);
- Deposit Insurance Corporation of Ontario (DICO);
- Autorité des marchés financiers (Québec) (AMF);
- Credit Union Deposit Guarantee Corporation (Saskatchewan); and
- Saskatchewan Liquor and Gaming Authority (SLGA).[225]

These MOUs allow FINTRAC to "…regularly exchange statistics, risk assessment information, examination results, and examination plans" with these agencies.[226] The arrangements do not constitute a delegation of authority to ensure compliance, since FINTRAC still conducts examinations in reporting sectors that are covered by MOUs.[227] FINTRAC has described the work of its MOU partners as providing "significant supervisory coverage":

> The work done by regulators to assess risk, examine entities, identify deficiencies, require corrective action and possibly sanction entities under their own powers serves to provide significant supervisory coverage of financial intermediaries with [Anti-money Laundering/TF] requirements.[228]

Besides concern about the adequacy of reports from reporting entities – in 2006-07, FINTRAC identified over 1300 cases where transaction reports were sent back to the originator, for what were considered mostly substantive issues[229] – there is concern that not all reporting entities are reporting to FINTRAC. FINTRAC uses various strategies to identify non-reporting. These include media scans of entities that provide financial services, complaints from other reporting entities, identification by compliance officers or law enforcement agencies and information provided voluntarily by the public.[230] FINTRAC also does a comparative analysis of reporting volumes among activity sectors.[231] As well, when it knows the identities of entities that fail to report, it contacts them in order to "bring them into the fold," and it undertakes on-site examinations in appropriate cases.[232]

---

225 FINTRAC 2007 Annual Report, p. 22.
226 FINTRAC's Risk-Based Approach, p. 3.
227 FINTRAC's Risk-Based Approach, p. 3.
228 FINTRAC's Risk-Based Approach, p. 3.
229 FINTRAC 2007 Annual Report, p. 18; First FINTRAC Response to Supplementary Questions of the Commission, Question 2(j).
230 Exhibit P-233, Tab 8: FINTRAC Determining and Dealing with "Non-Reporting," p. 1 [FINTRAC Determining and Dealing with "Non-Reporting"].
231 FINTRAC Determining and Dealing with "Non-Reporting," p. 1.
232 FINTRAC Determining and Dealing with "Non-Reporting," p. 1.

Amendments introduced by Bill C-25[233] gave FINTRAC the authority to impose monetary penalties on entities that fail to comply with reporting requirements.[234] Under the *PCMLTFA*, FINTRAC also has the authority to disclose non-compliance to the police.[235] Fewer than 20 cases of non-compliance had been reported (as of the time of FINTRAC's 2008 Annual Report) to law enforcement agencies since the beginning of the compliance program in 2004.[236] FINTRAC indicated that it disclosed non-compliance to law enforcement agencies when it saw little likelihood of compliance by an entity.[237]

Monetary penalties add flexibility to FINTRAC's compliance work. However, the Office of the Privacy Commissioner of Canada argued that if reporting entities become fearful of the penalties and the attendant negative publicity, they could try to minimize the risk and over-report to ensure compliance as a result.[238] This would expand FINTRAC's databases to the point of allowing it to compile information on an even greater number of perfectly lawful transactions.

Other factors might lead to under-reporting of suspect transactions. For example, the lack of feedback by FINTRAC to reporting entities might lead the entities to conclude that the STRs they provide have little value in countering TF; as a result, the entities may become less vigilant and less likely to submit STRs, although they would still presumably report transactions that exceed a given monetary threshold.

3.2.7.2 Outreach and Guidance Tools

FINTRAC offers information sessions for reporting entities about changes in legislation,[239] as well as to help them comply with their reporting obligations. Private sector reporting entities are reminded regularly how important it is to provide reliable information to FINTRAC.[240]

---

233 Bill C-25, s. 40, introducing ss. 73.1-73.5 to the *PCMLTFA*; 2008 FATF Mutual Evaluation of Canada, p. 311.

234 The IMF and World Bank Overview of FIUs mentions that: "To obtain compliance with the AML/CFT reporting obligations, there needs to be in place a set of measures intended to foster improvements in the flow and quality of reports without resort to sanctions, such as awareness raising and training," but that "…[a]fter an outreach program has been in place for a certain length of time, the FIU needs to consider the case of entities that fall below the level of reporting of the sector as a whole [...] [a]n array of administrative sanctions may be set out in the legislation to deal with non-compliant entities, and the application of the sanction varies according to the gravity of the offense": pp. 53-54.

235 *PCMLTFA*, ss. 65(1), 65(2).

236 FINTRAC 2008 Annual Report, p. 17.

237 First FINTRAC Response to Supplementary Questions of the Commission, Question 2(l)(i).

238 Exhibit P-278, Tab 5: Office of the Privacy Commissioner of Canada, Submission in Response to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, "Canada's Financial Monitoring Regime," September 2007, p. 4.

239 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6985.

240 See, for example, Financial Transactions and Reports Analysis Centre of Canada, "Feedback on Suspicious Transaction Reporting: Banking Sector," para. 1.2, online: Financial Transactions and Reports Analysis Centre of Canada <http://www.fintrac.gc.ca/publications/FOR/2007-04-04/bsf-eng.asp#112> (accessed October 3, 2008).

In 2007-08, FINTRAC employees delivered 370 presentations and seminars to reporting entities, reaching over 18,000 individuals. Among these were 24 information sessions in 10 cities about the new requirements of the *PCMLTFA* brought about by Bill C-25.[241] FINTRAC's 2008 Annual Report acknowledged that financial institutions and intermediaries subject to the *PCMLTFA* were "undoubtedly" in a "challenging period" as they prepared for changes to their legal obligations under the *PCMLTFA*.[242]

In addition, FINTRAC operates a call centre to answer general inquiries about FINTRAC's operations, as well as more specific questions about reporting requirements.[243] In 2006-07, information officers answered 3,206 inquiries and the FINTRAC website received more than 600,000 "hits."[244] The website contains guidance on several topics for reporting entities and the public. In addition, FINTRAC employees publish articles in trade journals and newsletters.[245]

FINTRAC also has on its website a section for "Feedback on reporting," where several topics are explored, such as suspicious transactions in the banking sector.[246] The section offers several examples of typologies.

3.2.7.3 Views of Private Sector Reporting Entities about the Anti-TF Program

This Commission used various tools to learn the views of parties involved in the current anti-TF program. These included a survey of a group of private sector reporting entities conducted by the Deloitte consultancy. Deloitte asked a selection of reporting entities from across Canada for their observations about the anti-TF program. The survey was designed to provide a snapshot of views by sector. Two aspects of the Deloitte report warrant particular mention:

- The report was not intended to serve as hard evidence of the deficiencies of the anti-TF program. It was to be seen as an advisory report on various themes to inform the Commission, and as an opportunity for the Commission to receive other views; and
- The financial services sector received particular attention, since banks provide most of the financial transaction reports submitted to FINTRAC.

The Deloitte report raised several issues facing the private sector reporting entities. The issues are summarized below.

---

241 FINTRAC 2008 Annual Report, p. 16.
242 FINTRAC 2008 Annual Report, p. 4.
243 Department of Finance Memorandum of Evidence on Terrorist Financing, para. 4.33.
244 FINTRAC 2007 Annual Report, p 28. The FINTRAC 2008 Annual Report provided no statistics on this point.
245 Exhibit P-233, Tab 23: FINTRAC, "Overview of Canada's Financial Intelligence Unit – FINTRAC," CFE Ottawa Chapter Professional Development Day, October 18, 2006, p. 11.
246 Online: Financial Transactions and Reports Analysis Centre of Canada <http://www.fintrac.gc.ca/publications/general-general-eng.asp#1> (accessed October 3, 2008).

A. Lack of Understanding of the Distinction between Money Laundering and TF[247]

The report concluded that private sector reporting entities lack an understanding of how terrorist organizations fund their operations. The report noted that very few practical examples of TF have been provided to reporting entities,[248] although FINTRAC and other bodies have identified the indicators that should lead a reporting entity to prepare an STR in TF matters.

B. Lack of Prominence of the TF Issue

Representatives from some reporting entities who were interviewed by Deloitte suggested that TF and terrorism in general do not appear to be a concern in Canada. One representative offered an explanation:

I mean quite frankly the threat of terrorism, although we hear about it and we talk about it to some degree as a Canadian entity, it's not that high a profile. I think because nothing's happened in the country yet, that's my personal belief.[249]

C. Lack of Feedback from FINTRAC to Reporting Entities[250]

According to Deloitte, reporting entities viewed their information as being sent on a one-way trip to FINTRAC. At present, said one interviewee, "…it's difficult to keep staff motivated and interested in screening for [terrorism property matches] without them feeling that they're contributing to something."[251] The report continued:

> Those interviewed would like to see more feedback from FINTRAC in terms of whether or not their reporting is assisting, is useful and is of a benefit based on the time, effort, energy and cost that each institution expends to comply with the legislation.[252]

The lack of feedback also meant that reporting entities did not know whether they should continue to do business with some of their clients whose activities they had reported. One representative stated:

> One of the things we asked ourselves was, okay, well if we've identified suspicious activity and we report it and then it happens again and we report it again… at what point…do

247 Exhibit P-241, Tab 2: Deloitte, Report of Findings as a Result of the Interviews of Regulated Entities on the Topic of Terrorist Financing In, Through and Out of Canada, September 28, 2007, para. 5.1.1 [Deloitte Report on TF].
248 Deloitte Report, para. 5.1.4.
249 Deloitte Report, para. 5.1.12.
250 Deloitte Report, para. 5.1.3.
251 Deloitte Report, para. 5.1.9.
252 Deloitte Report, para. 5.1.3.

> we look at this and say we really shouldn't be or we need to be looking at whether we want to be doing business with this particular firm or client or entity.[253]

The Deloitte report included suggestions for improving feedback from FINTRAC. Some reporting entities expressed interest in more regular contact with the agencies responsible for national security matters – the RCMP and CSIS.[254]

FINTRAC does face some constraints in providing feedback. FINTRAC cannot provide feedback on the results its use of the information that reporting entities provide. Another reason invoked for restricting feedback is the possibility of alerting the individuals or groups being investigated.[255] As well, FINTRAC receives so many reports that it would be impossible to follow up with reporting entities on each report, even if it wanted to.

FINTRAC believed that its current approach of providing guidance, but not feedback, was appropriate. Mark Potter of FINTRAC testified that FINTRAC spends considerable time providing "feedback" (more like guidance) to the private sector:

> [W]e spend a lot of time providing feedback to the reporting entities, their associations and individual members on the quality of reports we're seeing, how they can improve, ways we can work better with them in implementing system changes, ensuring that they have sufficient lead time to change their IT systems if necessary, getting their views on what are the best means to provide the reports to us….[256]

Potter could not say whether it would be more effective if FINTRAC had the discretion to advise reporting entities on how their information was applied:

> I'm not sure. I think I'd step back and ask: What is the objective here? And if the objective is to get consistent, high quality reporting from these entities there are other ways we can achieve that objective, giving them some sort of feedback on their individual forms that they provide and the reports they provide to us and providing general feedback on the results of the initiative broadly.[257]

---

253 Deloitte Report, para. 5.1.3.
254 Deloitte Report, para. 5.1.5.
255 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6987.
256 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6986.
257 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6988.

D. Costs of Complying with the PCMLTFA

Private sector reporting entities bear the cost of reporting to FINTRAC. The federal government considers this appropriate.[258] It also appears to be in line with the current FATF policy.

Some reporting entities examined in the Deloitte report argued that complying with the *PCMLTFA* was costly.[259] One called for federal government financial assistance to help all entities acquire appropriate technologies,[260] especially since this would help them comply more effectively with the *PCMLTFA* and because they are doing this for the government's benefit.

Some reporting entities also wanted a "level playing field" for reporting entities and "broadly similar compliance obligations" as banks in other countries.[261] They wanted all private sector entities to be required to submit reports to FINTRAC. They complained that the obligations imposed on them were sometimes not applied to other types of reporting entities.[262] They spoke of gaps in coverage by the *PCMLTFA*: "white label" ATMs (ATMs that are not affiliated with a bank), money services businesses (MSBs), provincial mortgage brokers, pre-paid credit cards, stored value cards, Internet clearing houses such as PayPal, Internet gaming, precious metals, the legal profession and various religious communities.[263]

Several of the problems with gaps in coverage were corrected by Bill C-25 or are currently being reviewed. For example, MSBs and precious metals dealers are now covered by the *PCMLTFA*. The federal government is weighing options for white label ATMs and stored value and pre-paid cards.

E. Ineffectiveness of the Listing System

Some reporting entities complained that the lists of individuals identified as being associated with terrorism contained little biographical data beyond individuals' names. The entities claimed that this produced many false matches when an individual's name was similar to that of someone on the list, and that this in turn created much additional work for the entities, with no corresponding benefit.[264] Some entities also believed that having to report on "politically-exposed persons" (PEPs) would increase their workload. The FATF defines PEPs as "…individuals who are or have been entrusted with prominent public functions such as Heads of State, senior politicians, senior government, judicial or military

---

258 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6985.
259 Deloitte Report, para. 5.1.8.
260 Deloitte Report, para. 5.1.16.
261 Deloitte Report, para. 5.1.10; Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6985.
262 Deloitte Report, para. 5.1.11.
263 Deloitte Report, para. 5.1.11.
264 Deloitte Report, para. 5.1.9.

officials, senior executives of state-owned corporations and important political party officials."[265]

Many reporting entities criticized the listing process. However, many names that appear on the lists used in Canada are not entirely its responsibility. For example, the *United Nations Al-Qaida and Taliban Regulations*[266] (UNAQTR) listings are made by the United Nations Security Council and then adopted by Canada through regulation.

One interviewee noted that, since the lists were public, there was little chance that a listed individual would open a bank account using a name as it appeared on a list.[267] For that reason, the lists were of little value. Their only benefit could be rapid checks by reporting entities immediately after the listing of an individual, but before the individual learned of the addition of their name to the list. However, despite its limitations, Canada is bound by international instruments to participate in the listing process.[268]

This concern about the utility of the listing process in dealing with suspect individuals did not apply to the *Criminal Code*[269] list, which identifies terrorist groups, not individuals.

F. Other Issues

One reporting entity called for financial entities to increase the exchange of information about money laundering and TF.[270] Some entities, aware that charitable organizations can be used to finance terrorist activity, believed that such organizations should be more actively monitored.[271]

---

265 Department of Finance, *Enhancing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime*, Consultation Paper, June 2005, p. 12, online: Department of Finance <http://www.fin.gc.ca/activty/pubs/enhancing_e.pdf> (accessed October 2, 2008). The Consultation Paper continues: "While the FATF Recommendation focuses on foreign PEPs, countries are increasingly expanding the coverage of their regimes to both foreign and domestic PEPs, in line with the requirements of the United Nations Convention against Corruption and other international agreements. There is international concern, particularly for some foreign jurisdictions, that PEPs constitute higher risk customers for financial institutions and intermediaries as they have potentially greater opportunities to engage in corrupt activities, and Canada will do its part in the global fight against corruption. To prevent the laundering of the proceeds of corruption, financial institutions and intermediaries should take additional steps to identify customers that are PEPs and apply enhanced due diligence measures."

266 S.O.R./99-444.

267 Deloitte Report, para. 5.1.9.

268 For other criticisms of the listing regime (from an international standpoint), see Koh, *Suppressing Terrorist Financing and Money Laundering*, pp. 103-106.

269 R.S.C. 1985, c. C-46.

270 Deloitte Report, para. 5.1.16.

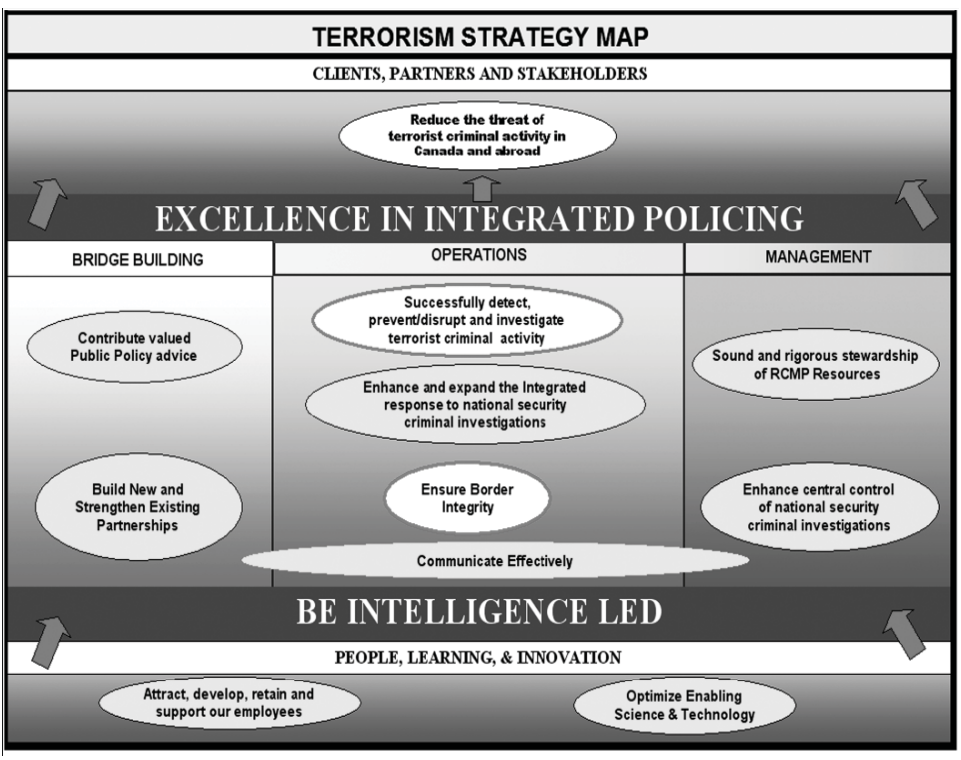
271 Deloitte Report, para. 5.1.13.

3.3 Royal Canadian Mounted Police

3.3.1 Roles, Goals and Structure

As an agency in the portfolio of the Minister of Public Safety, the RCMP acts as Canada's national police force and as a contract provincial or local police force in several Canadian provinces, territories, municipalities and aboriginal communities.[272] The RCMP is considered to be the "default" law enforcement agency in TF matters.

A recent RCMP publication estimates that "…[a]s many as 50 terrorist organizations are present in some capacity in Canada, involved in a range of activities that include fundraising (with money sent abroad to finance terrorist efforts), weapons procurement, and human and commodity trafficking."[273] The RCMP considers terrorism to be a priority. The RCMP's terrorism strategy is summarized in the following chart[274] from its 2008-09 Report on Plans and Priorities:



272 According to the RCMP's website, the RCMP provides a total federal policing service to all Canadians and policing services under contract to the three territories, eight provinces (except Ontario and Quebec), more than 190 municipalities, 184 aboriginal communities and three international airports: online: <http://www.rcmp-grc.gc.ca/about-ausujet/index-eng.htm> (accessed December 3, 2007).

273 Royal Canadian Mounted Police, *Royal Canadian Mounted Police Report on Plans and Priorities 2008-2009*, p. 47, online: Treasury Board Secretariat of Canada <http://www.tbs-sct.gc.ca/rpp/2008-2009/inst/rcm/rcm-eng.pdf> (accessed June 3, 2009) [RCMP 2008-09 Report on Plans and Priorities].

274 RCMP 2008-09 Report on Plans and Priorities, p. 48. A chart dealing with the Economic Integrity Strategy is found at p. 57.

The RCMP participates in the federal government's AML/ATF Initiative. The 2008 FATF Mutual Evaluation of Canada describes the RCMP's involvement in national security and TF matters:

> 469. The RCMP has an integrated model for responding to National Security Investigations (NSI), which forms part of the overall Public Safety Anti-Terrorism (PSAT) initiative. The NSI centrally coordinates and directs all national security investigations, intelligence and policy. At the operational level in each province of Canada, NSI serves as the policy centre for the Integrated National Security Enforcement Teams (INSETs) and the National Security Investigation Sections (NSIS).
>
> 470. The NSI includes a unit in Ottawa called the Anti-Terrorist Financing Team which consists of the RCMP and CRA. The team is responsible for (1) monitoring and coordinating major ongoing investigational projects related to terrorist organizations focusing primarily on their financial and procurement infrastructures and (2) liaising on a routine basis with partner agencies such as FINTRAC, CSIS and CRA Charities Directorate. The unit has also hosted terrorist financing courses in 2005 and 2006.
>
> 471. National Security Operations Branch (NSOB) supports and coordinates all national security field operations by reviewing, analyzing and disseminating information from all sources, including international partners, the CSIS, third parties and RCMP field investigations. NSOB also prepares subject profiles, case briefs and briefing notes for senior management, ensures compliance with RCMP policy, and tasks RCMP liaison officers in support of RCMP National Security investigations.
>
> 472. The Anti-Terrorist Financing Team (ATFT) supports counter-terrorism strategies with respect to financial intelligence investigations, enforcement, and the listing process in respect to Terrorist Entities.[275]

The RCMP created an Anti-Terrorist Financing Task Force in October 2001, making the Task Force permanent under its Financial Intelligence Branch in April 2002:

> This intelligence/investigative body was established to support national security efforts to identify financial intelligence and enforcement opportunities related to terrorist financing, as well as to provide direction and support to field units. An Internet investigation team was established as part of the branch to investigate terrorist fundraising on the Internet.[276]

---

275 2008 FATF Mutual Evaluation of Canada, paras. 469-472.
276 Department of Finance Memorandum of Evidence on Terrorist Financing, p. 36.

Since October 2006, RCMP responsibilities in TF matters have fallen under the National Security Investigations Branch (NSI). The NSI is supervised by its own Assistant Commissioner, who reports to the Deputy Commissioner, Operations.[277] One component of the NSI, the Anti-Terrorist Financing Team (ATFT), is dedicated to TF matters. The tasks of the ATFT are as follows:

- Monitor and coordinate major national security ongoing investigations (and projects) in terrorist matters, more specifically on the financing and procurement sides;[278]
- make recommendations based on the analysis of financial information received from various sources in matters related to TF offences;
- liaise with other anti-TF partners in Canada;[279]
- support the listing process.[280]

The ATFT consists of the RCMP and the CRA.[281] The RCMP also sends liaison officers to some countries to assist in the fight against money laundering and TF, and to perform other roles.[282]

3.3.2 Activities Aimed at Fighting TF

For about 18 months after TF offences appeared in the *Criminal Code* in late 2001, RCMP activity on terrorism matters as a whole remained focused on preventing attacks[283] rather than on "following the money." RCMP Superintendent Reynolds testified that this was because it takes time after legislation is adopted to put resources in place and to do investigations and gather evidence.[284]

Superintendent Reynolds also testified that the RCMP saw TF investigations as "highly complex" and lengthy. Simply gathering the evidence in a single case could take three years.[285] He stated that every significant national security investigation includes a TF component.[286] TF investigations address matters such as raising and moving funds and the procurement of materials.[287] As of March 31, 2006, there were 90 active intelligence investigations and four major project investigations with respect to TF.[288]

---

277 Exhibit P-230, Tab 2: RCMP Organizational Chart.
278 2008 FATF Mutual Evaluation of Canada, para. 470. The FATF Mutual Evaluation contains a description of the structure of the RCMP and other law enforcement agencies in regard to TF matters: see paras. 460-480
279 2008 FATF Mutual Evaluation of Canada, para. 470.
280 2008 FATF Mutual Evaluation of Canada, para. 472.
281 2008 FATF Mutual Evaluation of Canada, para. 470.
282 2008 FATF Mutual Evaluation of Canada, paras. 179, 1554.
283 This is also described as "chasing the bomber."
284 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6819.
285 Testimony of Rick Reynolds, vol. 55, October 1, 2007, pp. 6819-6820.
286 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6823.
287 Testimony of Rick Reynolds, vol. 55, October 1, 2007, pp. 6820-6821.
288 *Royal Canadian Mounted Police Departmental Performance Report for the period ending March 31, 2006*, p. 62, online: Treasury Board of Canada Secretariat <http://www.tbs-sct.gc.ca/dpr-rmr/2005-2006/rcmp-grc/rcmp-grc-eng.pdf> (accessed May 13, 2009).

When the RCMP receives information or intelligence relating to TF, it first determines whether a criminal investigation is warranted.[289] In all TF investigations, RCMP Headquarters provides direction, international liaison, and central coordination with other agencies such as CRA and FINTRAC.[290] Investigative teams gather the necessary intelligence.[291] The RCMP also relies to a great extent on Integrated National Security Enforcement Teams (INSETs) to investigate TF cases. The work of the INSETs is described later in this chapter.

Reynolds testified that the priority of the RCMP in TF investigations is always to prevent the loss of life, and that prevention and disruption of terrorist activities as a whole are by-products of TF investigations.[292] He testified that, although disruption can prevent individual terrorist incidents, it does not stop the desire to raise funds.[293] Reynolds explained that another key goal of investigations is to understand the reach and capacity of organizations and identify the persons involved with the activities.[294]

Significant resources are devoted to the investigation of potential TF offences.[295] Reynolds identified two main areas of concern: (i) micro-financing in respect of operations in support of individual terrorist actions and (ii) macro-financing to support certain organizations. He testified that investigations cannot be focused solely on the "bomber" (the terrorist act). They must focus as well on the larger organization behind the terrorist act.[296] He stated that the RCMP does not have the capacity to investigate all potential TF matters.[297]

The RCMP also provides information to the CRA to help the Charities Directorate review applications for charitable status and assess whether existing charities comply with the *Income Tax Act*.[298]

The RCMP is the main recipient of FINTRAC's disclosures of designated information.[299] The *PCMLTFA* does not specifically require FINTRAC to disclose information to the RCMP, requiring disclosure only to "the appropriate police force."[300] However, the *Criminal Code* specifically identifies the RCMP when setting out the obligations of reporting entities. These entities must disclose to the RCMP Commissioner the existence of property in their possession that is connected to a terrorist group.[301]

289 Department of Finance Memorandum of Evidence on Terrorist Financing, p. 36.
290 Testimony of Rick Reynolds, vol. 55, October 1, 2007, pp. 6825-6826.
291 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6890.
292 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6823.
293 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6824.
294 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6823.
295 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6880.
296 Testimony of Rick Reynolds, vol. 55, October 1, 2007, pp. 6827-6828.
297 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6839.
298 Department of Finance Memorandum of Evidence on Terrorist Financing, p. 36; FINTRAC 2008 Annual Report, p. 11.
299 According to the Department of Finance, "The RCMP, through its money laundering and terrorist financing units, is the major recipient of disclosures from FINTRAC": Department of Finance Memorandum of Evidence on Terrorist Financing, p. 36.
300 *PCMLTFA*, s. 55(3)(a).
301 *Criminal Code*, s. 83.1(1).

As well, in both money laundering and TF matters, the RCMP receives information from the CBSA, private sector reporting entities, other RCMP units, CSIS,[302] foreign partners and the public.[303]

The RCMP is involved in training and raising awareness among AML/ATF Initiative partners and the private sector, as well as police forces abroad. The Department of Finance Memorandum on Terrorist Financing noted that "…the RCMP has provided direct technical assistance and training to police forces in developing countries to help them conduct anti-money laundering and anti-terrorist financing investigations and enhance their investigative techniques."[304] The ATFT also offers a course on TF,[305] including Internet TF.

The RCMP participates in several domestic and international groups dealing with TF matters, such as the Financial Action Task Force, the G8 Law Enforcement Projects Subgroup (Roma/Lyon Group), the International Working Group on Terrorist Financing, the Terrorist Financing Working Group of the Canadian Bankers Association, the Five Eyes Terrorist Financing Working Group, and the Bi-lateral (US-Canada) Anti-Terrorist Financing Working Group.[306]

3.3.3 Resources

Superintendent Reynolds testified that in 2001 the RCMP had projected a need for about 126 individuals to cover both intelligence and investigations.[307] That year, the RCMP acquired 17 positions for TF matters, of which three were assigned to three separate INSETs and 14 were assigned to RCMP Headquarters in Ottawa. Existing personnel in some INSETs were taken off other duties and assigned to TF matters. In 2006, the RCMP received additional funding. As a result, 33 new positions were created, for a total of 50 positions on TF matters.[308]

According to Reynolds, the resources challenge extended beyond proper funding. It took time to develop employees with the required skills for TF investigations. There were also problems with retaining employees because of competition for the same candidates within the private and public sectors. As well, not everyone in law enforcement was attracted to financial investigations.[309] Reynolds testified that "court time" also took time away from investigations:

> So, there has been an increase in the amount of court time, which isn't criticism by any standpoint but bearing in mind, as we spend more time authoring court processes, defending court processes or providing disclosure and responsibility to it,

---

302 *Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C-23, s. 19(2)(a) [CSIS Act].
303 Department of Finance Memorandum of Evidence on Terrorist Financing, p. 36.
304 Department of Finance Memorandum of Evidence on Terrorist Financing, p. 37.
305 2008 FATF Mutual Evaluation of Canada, para. 470.
306 Exhibit P-383, Tab 7: Description of RCMP's Anti-Terrorist Financing Team.
307 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6838.
308 Testimony of Rick Reynolds, vol. 55, October 1, 2007, pp. 6824-6825.
309 Testimony of Rick Reynolds, vol. 55, October 1, 2007, pp. 6838-6841, 6892-6893.

> that of course reduces the amount of time that could be spent on investigations.[310]

The FATF addressed RCMP resources in its 2008 Mutual Evaluation of Canada:

> [T]he RCMP lacks the resources that would allow it to focus on a larger spectrum of ML/TF investigations. The RCMP acknowledges that, due to resources constraints, it essentially dedicates its resources to large and complex ML investigations related to organised crime groups.[311]

The dissenting opinion of two MPs, Joe Comartin and Serge Ménard, who sat on the House of Commons subcommittee that reviewed the *Anti-terrorism Act* in 2007, described the importance of "operations" – intelligence and law enforcement efforts:

> Terrorism cannot be fought with legislation; it must be fought through the efforts of intelligence services combined with appropriate police action. ...Therefore, one cannot expect that new legislation will provide the tools needed to effectively fight terrorism. Legislation can, however, be amended if police do not seem to have the legal means needed to deal with the new threat of terrorism.[312]

Bromley emphasized in a paper for the Commission the need for law enforcement and other authorities to ask intuitive questions instead of relying on the analysis of complicated data.[313] Quiggin testified in support of being "on the ground" and on the front lines through community engagement.[314]

---

310 Testimony of Rick Reynolds, vol. 55, October 1, 2007, pp. 6842-6843.

311 2008 FATF Mutual Evaluation of Canada, para. 517. See also 2008 FATF Mutual Evaluation of Canada, para. 468.

312 House of Commons Canada, Final Report of the Standing Committee on Public Safety and National Security, Subcommittee on the Review of the *Anti-terrorism Act, Rights, Limits, Security: A Comprehensive Review of the Anti-terrorism Act and Related Issues*, March 2007, p. 116, online: Parliament of Canada <http://www2.parl.gc.ca/content/hoc/Committee/391/SECU/Reports/RP2798914/sterrp07/sterrp07-e.pdf> (accessed May 25, 2009).

313 Blake Bromley, "Funding Terrorism and Charities," October 26, 2007, online: Benefic Group <http://www.beneficgroup.com/files/getPDF.php?id=120> (accessed May 12, 2009), p. 9.

314 Testimony of Thomas Quiggin, vol. 91, December 7, 2007, p. 12078. Quiggin stated that, "... in order to be effective in counterterrorism intelligence, you have to be literally on the ground with the people involved right out at the front lines; that means community engagement….If you have good community engagement programs, if you're out working with people on the street day by day by day, you will be able to identify who the perpetrators are, who the radicals are."

3.4 Canadian Security Intelligence Service (CSIS)

3.4.1 Role, Goals and Structure

CSIS is a civilian intelligence agency, established in 1984 and governed by the *Canadian Security Intelligence Service Act (CSIS Act)*.[315]

CSIS investigates threats to the security of Canada, analyzes information and reports to and advises the Government of Canada about those threats. The CSIS website identifies the key threats that it investigates: terrorism, the proliferation of weapons of mass destruction, espionage, foreign interference and cyber-tampering affecting critical infrastructure.[316] Terrorism is its main priority.[317] Neither the definition of "threats to the security of Canada" in the *CSIS Act* nor the description of the key threats investigated by CSIS specifically mention TF, but TF clearly forms part of the work of CSIS.[318] As noted earlier in this chapter, FINTRAC has concluded that the definition of "terrorist activity financing offence" in the *PCMLTFA* comes within the definition of "threats to the security of Canada" in the *CSIS Act*.[319]

The ATA required FINTRAC to make disclosures to CSIS about threats to the security of Canada, whereas, before 2001, FINTRAC was focused solely on money laundering.[320]

The increase in concern about TF led CSIS to create a Terrorist Financing Unit (TFU) within its Counter Terrorism Branch in 2002, although CSIS had done some work on TF issues before then.[321] The mandate of the TFU is to identify and track financial structures which support terrorist organizations and to be a source of reliable intelligence for the Government of Canada.[322] A Security

---

315 Canadian Security Intelligence Service, "History of CSIS," online: Canadian Security Intelligence Service <http://www.csis-scrs.gc.ca/hstrrtfcts/index-eng.asp> (accessed September 15, 2009).

316 Online: <http://www.csis-scrs.gc.ca/bts/rlfcss-eng.asp> (accessed July 28, 2008). For more information on the various roles and responsibilities of CSIS, see the several backgrounder documents available online: <http://www.csis-scrs.gc.ca/nwsrm/bckgrndrs/index-eng.asp> (accessed August 8, 2008).

317 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6912; Canadian Security Intelligence Service, "Backgrounder No. 8 – Counter-Terrorism," online: Canadian Security Intelligence Service <http://www.csis-scrs.gc.ca/nwsrm/bckgrndrs/bckgrndr08-eng.asp> (accessed August 6, 2008) [CSIS Backgrounder on Counter-Terrorism], which states that: "Ensuring the safety and security of Canadians is one of the Government of Canada's most important responsibilities. With this in mind, the government has identified counter-terrorism as the Canadian Security Intelligence Service (CSIS) number one priority."

318 Canadian Security Intelligence Service, *Public Report 2005-2006*, p. 5, online: Canadian Security Intelligence Service <http://www.csis-scrs.gc.ca/pblctns/nnlrprt/2005/rprt2005-eng.pdf> (accessed July 28, 2008).

319 Second FINTRAC Response to Supplementary Questions of the Commission, Question 1(d).

320 *PCMLTFA*, s. 55.1. Jim Galt of CSIS testified that "Money laundering is not part of CSIS mandate. It's a criminal matter. If it came to our attention we'd immediately draw it to the attention of the RCMP but it's not something that we look at. It's not our -- as I say, it's not our mandate.": Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6921.

321 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6939.

322 Exhibit P-232, Tab 2: Security Intelligence Review Committee, *Review of the CSIS Investigation of Terrorist Financing Activities in Canada* (SIRC Study 2004-10), August 5, 2005, p. 5 [SIRC Study 2004-10].

Intelligence Review Committee (SIRC) study of a CSIS investigation of TF noted that, in 2002-03, a ministerial directive for the first time specifically directed CSIS to investigate and advise the Government of Canada about the threat arising from TF.[323] The same SIRC study noted that the growing international focus on TF created the need for CSIS to focus more specifically on TF and to develop a level of expertise and continuity in this area.[324]

In May 2006, in a reorganization of CSIS operational branches, the TFU was moved from the Counter Terrorism Branch to the Human Sources/Operational Support Branch and renamed the Financial Analysis Unit (FAU).

The SIRC study described the CSIS approach to TF issues:

> In February 2003, CSIS HQ issued a directional statement to explain the nature and objectives of the investigation into terrorist financing. According to this statement, its primary purpose was to collect and assess information in order to provide the Government of Canada with reliable intelligence on the extent and nature of terrorist financial support efforts in Canada, to provide assistance as required to law enforcement organizations, to respond as required under the [*Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism*] and the *Anti-Terrorism Act*, and to fulfill other international commitments. The investigation was intended "to deter and disrupt the flow of funds to terrorists, thus hindering their ability to mount operations."[325]

3.4.2 Activities Related to TF

Jim Galt, Director of the FAU at CSIS, testified that the FAU's responsibility is to support the operational branches of CSIS through financial analysis. The FAU is the only unit of its kind at CSIS and it supports three major operational branches.[326] Its mandate is to provide support to investigations with respect to financial aspects, and is not limited to TF.[327] Besides using information in the CSIS database and open source information,[328] the FAU receives reports that are sent to CSIS by private sector entities.[329]

Investigations are run by the operational unit that has conduct of and responsibility for a particular file.[330] The FAU's main responsibility is to view an operational file from a financial perspective to provide the operational branches

---

323 SIRC Study 2004-10, p. 6.
324 SIRC Study 2004-10, p. 9, referencing CSIS Counter Terrorism Program 2003-2004.
325 SIRC Study 2004-10, p. 13.
326 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6907.
327 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6906.
328 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6933.
329 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6927.
330 Testimony of Jim Galt, vol. 55, October 1, 2007, pp. 6906-6908.

with additional investigative leads, identify new targets or direct operational branches in other ways to further an investigation.[331] In his evidence, Galt stated that almost all CSIS operational files had a financial aspect.[332] The FAU brings together all the financial information received from FINTRAC or from regular CSIS investigations. Financial analysts on staff provide analysis of the information to the operational branches.[333] The FAU's work may involve providing an operational branch with a quick analysis of a particular matter. In most cases, however, the FAU's work is part of an ongoing counterterrorism effort.[334]

CSIS sends VIRs, prepared by the FAU, to FINTRAC.[335] Disclosure to FINTRAC was one of the first steps by the FAU after it receives a file.[336] CSIS relies on section 12 of the *CSIS Act* to share information within government.

During fiscal year 2006-07, CSIS sent 30 to 40 VIRs to FINTRAC. In these VIRs, CSIS explains why a particular individual or group is considered a threat to the security of Canada.[337] This helps FINTRAC to prepare its own analysis and its response to the VIR. FINTRAC must disclose "designated information"[338] to CSIS if FINTRAC has reasonable grounds to suspect that the information would be relevant to threats to the security of Canada.[339] CSIS is currently satisfied with the extent and quality of the disclosures from FINTRAC and finds the information it receives more detailed and useful than in the past.[340]

After obtaining approval from the Minister of Public Safety, CSIS can also apply to a judge for a production order requiring FINTRAC to disclose information – for example, information in addition to the designated information FINTRAC must disclose – to facilitate an investigation "in respect of a threat to the security of Canada."[341] CSIS does not maintain statistics on the usefulness of disclosures by FINTRAC. Galt testified that, like the RCMP, the FAU would prefer that the arm's-length relationship with FINTRAC become closer.[342]

Galt testified that the FAU now receives "some of their [FINTRAC's] analysis." There were some compatibility problems between CSIS and FINTRAC technology, leading to a less efficient transfer of information to the CSIS system.[343] At the time of the Commission's hearings, discussions were underway to resolve this.[344]

---

331 Testimony of Jim Galt, vol. 55, October 1, 2007, pp. 6908-6909.
332 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6909.
333 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6909.
334 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6921.
335 *PCMLTFA*, s. 54(a); *CSIS Act*, ss. 12, 19; Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6917.
336 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6941.
337 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6917.
338 For the purposes of disclosures to CSIS, "designated information" is defined in s. 55.1(3) of the *PCMLTFA*.
339 *CSIS Act*, s. 55.1.
340 CSIS Response to Supplementary Questions of the Commission, Question 3.
341 *PCMLTFA*, s. 60.1.
342 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6933.
343 Testimony of Jim Galt, vol. 55, October 1, 2007, pp. 6918-6919.
344 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6919.

One of the main counterterrorism activities of CSIS is to provide information for Canada's listing process. In the process under the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism*,[345] CSIS prepares an assessment for DFAIT and sits on the interdepartmental committee on listings.[346] A CSIS background document on counterterrorism states that, since the creation of the list, CSIS has played a role in the listing of 40 entities, including Al Qaida, the Liberation Tigers of Tamil Eelam (LTTE) and Hezbollah.[347] The FAU itself is not involved in this process.[348]

CSIS also has responsibility for making recommendations to the Minister of Public Safety regarding the issuance of a certificate under the *Charities Registration (Security Information) Act* (CRSIA) process – a process which can lead to denial of eligibility for charitable status or revocation of existing charitable status.[349]

The SIRC study mentioned above noted that efforts to combat TF required cooperation with domestic partners and that partners depended on CSIS for their enforcement actions. The study further stated that CSIS worked most closely with FINTRAC and the CRA's Charities Directorate in this regard.[350] CSIS "liaised and cooperated closely with CRA in ongoing efforts to prevent the exploitation of registered Canadian charities to finance terrorist activity."[351] In fact, CRA often consults with CSIS before granting registered charity status, and Galt testified that CSIS would become involved as well in the process of issuing certificates under CRSIA.[352] The SIRC study stated that it had reviewed all CSIS exchanges of information with domestic partners and found that "with the exception of a few omissions in the use of tracking codes, they complied with the *CSIS Act*, Ministerial Direction, operational policy and relevant MOUs."[353]

SIRC also noted that CSIS respected its legal obligations, policies and MOUs in its dealings with foreign partners. SIRC observed that CSIS, during the period of its investigation, cooperated with more than 35 foreign partners on TF issues and that it gathered information on foreign legal frameworks that were aimed at fighting TF. CSIS representatives also attended several international conferences and presentations on TF.[354]

---

345 S.O.R./2001-360.
346 SIRC Study 2004-10, pp. 20-21.
347 CSIS Backgrounder on Counter-Terrorism.
348 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6927.
349 *A New Review Mechanism for the RCMP's National Security Activities*, p. 190. The RCMP also makes recommendations to the Minister.
350 SIRC Study 2004-10, p. 15.
351 SIRC Study 2004-10, p. 17.
352 Testimony of Jim Galt, vol. 55, October 1, 2007, pp. 6929-6930, 6865.
353 SIRC Study 2004-10, p. 18.
354 SIRC Study 2004-10, p. 19.

3.4.3 Resources

When Galt testified before the Commission, the FAU had four permanent and three "borrowed" employees, occupied as follows:

- head;
- two contractual financial analysts (a chartered accountant and an RCMP officer formerly with the Integrated Proceeds of Crime unit);
- one individual seconded from CRA; and
- three intelligence officers.[355]

A tactical analyst position was not filled, at least in part because of a shortage of resources.[356] CSIS as a whole had 2,449 full-time employees as of March 31, 2007.[357] Galt testified that resources were a significant challenge[358] and that he would have liked to see the FAU's resources doubled or tripled.[359] The lack of resources was limiting the service that the unit could provide:

> [W]e are not able at this point to take on all operational files within the Service, mainly because of resourcing issues. So we have – we have gone through an exercise of creating a priority list of operational files that we look at, and with more resources obviously, I could expand that list. So resources are always an issue.[360]

CSIS made a request for 13 additional positions in 2008 to deal specifically with TF issues that had arisen since 2006. In addition, the February 2008 federal budget provided $10 million between 2008-09 and 2009-10, to be shared by CSIS and CRA for their anti-TF efforts. CSIS stated that it will consider itself adequately financed on anti-TF matters if planned funding allocations are implemented.[361]

3.5 Canada Border Services Agency

3.5.1 Role, Goals and Structure

The Canada Border Services Agency (CBSA), in the portfolio of the Minister of Public Safety, was created through a merger of departments. Since 2003, the

355 Testimony of Jim Galt, vol. 55, October 1, 2007, pp. 6909-6910.
356 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6915.
357 Canadian Security Intelligence Service, *Public Report 2006-2007*, p. 6, online: Canadian Security Intelligence Service <http://www.csis-scrs.gc.ca/pblctns/nnlrprt/2006/rprt2006-eng.pdf> (accessed June 3, 2009).
358 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6922.
359 Testimony of Jim Galt, vol. 55, October 1, 2007, pp. 6910-6911.
360 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6910.
361 CSIS Response to Supplementary Questions of the Commission, Question 1(b); Department of Finance, *The Budget Plan 2008, Responsible Leadership*, pp. 138, 140, online: Department of Finance <http://www.budget.gc.ca/2008/pdf/plan-eng.pdf> (accessed September 18, 2009). The budget allocation was intended to "bolster existing capacities": p. 138.

CBSA has included the customs component of the former Canada Customs Revenue Agency, the enforcement/intelligence component of Citizenship and Immigration Canada and the enforcement component of the Canadian Food Inspection Agency. The *Canada Border Services Agency Act* [362] (*CBSA Act*) sets out the mandate of the CBSA, which includes the following:

> …providing integrated border services that support national security and public safety priorities and facilitate the free flow of persons and goods, including animals and plants, that meet all requirements under the program legislation, by
>
> (a) supporting the administration or enforcement, or both, as the case may be, of the program legislation…
>
> … and
>
> (e) providing cooperation and support, including advice and information, to other departments and agencies of the Government of Canada to assist them in developing, evaluating and implementing policies and decisions in relation to program legislation for which they have responsibility.[363]

The FATF Special Recommendations on Terrorist Financing call for countries to have "…measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including a declaration system or other disclosure obligation." Furthermore, "…[c]ountries should ensure that their competent authorities have the legal authority to stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering, or that are falsely declared or disclosed."[364]

Separate divisions of the CBSA deal with enforcement, intelligence and policy development. The activities and responsibilities of these divisions in TF matters are outlined below.

3.5.2 CBSA Activities

3.5.2.1 In General

CBSA's responsibilities in relation to terrorism and TF are to gather and disseminate intelligence in support of the administration and enforcement

---

362 S.C. 2005, c. 38.

363 *Canadian Border Services Agency Act*, S.C. 2005, c. 38, s. 5(1).

364 See Special Recommendation IX of the FATF's "9 Special Recommendations (SR) on Terrorist Financing (TF)," online: Financial Action Task Force <http://www.fatf-gafi.org/document/9/0,3343,en_32250379_32236920_34032073_1_1_1_1,00.html#IXCashcourriers> (accessed February 11, 2009). The FATF has also published interpretive notes and best practices to help countries put in place the necessary regulations.

of the applicable rules regarding cross-border movements of currency and individuals.[365] The CBSA is also in charge of the *Immigration and Refugee Protection Act* process involving foreign nationals or permanent residents who may have been involved in criminal activities such as TF, or who may pose a threat to the security of Canada.[366] In short, the CBSA has two main "business lines" relating to terrorism and TF:

- detecting and monitoring the cross-border movement of currency and monetary instruments; and
- preventing the entry into Canada of persons who are not admissible because they may have been involved in terrorism or TF.[367]

Border Services Officers (BSOs) are trained to identify suspicious individuals as well as those who may be hiding contraband.[368] The CBSA also uses "sniffer dogs" that can detect money,[369] as well as scanners and other sophisticated equipment[370] – technologies recently acquired in the fight against terrorism.[371] The Borders Enforcement Division of the CBSA provides guidance to BSOs in their anti-TF activities. Denis Vinette, Director of the CBSA Borders Enforcement Division, testified about how CBSA attempts to identify illegal activity among the large volume of individuals and vehicles entering Canada:

> [We use] information we have in advance, either through our intelligence program [or] through our partnerships with other individuals, the training, the rigorous training our officers go through to prepare them to try and find those anomalies, either within individual behaviours, within documents, within patterns or trends…to try and deal with [the] significant challenge of finding that needle in the haystack.[372]

CBSA employees receive extensive training, including from the RCMP.[373] Instead of creating a single unit charged with pursuing money laundering and TF, the CBSA has trained its 7,200 BSO officers across the country to deal with these matters.[374] As a result, Vinette testified, "…[w]e didn't get 40 or 50 or 100 resources that solely worked on this. We get the benefit of 7000."[375]

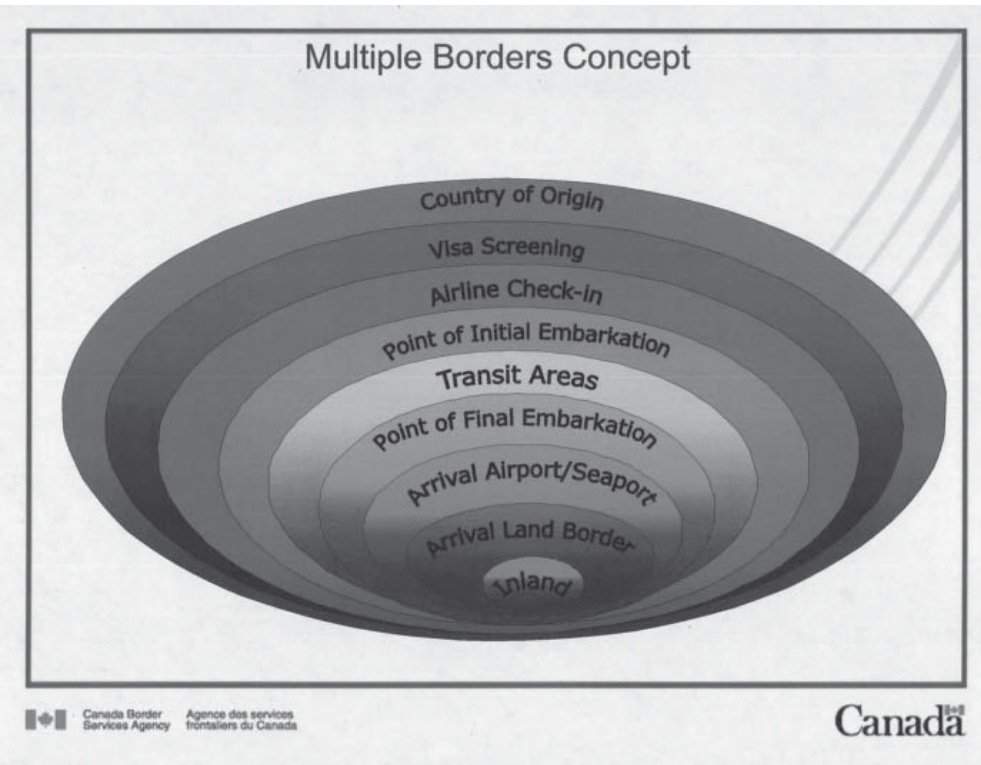
365 Testimony of Tyson George, David Quartermain and Denis Vinette, vol. 56, October 2, 2007, pp. 7033-7035.
366 Testimony of Tyson George, vol. 56, October 2, 2007, pp. 7033, 7052-7053. See also the Department of Finance Memorandum of Evidence on Terrorist Financing, p. 37.
367 Testimony of David Quartermain, vol. 56, October 2, 2007, p. 7053.
368 Testimony of Denis Vinette, vol. 56, October 2, 2007, p. 7036.
369 Testimony of Denis Vinette, vol. 56, October 2, 2007, p. 7084.
370 2008 FATF Mutual Evaluation of Canada, para. 585.
371 For examples of the technologies, such as the "Snake Eye Camera" and the "Merlin Density Meter," see 2008 FATF Mutual Evaluation of Canada, para. 588.
372 Testimony of Denis Vinette, vol. 56, October 2, 2007, pp. 7056-7057.
373 2008 FATF Mutual Evaluation of Canada, para. 594.
374 Testimony of Denis Vinette, vol. 56, October 2, 2007, pp. 7043-7044, 7049.
375 Testimony of Denis Vinette, vol. 56, October 2, 2007, p. 7063.

CBSA's Strategic Intelligence Analysis Division has as its sole purpose producing analytical products on a number of topics, including TF and proceeds of crime.[376] CBSA also collaborates with international partners in identifying TF cases.[377]

Within the Intelligence Directorate, the Borders Intelligence Division is charged with providing guidance to intelligence officers in the regions. The Division is the point of contact between headquarters and regional offices on TF matters. It has 44 "migration integrity officers" in 39 countries as well as three intelligence liaison officers overseas.[378]

3.5.2.2 The "Multiple Borders" Concept

The CBSA follows "multiple borders"[379] concept to identify problematic behaviours or activities. This approach affords the CBSA multiple opportunities to identify individuals who may pose some threat to Canada. The concept is illustrated in the following chart[380]:



376 Testimony of David Quartermain, vol. 56, October 2, 2007, p. 7062.
377 Testimony of David Quartermain, vol. 56, October 2, 2007, p. 7062.
378 Testimony of David Quartermain, vol. 56, October 2, 2007, p. 7034.
379 Sometimes abbreviated to "multi borders," and also called a "layered safety net," or the "onion."
380 Exhibit P-235, Tab 7: Multiple Borders Concept Model [Multiple Borders Concept Model].

The outer layer of the "onion" is the country of origin of the person or activity being monitored. There are several components to this "outer layer":

1. CBSA working with Citizenship and Immigration Canada visa officers;
2. CBSA's 44 Migration Integrity Officers, posted in various overseas locations, communicating with airline check-in staff. These officers act as liaison officers with local law enforcement agencies as well as with airline employees;
3. CBSA checking passenger lists (usually when a flight bound for Canada is in the air) against CBSA's database at its Risk Assessment Centre in Ottawa. This step allows CBSA to verify if there is a "look-out" (a mention in CBSA computers) or any other relevant information about a particular individual;
4. CBSA checks at transit areas in Canadian airports;
5. CBSA inspections at Canadian airports; and
6. The Inland Enforcement Program for cases where a potentially inadmissible person has managed to enter Canada.[381]

This layered approach also largely applies to cargo traffic.[382]

There are many ways to inspect cargo and individuals seeking to enter Canada. Still, the sheer volume of individuals and vehicles entering Canada is a key operational challenge for CBSA. As Vinette testified, "…you couldn't inspect every shipment; the border would shut down essentially."[383] As a result, the CBSA must be efficient and creative in minimizing the risks of contraband and ill-intentioned individuals entering Canada.

3.5.2.3 Business Line 1: Cross-border Movements of Currency and Monetary Instruments

Part 2 of the *PCMLTFA*, Reporting of Currency and Monetary Instruments, deals with two components of CBSA's work on cross-border activities – administrative rules governing the process for making declarations when entering Canada, and search and seizure powers.[384]

It is not illegal for an individual entering or leaving Canada to carry money in cash or other instruments, but this must be reported in certain cases. At or above a certain amount (currently $10,000) persons[385] must declare the import

---

381 For a description of the concept, see Testimony of David Quartermain, vol. 56, October 2, 2007, pp. 7057-7060.
382 Testimony of Denis Vinette, vol. 56, October 2, 2007, pp. 7060-7061.
383 Testimony of Denis Vinette, vol. 56, October 2, 2007, p. 7075.
384 Testimony of Denis Vinette, vol. 56, October 2, 2007, p. 7044.
385 The persons are defined in s. 12(3) of the *PCMLTFA* and include mainly exporters and people transporting money.

or export to an officer,[386] usually a BSO.[387] Designated persons must complete reports on both the import and export of currency, including import or export by mail, courier or any means of transportation.[388] CBSA also watches for cross-border movements of gold and precious metals and stones.[389]

Vinette stated that some individuals may understandably be reluctant to report – for example, if they are not familiar with Canada's border control system or come from a country where there is distrust of the authorities.[390] All reports about movements of funds – legitimate or improper – are forwarded to FINTRAC as Cross-Border Currency Reports (CBCRs).[391] FINTRAC then adds the information to its database.

After a report is made, the person entering or leaving Canada must answer any questions posed by the BSO and must present the currency or monetary instruments if the BSO requests.[392]

If a BSO suspects on reasonable grounds that an individual is hiding on or about themselves currency or monetary instruments worth $10,000 or more which has not been reported,[393] the BSO may search a person within a reasonable time after the person arrives in Canada. A BSO may on the same grounds search a person about to leave Canada at any time before the person's departure. BSOs also have the power to stop, board and search any means of transportation to determine if currency or monetary instruments of $10,000 or more are on board and have not been reported.[394] Similar powers exist to search baggage and mail.[395] Documents on concealment methods are circulated regularly, and officers also have access to a database of information and analysis.[396]

---

386 The *PCMLTFA*, at s. 2, defines the term "officer" to have the same meaning as in subsection 2(1) of the Customs Act, R.S.C. 1985, c. 1 (2nd Supp.) [*Customs Act*]. The *Customs Act* defines "officer" as "a person employed in the administration or enforcement of this Act, the *Customs Tariff* or the *Special Import Measures Act* and includes any member of the Royal Canadian Mounted Police."

387 "Monetary instruments" is defined to include stocks, bonds, debentures, treasury bills, bank drafts, cheques, promissory notes, travellers' cheques and money orders, other than warehouse receipts or bills of lading: *Cross-border Currency and Monetary Instruments Reporting Regulations*, s. 1(1). It appears that in around 90% of cases, currency is seized. See 2008 FATF Mutual Evaluation of Canada, para. 603. The Bank of Canada and several financial entities are exempt from reporting: *Cross-border Currency and Monetary Instruments Reporting Regulations*, ss. 15, 15.1; *PCMLTFA*, s. 12(1); *Cross-border Currency and Monetary Instruments Reporting Regulations*, s. 2(1). Section 2 of the Regulations provides that the amount is in Canadian currency or its equivalent and explains how to calculate it. Several exceptions to the reporting rules are specified.

388 *PCMLTFA*, s. 12(3).

389 Under the general provisions of s. 110 of the *Customs Act* and s. 489(2) of the *Criminal Code*. See 2008 FATF Mutual Evaluation of Canada, para. 583.

390 Testimony of Denis Vinette, vol. 56, October 2, 2007, p. 7039.

391 *PCMLTFA*, s. 12(5).

392 *PCMLTFA*, s. 12(4).

393 *PCMLTFA*, s. 15; *Cross-border Currency and Monetary Instruments Reporting Regulations*, s. 2(1).

394 *PCMLTFA*, s. 16(1).

395 *PCMLTFA*, ss. 16(2), 17; Testimony of David Quartermain, vol. 56, October 2, 2007, p. 7041. Officers do not have the authority to open mail that weighs 30 grams or less unless either the addressee or the sender agrees or is present: see *PCMLTFA*, ss. 17(2), 17(3). For other provisions specific to mail, see s. 21 of the *PCMLTFA*.

396 Testimony of David Quartermain, vol. 56, October 2, 2007, p. 7065.

Air passengers arriving from foreign countries must complete a Declaration Card.[397] For outbound flights, CBSA relies on intelligence and random searches on targeted flights where individuals are asked whether they are transporting currency or monetary instruments worth $10,000 or more.[398] Similar controls are in place at other types of border points.

The CBSA allocates a large portion of its time and resources to incoming flights, mainly because couriers might use such flights to bring money into Canada for terrorist purposes. However, the CBSA plays a limited role with departing passengers, so currency or monetary instruments can easily escape detection on flights leaving Canada. Remedying this would require the CBSA to devote as many resources to departing passengers as it does to incoming passengers.

If a BSO has reasonable grounds to believe that reporting obligations were not followed, the currency or monetary instruments may be seized.[399] Various "levels" of seizures are described in CBSA regulations, except for "Level 4" seizures (involving suspected proceeds of crime or TF funds, and the most serious of all seizures), which are described in the *PCMLTFA*. The seizure levels appear below:

397 Examples of declaration cards were entered into evidence: see Exhibit P-235, Tab 4: Declaration Card and Exhibit P-235, Tab 5: Family Declaration Card.

398 2008 FATF Mutual Evaluation of Canada, para. 563.

399 *PCMLTFA*, s. 18(1). Various procedural obligations must be respected, as set out in ss. 18(2)-(4) of the *PCMTLFA*. The Minister of Public Works and Government Services receives the seized currency or monetary instruments: see *PCMLTFA*, s. 22(2).

Level	Circumstances	Prescribed Penalty	Reference
1	In the case of a person or entity who: i. has not concealed the currency or monetary instruments, ii. has made a full disclosure of the facts concerning the currency or monetary instruments on their discovery, and iii. has no previous seizures under the Act [PCMLTFA];	$250	Regulations, section 18 (a)
2	In the case of a person or entity who: i. has concealed the currency or monetary instruments, other than by means of using a false compartment in a conveyance, or who has made a false statement with respect to the currency or monetary instruments, or ii. has a previous seizure under the Act, other than in respect of any type of concealment or for making false statements with respect to the currency or monetary instruments;	$2500	Regulations, section 18 (b)
3	In the case of a person or entity who: i. has concealed the currency or monetary instruments by using a false compartment in a conveyance, or ii. has a previous seizure under the Act for any type of concealment or for making a false statement with respect to the currency or monetary instruments;	$5000	Regulations, section 18 (c)
4	In the case of the officer having reasonable grounds to suspect that the currency or monetary instruments are proceeds of crime within the meaning of subsection 462.3(1) of the *Criminal Code* or funds for use in the financing of terrorist activities.	No specific amount prescribed	PCMLTFA, section 18(2)
"Regulations" refers to the *Cross-border Currency and Monetary Instruments Reporting Regulations*, SOR/2002-412.			

When currency or monetary instruments are seized, the officer who made the seizure must without delay (using a Cross-Border Seizure Report (CBSR)) report the seizure to FINTRAC. The officer must also notify the President of the CBSA.[400] If a foreign national or non-Canadian citizen is suspected of involvement in TF, the file is forwarded to CBSA's Organized Crime Section.[401] After the information is analyzed, the CBSA can request help from law enforcement agencies, CSIS and FINTRAC.[402]

After seizing currency or monetary instruments, the BSO refers to the information available to him or her to determine if the items are proceeds of crime or connected to money laundering or TF. With Level 4 seizures, this determination has already been made before the seizure, since Level 4 seizures occur only if an officer has reasonable grounds to suspect that the currency or monetary instruments are proceeds of crime or funds for use in TF. No subsequent determination is therefore necessary.[403]

The 2008 FATF Mutual Evaluation of Canada reported that, between January 2003 and September 2006, CBSA filed 174,938 CBCRs and 5,322 CBSRs with FINTRAC.[404] About 18 per cent of FINTRAC's disclosures to recipients contained information from a CBCR or CBSR.[405]

Numerous methods are used to smuggle money or goods into Canada.[406] Several were explained to the Commission during the hearings. CBSA's Strategic Intelligence Analysis Division circulates information to help BSOs and other CSBA employees stay current on new concealment methods.[407] Annual seizures are split about evenly between those at land border crossings and those at airports.[408]

Because of the potential seriousness of a Level 4 seizure, BSOs work with CBSA intelligence officers whenever such a seizure occurs.[409] David Quartermain, Director of the Borders Intelligence Division of CBSA's Intelligence Directorate, testified that intelligence officers transfer this information and their analysis to an Integrated Proceeds of Crime Unit (IPOC) within the RCMP. The IPOC may in turn transfer the file to an Integrated National Security Enforcement Team (INSET) or elsewhere in the RCMP if there are suspicions of TF.[410] In all cases

400 *PCMLTFA*, s. 20.
401 2008 FATF Mutual Evaluation of Canada, para. 581.
402 2008 FATF Mutual Evaluation of Canada, para. 581.
403 Testimony of Denis Vinette, vol. 56, October 2, 2007, p. 7045.
404 2008 FATF Mutual Evaluation of Canada, para. 596.
405 2008 FATF Mutual Evaluation of Canada, para. 597.
406 Exhibit P-235, Tab 8: CBSA Currency Concealment Presentation. See also Testimony of Denis Vinette, vol. 56, October 2, 2007, pp. 7054-7055.
407 Testimony of David Quartermain, vol. 56, October 2, 2007, p. 7040.
408 Testimony of Denis Vinette, vol. 56, October 2, 2007, pp. 7054-7055.
409 Testimony of Denis Vinette, vol. 56, October 2, 2007, p. 7045; Testimony of David Quartermain, vol. 56, October 2, 2007, p. 7048.
410 Testimony of David Quartermain, vol. 56, October 2, 2007, p. 7051.

involving a suspicion of money laundering or TF, the information is shared with law enforcement and intelligence agencies, including FINTRAC.[411]

Quartermain stated that amendments introduced by Bill C-25 helped address "…some of the information-sharing issues that [CBSA] had identified as gaps" with FINTRAC and other partners:

> [I]n the past, the information flow was more from CBSA into FINTRAC, and now…we can obtain information back from FINTRAC if it is relevant to investigating or prosecuting a money laundering offence or terrorist activity, as it relates to smuggling goods or subject to duties or evading taxes.
>
> Another issue was the exchange of information with foreign states. In the past, we couldn't do that. Now, amendments allow [sharing] information or disclosing seizure information that has been collected under Part II of the *PCMLTFA* with foreign agencies which have regimes similar to a centre such as FINTRAC. So I will use the example of the U.S. We're in the midst of negotiating with the various agencies in the United States …which will allow us then to share [information with U.S. organizations] with respect to seizures. [412]

Vinette testified that, between January 2003 and September 2007, CBSA had made about 900 seizures at border crossings involving suspected proceeds of crime, including TF. A total of roughly $48 million was involved.[413] However, CBSA had no breakdown to show how much of that total involved suspected TF.

Quartermain testified that the CBSA does not receive feedback in all cases where it shares information about suspected TF funds with its partners, and he was uncertain if there was a way to find out what percentage of those funds could be related to TF. There was no legislated requirement for feedback.[414]

CBSA provided the following Selected Commodities Seizure Report[415] to the Commission.

---

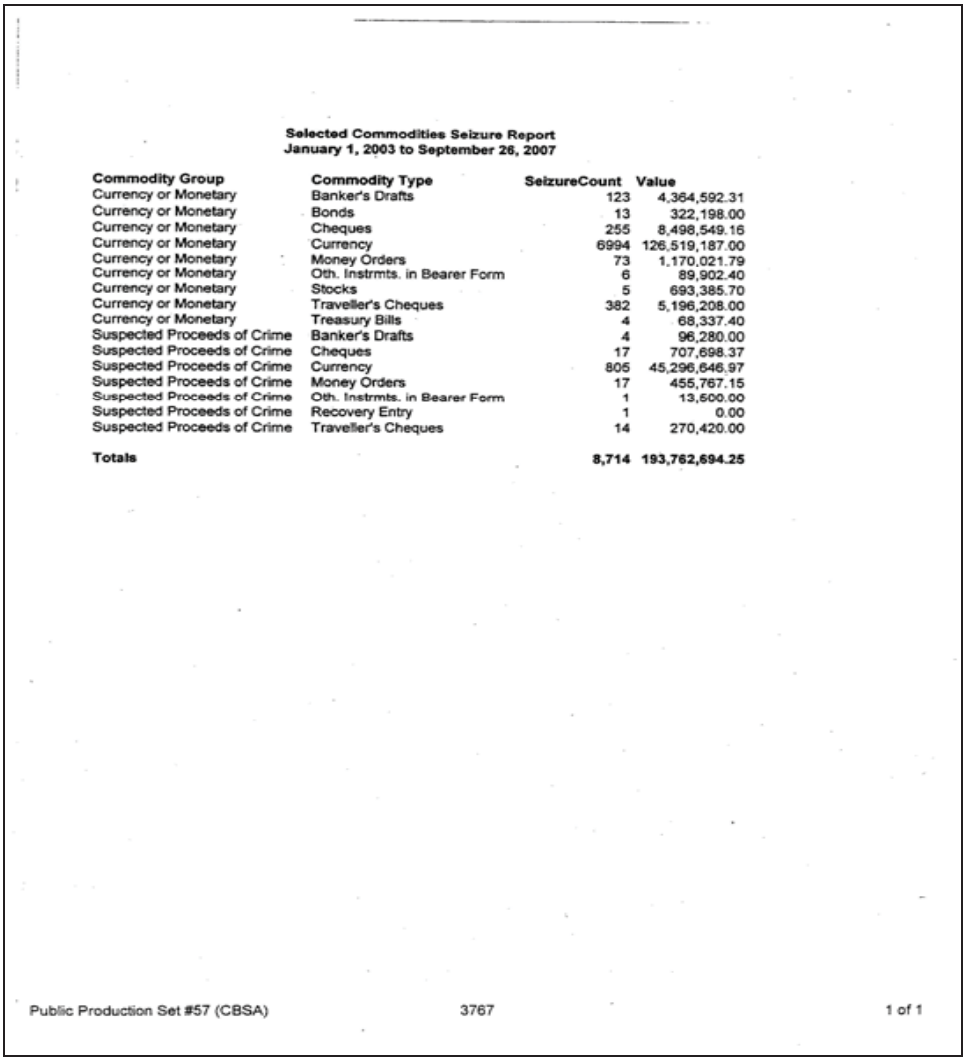
411 Testimony of Denis Vinette, vol. 56, October 2, 2007, p. 7055. See also *PCMLTFA*, s. 36(2) which states: "An officer who has reasonable grounds to suspect that information referred to in subsection (1) would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence may disclose the information to the appropriate police force."

412 Testimony of David Quartermain, vol. 56, October 2, 2007, p. 7069.

413 Testimony of Denis Vinette, vol. 56, October 2, 2007, p. 7050.

414 Testimony of David Quartermain, vol. 56, October 2, 2007, pp. 7053-7056.

415 Exhibit P-235, Tab 10: CBSA Selected Commodities Seizure Report, January 1, 2003 to September 26, 2007.



Selected Commodities Seizure Report
January 1, 2003 to September 26, 2007

Commodity Group	Commodity Type	SeizureCount	Value
Currency or Monetary	Banker's Drafts	123	4,364,592.31
Currency or Monetary	Bonds	13	322,198.00
Currency or Monetary	Cheques	255	8,498,549.16
Currency or Monetary	Currency	6994	126,519,187.00
Currency or Monetary	Money Orders	73	1,170,021.79
Currency or Monetary	Oth. Instrmts. in Bearer Form	6	89,902.40
Currency or Monetary	Stocks	5	693,385.70
Currency or Monetary	Traveller's Cheques	382	5,196,208.00
Currency or Monetary	Treasury Bills	4	68,337.40
Suspected Proceeds of Crime	Banker's Drafts	4	96,280.00
Suspected Proceeds of Crime	Cheques	17	707,698.37
Suspected Proceeds of Crime	Currency	805	45,296,646.97
Suspected Proceeds of Crime	Money Orders	17	455,767.15
Suspected Proceeds of Crime	Oth. Instrmts. in Bearer Form	1	13,500.00
Suspected Proceeds of Crime	Recovery Entry	1	0.00
Suspected Proceeds of Crime	Traveller's Cheques	14	270,420.00
Totals		**8,714**	**193,762,694.25**

Public Production Set #57 (CBSA) 3767 1 of 1

The *PCMLTFA* provides a review and appeal procedure for seizures by CBSA and also specifies the penalties for failing to report currency imports or exports as required by section 12(1).[416] The *PCMLTFA Act* permits a person from whom currency or monetary instruments have been seized, or the lawful owner, to ask the Minister of Public Safety to review the seizure.[417] Vinette confirmed that seven attempts, all unsuccessful, had been made to challenge Level 4 seizures in court.[418] At the time of the 2008 FATF Mutual Evaluation of Canada, 45 cases challenging Level 4 seizures were before the courts.[419] It is not known how many of these, if any, were related to TF.

---

416 *PCMLTFA*, ss. 24-31. The *PCMLTFA* also sets out a procedure for third party claims: see ss. 32-35.
417 *PCMLTFA*, s. 25.
418 Testimony of Denis Vinette, vol. 56, October 2, 2007, p. 7049.
419 2008 FATF Mutual Evaluation of Canada, para. 601.

Information that CBSA gathers can be used in other ways.[420] In addition to the information provided through CBCRs and CBSRs, a BSO may provide information to FINTRAC if the BSO has reasonable grounds to suspect that it would be of assistance to FINTRAC in the detection, prevention or deterrence of money laundering or the financing of terrorist activities – a sort of "catch-all" provision.[421]

In turn, FINTRAC must disclose information to CBSA when FINTRAC concludes that any of the following conditions are met:

> (i) the information is relevant to an offence of evading or attempting to evade paying taxes or duties imposed under an Act of Parliament administered by the CBSA;[422]
>
> (ii) the information is relevant to determining whether a person is a person described in sections 34 to 42 of the *Immigration and Refugee Protection Act* or is relevant to an offence under any of sections 117 to 119, 126 or 127 of the Act;[423] or
>
> (iii) the information is relevant to investigating or prosecuting an offence of smuggling or attempting to smuggle goods subject to duties or an offence related to the importation of goods that are prohibited, controlled or regulated under the *Customs Act* or under any other Act of Parliament.[424]

The 2008 FATF Mutual Evaluation of Canada gave Canada a "Compliant" rating for its cross-border procedures. The FATF noted as well that the monetary threshold ($10,000 – explained below) triggering the need to make a currency declaration was even lower than that recommended by the FATF, and that Canada has implemented the border control measures outlined in the FATF Best Practices Paper.[425]

3.5.2.4 Business Line 2: The Immigration and Refugee Protection Act Process and Other Activities Related to TF

Besides monitoring the cross-border movement of currency and monetary instruments, the CBSA has a role in immigration matters. One of CBSA's goals is to prevent individuals who may have been involved in TF from entering the country.[426]

---

420 Information in this context is that referred to in s. 36(1) of the *PCMLTFA* and consists of: (a) information set out in a report made under section 12(1) of the *PCMLTFA*, (b) any other information obtained for the purposes of Part 2 of the *PCMLTFA*, and (c) information prepared from information referred to in paragraph (a) or (b).

421 *PCMLTFA*, s. 36(3).

422 *PCMLTFA*, s. 55(3)(b.1).

423 *PCMLTFA*, s. 55(3)(d).

424 *PCMLTFA*, s. 55(3)(e).

425 2008 FATF Mutual Evaluation of Canada, para. 585.

426 Testimony of David Quartermain, vol. 56, October 2, 2007, p. 7053.

Section 37(1) of the *Immigration and Refugee Protection Act*[427] sets out the activities which make a permanent resident or a foreign national inadmissible to Canada on grounds of "organized criminality." Tyson George, a Senior Analyst with the Organized Crime Section of the National Security Division of the CBSA, testified that TF could be one such activity.[428]

If Citizenship and Immigration Canada visa officers overseas have reason to believe that a person may be inadmissible under section 37, they send that information to the Organized Crime Section. The Section analyzes the information and, if it believes that there is a possibility of TF being involved, it consults its partner agencies, including FINTRAC. It may also submit a VIR to FINTRAC. FINTRAC in turn may disclose designated information to the Section. Based on any information it receives from FINTRAC and other agencies, and on its own analysis, the Section provides its opinion to the visa officers about whether the person is inadmissible.[429]

3.5.3 International Cooperation

The *PCMLTFA* allows the Minister of Public Safety, with the consent of the Minister of Finance, to enter into an agreement with a foreign state, or an institution or agency of that state, to allow for an exchange of information from reports about currency or monetary instruments between CBSA and a similar foreign counterpart.[430] Information obtained by Canada under the agreement must also be sent to FINTRAC.[431]

The 2008 FATF Mutual Evaluation of Canada described the exchanges of information allowed by a partnership agreement between Canada and the United States under the Shared Border Accord. The exchanges were to help both countries manage the flow of refugee claimants at their shared border (some of the information-sharing would also relate to TF):

- Advance Passenger Information and agreed-to Passenger Name Records on flights between Canada and the United States, including in-transit flights, in order to identify risks posed by passengers on international flights arriving in each other's territory;
- Data related to customs fraud, and agreed-upon customs data pursuant to NAFTA, as well as any additional commercial and trade data, for national security purposes;
- Advance information on designated individuals and organizations for the purpose of freezing terrorist assets;
- Refugee and asylum claimants, in order to ensure that applicants are thoroughly screened for security risks;

427 S.C. 2001, c. 27.
428 Testimony of Tyson George, vol. 56, October 2, 2007, p. 7052.
429 Testimony of Tyson George, vol. 56, October 2, 2007, pp. 7052-7053.
430 *PCMLTFA*, s. 38(1).
431 *PCMLTFA*, s. 38(3).

- Marine in-transit containers arriving in Canada and the United States; and
- Anti-terrorism efforts, through the Cross-Border Crime Forum and Project Northstar.[432]

As noted above, Quartermain told the Commission that negotiations were underway with various agencies in the United States to share information about seizures with US organizations.[433]

3.5.4 Funding

In 2006-07, the CBSA was allocated $7.8 million under the AML/ATF Initiative and was allocated $7.7 million for each of the subsequent three fiscal years.[434]

3.6 Department of Foreign Affairs and International Trade

The Department of Foreign Affairs and International Trade (DFAIT), through the Minister of Foreign Affairs, is responsible for matters relating to the conduct of the external affairs of Canada, including international trade and commerce and international development, where those matters have not been assigned to another federal department, board or agency.[435] The *Department of Foreign Affairs and International Trade Act* requires the Minister to perform the following duties, among others:

- 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 Government of Canada to the heads of Canada's diplomatic and consular missions; and
- foster the development of international law and its application in Canada's external relations.[436]

Several sections of DFAIT play a role in TF matters. The Commission heard evidence from Keith Morrill, Director of the Criminal, Security and Treaty Law

---

432 2008 FATF Mutual Evaluation of Canada, para. 577.
433 Testimony of David Quartermain, vol. 56, October 2, 2007, p. 7069.
434 Department of Finance Presentation, slide 1.
435 *Department of Foreign Affairs and International Trade Act*, R.S.C. 1985, c. E-22, s. 10(1) [*Department of Foreign Affairs and International Trade Act*].
436 *Department of Foreign Affairs and International Trade Act*, s. 10(2).

Division, part of the Legal Bureau at DFAIT.[437] The Division helps address legal issues at the international and domestic levels. The Division has two goals:

> (i) to ensure that Canadian views are put forward at the international level and that its objectives are integrated at that level, as well as being consistent with Canadian domestic policy; and
>
> (ii) to ensure that Canadian foreign policy and the appropriate domestic legislation is in line with Canadian contributions at the international level in regard to terrorism, TF and other related issues.[438]

Two other groups within DFAIT also deal with these issues: the International Crime and Terrorism Division and the Economic Crime Section of the International Humanitarian and Human Rights Law Section.[439]

DFAIT coordinates Canada's international TF activities and "develops and advocates Canadian positions" by representing Canada at the United Nations, G8 (in particular through the Roma/Lyon Anti-Crime and Terrorism Experts Group), Asia-Pacific Economic Cooperation, Organization of American States, and Organization for Security and Co-operation in Europe, among other organizations.[440] DFAIT supports its Minister in the fulfillment of the Minister's responsibilities for the terrorist listing mechanisms implemented under Canada's *United Nations Act*, through the *United Nations Al-Qaida and Taliban Regulations* (UNAQTR) and the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism* (RIUNRST).[441] Finally, DFAIT co-chairs the Interdepartmental Working Group on Terrorist Listings with Public Safety Canada in support of the Minister's legal responsibility to recommend entities to be listed under the RIUNRST. DFAIT also ensures that Canadian foreign policy and international programming complies with Canada's international obligations and domestic regulations to counter TF.[442]

3.7 Public Safety Canada

Public Safety Canada (PS) is responsible for providing support and policy advice to the Minister of Public Safety on all matters of public safety and national security, including money laundering and TF.[443] The Public Safety website describes its areas of activity as emergency management, national security, law

---

437 Testimony of Keith Morrill, vol. 54, September 28, 2007, p. 6677.
438 Testimony of Keith Morrill, vol. 54, September 28, 2007, p. 6678; Department of Finance Memorandum of Evidence on Terrorist Financing, pp. 39-40.
439 Testimony of Keith Morrill, vol. 54, September 28, 2007, p. 6679.
440 Department of Finance Memorandum of Evidence on Terrorist Financing, p. 39.
441 Department of Finance Memorandum of Evidence on Terrorist Financing, p. 39.
442 Department of Finance Memorandum of Evidence on Terrorist Financing, pp. 39-40.
443 Department of Finance Memorandum of Evidence on Terrorist Financing, p. 40.

enforcement, corrections and crime prevention,[444] and its mandate as being to "…keep Canadians safe from a range of risks such as natural disasters, crime and terrorism."[445]

Public Safety works with the agencies within its portfolio, such as the RCMP and CSIS, other levels of government, first responders, community groups, the private sector and foreign countries.[446] Departmental staff members advise the Minister of Public Safety on enforcement and intelligence matters, including those related to money laundering and TF. The Department coordinates policy advice received from its portfolio agencies, as well as the input of these agencies in government-wide exercises, such as the 2008 FATF Mutual Evaluation of Canada.[447]

Two important administrative processes involve the Minister of Public Safety directly in TF matters – the *Criminal Code* listing of terrorist groups and the process under the *Charities Registration (Security Information) Act* (CRSIA):

- The *Criminal Code* authorizes the Minister of Public Safety to recommend to the Governor in Council the listing of terrorist entities under the Code.[448] Public Safety maintains a current *Criminal Code* listing on its website.[449] Along with DFAIT, PS co-chairs the Interdepartmental Working Group on Terrorist Listings; and
- The Minister, with the Minister of National Revenue, is responsible under the CRSIA for preventing the use of charitable organizations for TF purposes.[450] Both CSIS and the RCMP make recommendations to the Minister of Public Safety in this regard.[451] This process and the Minister's role are described in Chapter VI.

3.8 Office of the Superintendent of Financial Institutions

The Office of the Superintendent of Financial Institutions (OSFI) was established by the *Office of the Superintendent of Financial Institutions Act* (*OSFI Act*).[452] The Minister of Finance presides over and is responsible for OSFI.[453] OSFI has a

444 Public Safety Canada, "What we do," online: Public Safety Canada <http://www.ps-sp.gc.ca/abt/wwd/index-eng.aspx> (accessed April 22, 2009) [Public Safety Canada, "What we do"].
445 Public Safety Canada, "What we do."
446 Public Safety Canada, "What we do."
447 Exhibit P-383, Tab 11: Public Safety Canada's Submission to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, October 24, 2007, p. 1 [Public Safety Submission to the Commission].
448 *Criminal Code*, s. 83.05.
449 See Public Safety Canada, "Currently listed entities," online: Public Safety Canada <http://www.publicsafety.gc.ca/prg/ns/le/cle-en.asp> (accessed April 22, 2009).
450 Department of Finance Memorandum of Evidence on Terrorist Financing, p. 40.
451 Public Safety Submission to the Commission, p. 1; *A New Review Mechanism for the RCMP's National Security Activities*, p. 190.
452 R.S.C. 1985, c. 18 (3rd Supp.), Part I.
453 *OSFI Act*, ss. 3, 4(1).

broad supervisory authority over financial institutions coming under federal jurisdiction and responsibility for providing guidance to these institutions. OSFI's powers are derived from several statutes besides the *OSFI Act*. These include the *Bank Act*,[454] *Insurance Companies Act*,[455] *Trust and Loan Companies Act*,[456] *Pension Benefits Standards Act*, 1985[457] and *Cooperative Credit Associations Act*.[458] The financial institutions regulated by OSFI include the following:

(i) banks;

(ii) foreign bank branches in Canada;

(iii) federally regulated trust and loan companies;

(iv) federally regulated cooperative credit associations;

(v) federally regulated property and casualty insurance companies; and

(vi) fraternal benefit societies.[459]

OSFI's objects relating to financial institutions are as follows:

(i) to supervise financial institutions in order to determine whether they are in sound financial condition and are complying with their governing statute and supervisory requirements;

(ii) to promptly advise the management and board of directors of a financial institution if the institution is not in sound financial condition or is not complying with its governing statute or supervisory requirements and, in such a case, to take, or require the management or board to take, the necessary corrective measures or series of measures to deal with the situation in an expeditious manner;

(iii) to promote the adoption by management and boards of directors of financial institutions of policies and procedures designed to control and manage risk; and

(iv) to monitor and evaluate system-wide or sectoral events that may have a negative impact on the financial condition of financial institutions.[460]

---

454 S.C. 1991, c. 46.
455 S.C. 1991, c. 47.
456 S.C. 1991, c. 45.
457 R.S.C. 1985, c. 32 (2nd Supp.).
458 S.C. 1991, c.48.
459 See the definition of "financial institution" in s. 3 of the *OSFI Act*, and Office of the Superintendent of Financial Institutions Canada, "Who We Regulate," online: Office of the Superintendent of Financial Institutions Canada <http://www.osfi-bsif.gc.ca/osfi/index_e.aspx?DetailID=568> (accessed August 1, 2008).
460 *OSFI Act*, s. 4(2).

OSFI states that it contributes to public confidence in the financial system.[461] It does not have any specific legislated role in TF matters but conducts its TF work as part of its obligation to regulate and monitor the financial sector.[462]

OSFI disseminates information about terrorist entities listed under the *Criminal Code* or under the two lists adopted by Canada through the RIUNRST and UNAQTR. OSFI has consolidated these three lists into two – one covering entities and the other covering individuals – and posts them on its website.[463] It distributes updated information to the institutions under its jurisdiction.[464] OSFI also communicates changes to the lists to provincial regulators and supervisors and several associations, such as the Canadian Bankers Association, the Canadian Life and Health Insurance Association and the Canadian Securities Administrators.[465] OSFI provides monthly reminders to institutions under its jurisdiction that they must report any transaction related to an entity or individual named on the lists.

Financial institutions must report to OSFI whether they are in possession or control of property owned or controlled by or on behalf of a listed entity.[466] "Reporting entities" must also report to FINTRAC,[467] CSIS and the RCMP[468] if property in their possession belongs to a listed entity or person. OSFI issues a monthly written reminder that financial institutions are required to file a report showing, in aggregate, the number of accounts and the dollar value of terrorist property frozen and reported to law enforcement.[469]

Unlike the case with other FINTRAC partners such as the RCMP, CSIS, CBSA and the CRA, there is no provision in the *PCMLTFA* permitting or requiring FINTRAC to disclose designated information to OSFI. Under a Memorandum of Understanding between OSFI and FINTRAC, OSFI sends FINTRAC copies of all OSFI's dealings with the entities obliged to report to OSFI. Furthermore, OSFI

---

461 Office of the Superintendent of Financial Institutions (OSFI), Plans and Priorities 2008-2011, p. 1, online: Office of the Superintendent of Financial Institutions Canada <http://www.osfi-bsif.gc.ca/app/DocRepository/1/eng/reports/osfi/PP_2008_2011_e.pdf> (accessed August 1, 2008) [OSFI 2008-11 Plans and Priorities].

462 Department of Finance Memorandum of Evidence on Terrorist Financing, p. 42.

463 "Terrorism Financing," online: Office of the Superintendent of Financial Institutions Canada <http://www.osfi-bsif.gc.ca/osfi/index_e.aspx?DetailID=525> (accessed August 1, 2008) [OSFI, "Terrorism Financing"].

464 For list of OSFI notices, see OSFI, "Terrorism Financing."

465 See, for example, online: Office of the Superintendent of Financial Institutions Canada <http://www.osfi-bsif.gc.ca/app/DocRepository/1/eng/issues/terrorism/updates/2008_08_01_e.pdf> (accessed August 1, 2008).

466 All entities listed in s. 83.11(1) of the *Criminal Code* are required to report the information "to the principal agency or body that supervises or regulates it under federal or provincial law." In the case of federal institutions, it is OSFI: *Criminal Code*, s. 83.11(2); RIUNRST, s. 7(2); *United Nations Al-Qaida and Taliban Regulations*, S.O.R./99-444, s. 5.1(2) [UNAQTR].

467 S. 7.1(1) of the *PCMLTFA*. A person or entity who is required to make a disclosure under s. 83.1 of the *Criminal Code*, or s. 8 of the RIUNRST, must file a report with FINTRAC if that person or entity is also subject to the *PCMLTFA* (as described in s. 5 of the *PCMLTFA*).

468 *Criminal Code*, s. 83.1(1), RIUNRST, s. 8(1), UNAQTR, s. 5.2(1).

469 2008 FATF Mutual Evaluation of Canada, para. 332.

meets regularly with senior FINTRAC officials to discuss findings, trends and emerging issues.[470]

Besides issuing reminders and notices and providing current listings, OSFI conducts educational programs for financial institutions. For example, OSFI holds annual information sessions for compliance and risk management senior officers to discuss money laundering and TF.[471] As of May 2008, OSFI was scheduled to begin consultations with the private sector on a revised AML/ATF guideline that would take into account OSFI's accumulated experience with money laundering compliance efforts since 2004, the changes brought by Bill C-25 and the 2008 FATF Mutual Evaluation of Canada.[472] Another OSFI priority, identified in its 2008-2012 Plans and Priorities, was to respond to the recommendations of the FATF Mutual Evaluation.[473]

3.9 Integrated Threat Assessment Centre

The Integrated Threat Assessment Centre (ITAC) was created in 2004. Following the release of the National Security Policy later that year, it replaced the former CSIS Integrated National Security Assessment Centre.[474]

ITAC's role is to produce comprehensive and integrated assessments of threats to Canada's national security and to distribute them within the intelligence community and to first-line responders. [475] ITAC focuses primarily on terrorist trends and on domestic and international events related to terrorism. ITAC threat assessments may be classified or unclassified.[476]

ITAC's director is appointed by the National Security Advisor (NSA) in consultation with the Director of CSIS. ITAC's Assessment Management Committee (composed of assistant deputy ministers from ITAC partners) advises the Management Board on the focus, effectiveness and efficiency of ITAC's activities.[477] ITAC is staffed by representatives of several organizations, normally for two-year terms: CBSA, CSIS, Correctional Service of Canada, CSE, DND, DFAIT, FINTRAC, the Ontario

470 Department of Finance Memorandum of Evidence on Terrorist Financing, p. 42.
471 Department of Finance Memorandum of Evidence on Terrorist Financing, p. 42.
472 Remarks by Superintendent Julie Dickson, Office of the Superintendent of Financial Institutions Canada (OSFI), to the OSFI AML/ATF Conference, Toronto May 7, 2008, p. 3, online: Office of the Superintendent of Financial Institutions Canada <http://www.osfi-bsif.gc.ca/app/DocRepository/1/eng/speeches/JDickson_OSFI_AML_ATF_e.pdf> (accessed August 1, 2008).
473 OSFI 2008-11 Plans and Priorities, p. 9.
474 Canadian Security Intelligence Service, "Backgrounder No. 13 - The Integrated Threat Assessment Centre (ITAC)," p. 1, online: Canadian Security Intelligence Service <http://www.csis-scrs.gc.ca/nwsrm/bckgrndrs/bckgrndr13-eng.pdf> (accessed August 6, 2008) [CSIS Backgrounder on ITAC]; *A New Review Mechanism for the RCMP's National Security Activities*, p. 141. For further information about the structure, mission and activities of ITAC, see the testimony of Daniel Giasson, Director, Integrated Threat Assessment Centre, Canadian Security Intelligence Service, Proceedings of the Standing Senate Committee on National Security and Defence, Issue 16 – Evidence, May 28, 2007, online: Parliament of Canada <http://www.parl.gc.ca/39/1/parlbus/commbus/senate/Com-e/defe-e/16ev-e.htm?Language=E&Parl=39&Ses=1&comm_id=76> (accessed December 3, 2007).
475 CSIS Backgrounder on ITAC, p. 2.
476 *A New Review Mechanism for the RCMP's National Security Activities*, p. 141.
477 CSIS Backgrounder on ITAC, p. 2.

Provincial Police, PS, Privy Council Office, the RCMP, the *Sûreté du Québec* and Transport Canada.[478] Individuals who are seconded to ITAC bring with them knowledge acquired at their home agencies. [479]

Besides providing threat assessments, ITAC has published studies either specifically about TF[480] or about both terrorism and TF.[481] For example, in 2006 it published *Terrorist Financing - How It's Done and How It's Countered*.[482]

At the international level, ITAC carries out its functions mainly as part of the Five Eyes Terrorist Financing Working Group – a group with representatives from Canada, the UK, the US, Australia and New Zealand. Part of the work of the Five Eyes Working Group is to exchange threat assessments among members of the Group – the Joint Terrorism Analysis Centre in Britain, the National Counterterrorism Center in the United States, the National Threat Assessment Centre in Australia, the Combined Threat Assessment Group in New Zealand, and ITAC.[483] Threat assessments produced by ITAC are shared with international partners unless designated "for Canadian eyes only." ITAC also shares information with other foreign partners on a case-by-case basis.[484]

3.10 Other Departments and Agencies

Other federal departments and agencies have smaller roles in the fight against terrorism and TF, notably the Department of Justice, the Communications Security Establishment and the Privy Council Office.

3.10.1 Department of Justice

The Department of Justice is headed by a single Minister who serves as both Minister of Justice and Attorney General of Canada. The Minister is responsible for the development of law and procedure in regard to criminal law. The Minister is also responsible for the *Mutual Legal Assistance in Criminal Matters*

478 Testimony of John Schmidt, vol. 53, September 27, 2007, pp. 6642-6643; CSIS Backgrounder on ITAC, p. 2. ITAC can also draw information and expertise as needed from Agriculture Canada, Health Canada, Environment Canada and Natural Resources Canada. FINTRAC became a partner only in April 2006: see Testimony of John Schmidt, vol. 53, September 27, 2007, p. 6644.

479 CSIS Backgrounder on ITAC, p. 2; Testimony of John Schmidt, vol. 53, September 27, 2007, p. 6645.

480 Canadian Centre for Intelligence and Security Studies, The Norman Paterson School of International Affairs, Carleton University, "Terrorism Financing and Financial System Vulnerabilities: Issues and Challenges" (ITAC Presents, Trends in Terrorism Series, Volume 2006-3), online: Integrated Threat Assessment Centre <http://www.itac-ciem.gc.ca/pblctns/tc_prsnts/2006-3-eng.pdf> (accessed December 3, 2007).

481 Canadian Centre for Intelligence and Security Studies, The Norman Paterson School of International Affairs, Carleton University, "A Framework for Understanding Terrorist Use of the Internet" (ITAC Presents, Trends in Terrorism Series, Volume 2006-2), online: Integrated Threat Assessment Centre <http://www.itac-ciem.gc.ca/pblctns/tc_prsnts/2006-2-eng.pdf>; Canadian Centre for Intelligence and Security Studies, The Norman Paterson School of International Affairs, Carleton University, "Actual and Potential Links Between Terrorism and Criminality" (ITAC Trends in Terrorism Series, Volume 2006-5), online: Integrated Threat Assessment Centre <http://www.itac-ciem.gc.ca/pblctns/tc_prsnts/2006-5-eng.pdf> (accessed December 3, 2007).

482 Other similar classified studies were examined by Commission counsel.

483 CSIS Backgrounder on ITAC, p. 3.

484 *A New Review Mechanism for the RCMP's National Security Activities*, p. 142.

Act.[485] The 2008 FATF Mutual Evaluation of Canada criticized Canada's mutual legal assistance program, saying that "…[t]here are concerns about the ability of Canada to handle [mutual legal assistance] requests in a timely and effective manner and effectiveness of the current regime cannot be demonstrated due to the lack of adequate data."[486]

The *PCMLTFA* allows the Attorney General to apply for a production order for an investigation of a TF offence.[487] The Attorney General, by way of the Director of Public Prosecutions and the Public Prosecution Service of Canada, has concurrent jurisdiction with provincial Attorneys General for TF prosecutions.[488]

3.10.2 Communications Security Establishment Canada

The Communications Security Establishment Canada (CSE) is Canada's cryptologic agency.[489] Its mandate has three components:

> a. to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence 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 lawful duties.[490]

CSE can be involved in TF work in several ways:

- by providing technical and operational assistance to the RCMP or CSIS (mandate "c" above);[491]
- by receiving information through its own activities (mandate "a") and forwarding it to the relevant agency, including FINTRAC; and
- by being the recipient of disclosures of designated information by FINTRAC. FINTRAC must disclose designated information to CSE if FINTRAC has reasonable grounds to suspect that the information

485 R.S.C. 1985, c. 30 (4th Supp.).
486 2008 FATF Mutual Evaluation of Canada, p. 298.
487 *PCMLTFA*, s. 60(2).
488 Department of Finance Memorandum of Evidence on Terrorist Financing, p. 39.
489 Communications Security Establishment Canada, "Welcome to the Communications Security Establishment Canada," online: Communications Security Establishment Canada <http://www.cse-cst.gc.ca/index-eng.html> (accessed September 16, 2009).
490 *National Defence Act*, R.S.C. 1985, c. N-5, s. 273.64(1).
491 Testimony of Jim Galt, vol. 55, October 1, 2007, pp. 6930-6931.

would be relevant to investigating or prosecuting a money laundering or TF offence and if FINTRAC also determines that the information is relevant to the mandate of CSE.[492]

3.10.3 Privy Council Office

The Privy Council Office (PCO) reports directly to the Prime Minister and is headed by the Clerk of the Privy Council and Secretary to the Cabinet. The PCO acts as the Cabinet secretariat and as the Prime Minister's main source of public service advice for the policy questions and operational issues of concern to the government of the day. The Clerk of the Privy Council is Canada's most senior public servant supporting the Prime Minister and has three main responsibilities: serving as the Prime Minister's Deputy Minister, Secretary to the Cabinet and Head of the Public Service. [493]

The National Security Advisor to the Prime Minister and Associate Secretary to the Cabinet assists the Clerk and provides information, advice and recommendations to the Prime Minister as follows:

- as Associate Secretary to the Cabinet, by acting on the Clerk's behalf on any of the policy and operational issues that come before the PCO; and
- as National Security Advisor to the Prime Minister, by ensuring the effective coordination of Canada's security and intelligence community and, together with the Deputy Minister of National Defence, by being responsible for CSE. The National Security Advisor also oversees the provision of intelligence assessments to the Prime Minister, other ministers and senior government officials.

3.11 Cooperation among Agencies

As this chapter has explained, several federal agencies are involved in implementing Canada's anti-TF program. Cooperation is not limited to formal interdepartmental committees. Some agencies work with each other one-on-one. RCMP Superintendent Reynolds testified, for example, that the RCMP works in this manner on a regular basis with CSIS, CRA and FINTRAC.[494]

---

492 *PCMLTFA*, s. 55(3)(f).

493 Privy Council Office, "The Role and Structure of the Privy Council Office," November 2008, p. 1, online: Privy Council Office <http://www.pco-bcp.gc.ca/docs/information/Publications/Role/docs/2008/role2008-eng.pdf> (accessed September 16, 2009) [PCO, "The Role and Structure of the Privy Council Office"].

494 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6841.

Several formal cooperation mechanisms are discussed below.

3.11.1 Financial Crimes Interdepartmental Coordinating Committee (ICC)

The head of the Financial Crimes Section (Domestic/International) of Finance Canada chairs this working-level committee, which meets at least quarterly to "…address operational and administrative issues related to Canada's Anti-Money Laundering and Anti-Terrorist Financing regime and to coordinate policy in this area."[495] Meetings may occur more often when Parliament is revising legislation and regulations. Diane Lafleur of Finance Canada testified that the committee can deal with both policy and operational issues related to the AML/ATF Initiative.[496]

The ICC's tasks include the following:

- to provide a forum for government working-level stakeholders to assess the operational efficiency and effectiveness of the AML/ATF Initiative, and identify problems/solutions;
- to coordinate and manage all parliamentary, Treasury Board-mandated and Auditor General reviews and audits related to the AML/ATF Initiative; and
- to provide input and advise on Government policy relating to Canada's AML/ATF Initiative.[497]

The ICC's participants are the Departments of Finance, Justice, Public Safety and DFAIT and the following agencies: CRA, FINTRAC, RCMP, CBSA, CSIS and OSFI.[498]

The Committee coordinated the 2008 FATF Mutual Evaluation of Canada and met several times for that purpose.

3.11.2 Financial Crimes Interdepartmental Steering Committee (ADM Steering Committee)

The Assistant Deputy Minister of the Financial Sector Policy Branch of Finance Canada chairs this committee, often referred to as the ADM Steering Committee. It meets twice a year, or as necessary, and provides strategies and general guidance for Canada's AML/ATF Initiative. The terms of reference of the committee describe its functions as follows:

---

495 Exhibit P-227, Tab 4: Financial Crimes Interdepartmental Committees (Coordinating & Steering) Terms of Reference, p. 1 [Financial Crimes Interdepartmental Committees Terms of Reference].

496 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6782.

497 Financial Crimes Interdepartmental Committees Terms of Reference, p. 2.

498 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6782; Financial Crimes Interdepartmental Committees Terms of Reference, p. 1. DFAIT participates only when international AML/ATF matters are involved.

- to provide a forum for ADM-level government stakeholders to assess the overall effectiveness of the AML/ATF Initiative;
- to provide guidance on the Government's AML/ATF communications strategy;
- to provide input and advice on Government policy relating to Canada's AML/ATF Initiative; and
- to oversee the work of a related working-level group, including providing feedback on issues of strategic importance that arise in the group.[499]

The participants are officials at the assistant deputy minister level from the same departments and agencies that belong to the ICC except that DFAIT does not participate in the ADM Steering Committee.

3.11.3 Interdepartmental Coordinating Committee on Terrorist Listings

The Interdepartmental Coordinating Committee on Terrorist Listings is co-chaired by officials from Public Safety and DFAIT. It coordinates the activities of all departments and agencies involved in the listing processes – not only the *Criminal Code* listing process but also the processes flowing from the RIUNRST and the UNAQTR. The committee consists of PS and DFAIT as co-chairs, RCMP and CSIS as intelligence providers, and the Privy Council Office, Department of Finance, CBSA, Department of Justice, CRA and OSFI.[500] CSIS and the RCMP are the lead agencies responsible for preparing recommendations to list an entity and for collecting intelligence in support of the recommendation.

3.11.4 Integrated National Security Enforcement Teams (INSETs)

The RCMP describes the purpose of the INSETs as being to increase the capacity for the collection, sharing and analysis of intelligence among partners with respect to individuals and entities that are a threat to national security, create an enhanced investigative capacity to bring such individuals and entities to justice, and enhance partner agencies' collective ability to combat national security threats."[501] National Security Investigation Sections[502] (NSISs) and INSETs operate at the divisional level of the RCMP and have the primary responsibility for carrying out criminal investigations in national security matters.[503]

INSETs deal with TF issues as well as with terrorist investigations. They also provide a forum for the exchange of information among the agencies that may be involved alongside the RCMP – for example, CSIS, CBSA, Citizenship and

499 Financial Crimes Interdepartmental Committees Terms of Reference, pp. 3-4.
500 Public Safety Submission to the Commission, p. 2.
501 Royal Canadian Mounted Police, "Integrated National Security Enforcement Teams," online: Royal Canadian Mounted Police <http://www.rcmp-grc.gc.ca/secur/insets-eisn-eng.htm> (accessed August 28, 2008) [RCMP, "Integrated National Security Enforcement Teams"].
502 Since renamed "National Security Enforcement Sections."
503 *A New Review Mechanism for the RCMP's National Security Activities*, p. 102.

Immigration Canada, CRA, provincial and municipal police forces and other federal and provincial agencies.[504] INSETs are located in Vancouver, Toronto, Ottawa and Montreal.[505] Their activities are coordinated by RCMP National Headquarters. The RCMP is fully accountable for INSET operations and RCMP policies and rules apply to the work of INSET members.[506]

3.11.5 Integrated Border Enforcement Teams (IBETs)

In TF matters, Integrated Border Enforcement Teams (IBETs) coordinate the work of various agencies in monitoring the cross-border transportation of currency and other monetary instruments.[507] The RCMP states that IBETs "…enhance border integrity and security along the shared Canada/US border, between designated ports of entry."[508]

IBETs consist of Canadian and American partners: the RCMP, the CBSA, the US Customs and Border Protection/Office of Border Patrol, the US Bureau of Immigration and Customs Enforcement, and the US Coast Guard. [509] The RCMP and the CBSA share responsibility for collecting information to develop intelligence for investigations relating to national security or crimes such as organized crime and human smuggling.[510]

3.11.6 Relationships among Agencies in the Same Ministerial Portfolio

David Quartermain, Director of the Borders Intelligence Division of CBSA's Intelligence Directorate, testified to having a close relationship with agencies within Public Safety Canada (for example, the RCMP and CSIS).[511] Denis Vinette, Director of the CBSA Borders Enforcement Division, testified about the advantages of working with agencies from the same department:

> [T]here is a benefit, I guess, to our reporting into the same organization, as well as to the same Minister, in terms of what the direction is in terms of our strategies and priorities of the day. And so it ensures that, as we work through the portfolio, Department of Public Safety, that those priorities are shared amongst all the agencies because we all have different roles

---

504 *A New Review Mechanism for the RCMP's National Security Activities*, p. 102. The report states that, for example, "in 2004, O-INSET (located in Toronto) had members from the Ontario Provincial Police, Toronto Police Service, York Regional Police, Durham Regional Police, Peel Regional Police, CSIS and the CBSA. As of August 2004, O-INSET comprised 53 RCMP regular members, two RCMP civilian members and 22 people on secondment from other agencies and RCMP units."

505 RCMP, "Integrated National Security Enforcement Teams."

506 *A New Review Mechanism for the RCMP's National Security Activities*, p. 102.

507 2008 FATF Mutual Evaluation of Canada, para. 572.

508 Royal Canadian Mounted Police, "Integrated Border Enforcement Teams (IBETs)," online: Royal Canadian Mounted Police <http://www.rcmp-grc.gc.ca/ibet-eipf/index-eng.htm> (accessed February 18, 2009) [RCMP, "Integrated Border Enforcement Teams"].

509 RCMP, "Integrated Border Enforcement Teams."

510 2008 FATF Mutual Evaluation of Canada, para. 574.

511 Testimony of David Quartermain, vol. 56, October 2, 2007, p. 7071.

> to play, but in the same fight, if you will, when it comes to different types of priorities. And so it just ensures that all of our activities are aligned, be it intelligence information sharing, be it operationally on the ground.[512]

3.11.7 International Cooperation

The number of interdepartmental activities[513] involving TF matters has increased, in part because Canadian agencies need to collaborate to fulfill international commitments and programs. The 2008 FATF Mutual Evaluation of Canada was one example. As well, FINTRAC has contributed to the typology exercises of a subgroup of FATF on topics such as the use of casinos and "proliferation financing."[514]

CSIS and the RCMP participate in the Five Eyes Terrorist Financing Working Group.[515] CSIS described its participation in the Working Group as follows:

> The intent of the Five-Eyes working group is to bring together law enforcement and intelligence agencies to develop recommendations on countering terrorist financing through a coordinated international response. The [CSIS] Financial Analysis Unit has benefited from its continued participation in the Five-Eyes group. It serves to identify areas of mutual interest and emerging trends, and it assists in identifying issues that the Unit should consider in its provision of operational support on terrorist financing.[516]

The meetings of the Working Group – involving representatives from Australia, Canada, New Zealand, the United Kingdom and the United States – are held under high security, which allows for the sharing of operational information about cases of mutual interest, including information about investigative and analytical techniques.[517]

3.11.8 Secondments

As is the case in the federal government generally, secondments are common among the partners of the AML/ATF Initiative and are an effective means of promoting cooperation and better communication.[518] FINTRAC has a person

---

512 Testimony of Denis Vinette, vol. 56, October 2, 2007, pp. 7072-7073.
513 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6997.
514 Second FINTRAC Response to Supplementary Questions of the Commission, Question 2(d).
515 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6928.
516 CSIS Response to Supplementary Questions of the Commission, Question 3.
517 CSIS Response to Supplementary Questions of the Commission, Question 3.
518 Testimony of John Schmidt, vol. 53, September 27, 2007, p. 6642; Testimony of Jim Galt, vol. 55, October 1, pp. 6909-6910.

seconded to the RCMP Integrated Proceeds of Crime Unit.[519] CRA has employees seconded to the RCMP National Security Operations Branch and to CSIS. ITAC is staffed by representatives of several organizations.

Tom Quiggin, an expert in terrorism matters, testified about the value of personal contacts – the types of contacts that secondments help to develop:

> During a time of crisis, during a time of stress, an organization like CSIS or an organization like the RCMP will almost never refuse to share information assuming there is a personal contact somewhere.[520]

3.11.9 Private/Public Sector Advisory Committee

The Department of Finance chairs a private/public sector advisory committee that was created in 2007 in response to recommendations from the November 2004 Auditor General's Report.[521] Its first meeting was held in November 2007. The membership of the committee includes representatives of many federal agencies and private sector organizations.[522]

A summary of the proceedings of the first meeting of the committee showed that it focused on guidance for the benefit of reporting entities and on opinions of the private sector about the anti-TF program. Several questions for future consideration by the private sector were raised on topics such as feedback from government authorities, the consultation process that led to Bill C-25 and communication between government authorities and the private sector.[523] This committee offers government agencies direct contact with private sector representatives.

3.12 Conclusion

Those engaged in raising and moving funds for terrorist purposes have a host of means to do so. Many of those means are very difficult to detect among the massive number of legitimate movements of funds around the globe. Responding to TF involves many government agencies, international organizations and private sector entities.

This chapter has shown the range of government agencies and private sector entities involved in anti-TF efforts. It has also pointed to the complexity of the relationships among these agencies and entities, both in how they cooperate in practice and in the laws that frame their cooperation.

---

519 Summary of Meeting with FINTRAC, p. 3.
520 Testimony of Thomas Quiggin, vol. 91, December 7, 2007, pp. 12053-12054.
521 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6784; 2004 Auditor General Report on Money Laundering, para. 2.29.
522 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6784.
523 Department of Finance Response to Supplementary Questions of the Commission, Question 3(b).

VOLUME FIVE
TERRORIST FINANCING

CHAPTER IV: EXTERNAL REVIEWS OF CANADA'S ANTI-TF PROGRAM

Diane Lafleur, Director of the Financial Sector Division at the Department of Finance, testified that Canada's Anti-Money Laundering/Anti-Terrorist Financing (AML/ATF) Initiative has been "heavily evaluated," including by international organizations.[1] These reviews have attempted to measure the effectiveness of Canada's anti-TF efforts and have not been restricted to reviewing only the propriety of governmental actions with respect to TF. This chapter examines the reviews completed to date.

4.1 Domestic Reviews

4.1.1 Auditor General of Canada

In a November 2004 report, the Auditor General reviewed the implementation of the National Initiative to Combat Money Laundering in relation to both money laundering and TF. Since work on TF was still in its early stages at that time, the report focused mainly on money laundering. As was typical with that type of review, it was a value-for-money audit.[2] It sought to determine whether the management framework for implementing the Initiative was "…designed appropriately to promote the detection and deterrence of money laundering and terrorist financing and [provided] accountability to Parliament for results achieved."[3]

The audit focused primarily on the operations[4] of tlhe Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), but also described the work of other agencies and their interactions with FINTRAC. The Auditor General concluded that "…Canada now has a comprehensive strategy against money laundering and terrorist financing that is generally consistent with international standards."[5] The report recognized that, since the anti-money laundering program was then

---

1 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6764. Mark Potter, Assistant Director for Government Relationships at FINTRAC, made similar remarks: see Testimony of Mark Potter, vol. 56, October 2, 2007, pp. 6979-6980.

2 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6766; Exhibit P-227, Tab 3: Department of Finance Memorandum of Evidence on Terrorist Financing, February 28, 2007, para. 5.5 [Department of Finance Memorandum of Evidence on Terrorist Financing].

3 *Report of the Auditor General of Canada to the House of Commons*, November 2004, Chapter 2: "Implementation of the National Initiative to Combat Money Laundering," para. 2.14, online: Office of the Auditor General of Canada <http://www.oag-bvg.gc.ca/internet/docs/20041102ce.pdf> (accessed January 16, 2009) [2004 Auditor General Report on Money Laundering].

4 2004 Auditor General Report on Money Laundering, para. 2.15.

5 2004 Auditor General Report on Money Laundering, paras. 2.1, 2.18.

relatively new, many problems could reflect "inevitable growing pains."[6] It also mentioned that it takes time to establish effective networks for cooperation and to build trust.[7] The report nevertheless identified several deficiencies:

- Disclosures by FINTRAC did not contain enough information to be useful to law enforcement and security intelligence;[8]
- There were frictions at the operating level: notably, the reluctance of law enforcement to share information with FINTRAC, law enforcement's hesitancy to give weight to FINTRAC's unsolicited disclosures, connectivity problems between the information technology systems of FINTRAC and the Canada Border Services Agency (CBSA), and the burden on reporting entities;[9]
- There were difficulties in assessing the impact of FINTRAC's disclosures as no prosecutions had yet been initiated as a result of FINTRAC information. Furthermore, follow-up on the disclosures by FINTRAC to receiving agencies was lacking; [10]
- There was no management framework to "…direct complementary actions in separate agencies" and it was said that "…more effective mechanisms and leadership are needed for co-ordinating efforts both within the federal government and among all stakeholders." The report noted that, at the federal level, the interdepartmental working group chaired by Finance Canada lacked the "…scope and mandate for effective support of a co-ordinated campaign against money laundering and terrorist financing."[11] Furthermore, "…[t]he Initiative would also benefit from mechanisms that would bring in provincial and private sector stakeholders;"[12]
- Feedback from FINTRAC to the reporting entities was limited;[13] and Limited information was available about the effectiveness of the Initiative. This could be partly because FINTRAC was then still a fairly young agency.[14] The Initiative was also in its early stages. Accountability mechanisms were not yet all in place.[15] The report went on to state that "…[i]t is not possible to assess the Initiative's effectiveness without information on the impact that FINTRAC disclosures have had on the investigation and prosecution of money-laundering and terrorist-financing offences. All partners in the Initiative thus have a shared interest in co-operating to establish mechanisms for tracking the use of

6 2004 Auditor General Report on Money Laundering, para. 2.26.
7 2004 Auditor General Report on Money Laundering, para. 2.26.
8 2004 Auditor General Report on Money Laundering, paras. 2.38-2.46, 2.94.
9 2004 Auditor General Report on Money Laundering, para. 2.25.
10 2004 Auditor General Report on Money Laundering, para. 2.22.
11 2004 Auditor General Report on Money Laundering, para. 2.27.
12 2004 Auditor General Report on Money Laundering, para. 2.28.
13 2004 Auditor General Report on Money Laundering, para. 2.56.
14 2004 Auditor General Report on Money Laundering, para. 2.88.
15 2004 Auditor General Report on Money Laundering, para. 2.93.

FINTRAC disclosures and measuring their effects, to the extent that is possible. For accountability purposes, summary information on these results needs to be reported to Parliament regularly."[16]

The Auditor General made the following recommendations:

- The government should establish an effective management framework to provide direction and to co-ordinate anti-money laundering efforts at the federal level. It should consider establishing an anti-money laundering advisory committee with representatives from government, industry and law enforcement to discuss issues of common interest regularly and to develop approaches for dealing with emerging issues;[17]
- In cooperation with law enforcement and security agencies, FINTRAC should establish a set of written criteria to guide its analysts and its Disclosure Committee in determining which transactions should be disclosed to designated recipients;[18]
- The government should carry out a review to identify changes that would improve the value of FINTRAC disclosures and the means to bring about those changes;[19]
- FINTRAC should establish target turnaround times for voluntary information reports (VIRs) which it receives from law enforcement and security agencies, and should make those targets public;[20]
- In consultation with the Canada Revenue Agency (CRA), FINTRAC should establish criteria for disclosure to the CRA of cases involving possible tax evasion and should refer cases to the CRA that meet the criteria;[21] and
- The government should establish effective mechanisms to monitor the results of disclosures, including the extent to which disclosures are used and the impact they have on the investigation and prosecution of money laundering and TF offences. It should regularly provide summary information on these results to Parliament.[22]

---

16 2004 Auditor General Report on Money Laundering, para. 2.91.
17 2004 Auditor General Report on Money Laundering, para. 2.29.
18 2004 Auditor General Report on Money Laundering, para. 2.37. FINTRAC mentioned that it had developed "indicators" with the assistance of the FATF and the Egmont Group, but stated that "… the analysis and disclosure processes will continue to rely heavily on judgment, as each suspected case of money laundering, terrorist activity financing, or threat to the security of Canada must be assessed on its own merit."
19 2004 Auditor General Report on Money Laundering, para. 2.46.
20 2004 Auditor General Report on Money Laundering, para. 2.54.
21 2004 Auditor General Report on Money Laundering, para. 2.67.
22 2004 Auditor General Report on Money Laundering, para. 2.92.

4.1.2 EKOS Research Associates Evaluation

Also in 2004, EKOS Research Associates published an evaluation of Canada's AML/ATF Initiative.[23] The Treasury Board of Canada had requested the evaluation. Diane Lafleur of the Department of Finance described the evaluation as follows:

> The Treasury Board evaluation was to assess whether the initiative was broadly in line with Canada's overall stated objectives in international commitments and whether the initiative was actually going in the right direction and continued funding for the initiative was contingent on the successful completion of that evaluation.[24]

In 2002, EKOS had performed an interim evaluation only about money laundering matters. The November 2004 EKOS review was directed at both money laundering and TF.

Among other conclusions, the 2004 report found that:

- "…[t]he Initiative [was] well aligned with the federal government's concern with fighting organized crime and maintaining public security;"[25]
- the Initiative was effective;[26]
- the Initiative compared well internationally;[27] and
- "…[t]he relationship between the Initiative's activities (as a whole) and expected outcomes was logical and appropriate."[28]

The EKOS report made several additional observations:

- At that time, it would be difficult to measure the contribution of the Initiative, particularly since it had then been fully operational for less than two years;[29]
- In many cases, the impact on prosecutions would not be realized for a number of years;[30]

---

23 EKOS Research Associates Inc., *Year Five Evaluation of the National Initiatives to Combat Money Laundering and Interim Evaluation of Measures to Combat Terrorist Financing* (November 30, 2004), online: Department of Finance <http://www.fin.gc.ca/activty/pubs/nicml-incba_e.pdf> (accessed January 16, 2009) [EKOS Report on Money Laundering and Terrorist Financing].

24 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6766.

25 EKOS Report on Money Laundering and Terrorist Financing, p. 20.

26 EKOS Report on Money Laundering and Terrorist Financing, p. 55.

27 EKOS Report on Money Laundering and Terrorist Financing, p. 55.

28 EKOS Report on Money Laundering and Terrorist Financing, p. 21.

29 EKOS Report on Money Laundering and Terrorist Financing, p. 42.

30 EKOS Report on Money Laundering and Terrorist Financing, p. 52.

- The Initiative had "…contributed to investigations, seizures and prosecutions as intended;"[31] and
- "[T]he evidence indicates that the Initiative's measures are having some impact."[32]

The Department of Finance Memorandum of Evidence on Terrorist Financing noted that "…[m]any of the conclusions of [the EKOS] report echoed the findings of the Auditor General report."[33]

The EKOS report made the following recommendations to the Government of Canada:

- Continue to conduct consultations with representatives of the financial services sector, including organizations at the national and other jurisdictional levels, to help representatives see the value of their contributions. Before implementing any future changes to regulations or compliance activities, ensure that timely input is obtained from these organizations and that the potential for compliance fatigue in the financial services sector is taken into account.[34]
- At a minimum, consider maintaining current funding allocations to the Initiative's partners. In addition, consider responding over the short term to certain funding pressures, including: (i) funding needed to finance IT renewal needs at FINTRAC; (ii) funding increases identified by the CBSA to expand the CBCR [Cross-Border Currency Reporting] Teams and Currency Detector Dog Teams; to collect, develop, and to coordinate the dissemination of tactical and operation intelligence (CBSA Intelligence) and to deal with the high volume of appeals of currency seizures (CBSA Adjudication); (iii) increased funding identified by the RCMP to enhance its capacity for investigation of money laundering and terrorist financing intelligence, leads and tips provided by all sources; capacity to analyse and measure the impact of intelligence received; and delivery of educational programs for the private sector; and (iv) future funding pressures associated with the planning and conduct of the next full evaluation of the Initiative.[35]
- Assess the feasibility of increasing the amount of information that may be included in FINTRAC disclosures in order to improve their value to recipients.[36]

---

31 EKOS Report on Money Laundering and Terrorist Financing, p. 46.
32 EKOS Report on Money Laundering and Terrorist Financing, p. 50.
33 Department of Finance Memorandum of Evidence on Terrorist Financing, para. 5.6.
34 EKOS Report on Money Laundering and Terrorist Financing, p. 35.
35 EKOS Report on Money Laundering and Terrorist Financing, pp. 41-42.
36 EKOS Report on Money Laundering and Terrorist Financing, p. 44.

- Devote efforts to assessing the capacity of the existing evaluation model in demonstrating the outcomes and cost effectiveness of the Initiative. Efforts needed to occur at several levels:

  a. The existing logic model had not been revisited since its development several years earlier. As logic models are not intended to be static, it should be revisited and updated to accurately reflect activities and intended outcomes of the Initiative;

  b. The evaluation framework for the Initiative would need to be updated to establish clear expectations around how to measure the future success of the Initiative;

  c. There was a need for special studies to identify appropriate measurement tools and models to further assess current difficulties in determining outcomes, or at least to understand the degree to which such tools and models could best be used; and

  d. A continued focus on performance measurement was needed across partners to ensure ongoing data collection tied to the revised evaluation framework.[37]

- Since the evaluation occurred when the measures had been implemented for only a short time, and given the measurement difficulties, a full evaluation of the Initiative should be conducted again before 2009.[38]
- Canada should maintain its current strong level of commitment to combat money laundering and terrorist financing through the continued active support of the Initiative.[39]

4.1.3 Senate Review of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*

Section 72(1) of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*[40] (*PCMLTFA*) requires a review of the administration and operation of the Act every five years. In October 2006, the Standing Senate Committee on Banking, Trade and Commerce published its interim report on the review of the *PCMLTFA*:

---

37 EKOS Report on Money Laundering and Terrorist Financing, p. 55.
38 EKOS Report on Money Laundering and Terrorist Financing, p. 55.
39 EKOS Report on Money Laundering and Terrorist Financing, p. 56.
40 S.C. 2007, c. 17.

Stemming the Flow of Illicit Money: A Priority for Canada.[41] The interim report recommended that:

1. the federal government develop a registration system for money services businesses;[42]
2. the federal government amend the *PCMLTFA* to require dealers in precious metals, stones and jewellery to report suspicious cash transactions above $10,000 to FINTRAC. The Act's customer due-diligence and record-keeping requirements should also apply to these dealers when they are involved in cash transactions exceeding $10,000;[43]
3. the federal government, within the context of the *PCMLTFA*, ensure that customer-identification requirements as they relate to non-face-to-face transactions are appropriate to the risks associated with these transactions. To the extent practicable, these requirements should be consistent with the practices used by other industrialized countries regarding similar transactions;[44]
4. the federal government, in considering amendments to the *PCMLTFA*, employ a risk-based approach in determining the level of client-identification, record-keeping and reporting requirements for entities and individuals that are required to report under the *Act*;[45]
5. the federal government complete its negotiations with the Federation of Law Societies regarding the client-identification, record-keeping and reporting requirements imposed on solicitors under the *PCMLTFA*. These requirements should respect solicitor-client privilege, the *Canadian Charter of Rights and Freedoms and the Quebec Charter of Human Rights and Freedoms*;[46]
6. the federal government amend the *PCMLTFA* to permit FINTRAC to disclose to law enforcement and intelligence agencies its rationale for disclosing information, as well as additional publicly available information;[47]
7. the federal government meet with representatives from FINTRAC, law enforcement and intelligence agencies, and the entities and individuals required to report under the *PCMLTFA*, to develop an information-sharing protocol with respect to how reports and disclosures under the Act might be modified to be more useful;[48]

---

41 Online: Parliament of Canada <http://www.parl.gc.ca/39/1/parlbus/commbus/senate/com-e/bank-e/rep-e/rep09oct06-e.pdf> (accessed January 16, 2009) [Senate Review of the *PCMLTFA*]. Hearings were held in May and June 2006: Senate Review of the *PCMLTFA*, p. 1.

42 Senate Review of the *PCMLTFA*, p. 10.

43 Senate Review of the *PCMLTFA*, p. 10.

44 Senate Review of the *PCMLTFA*, p. 11.

45 Senate Review of the *PCMLTFA*, p. 12.

46 Senate Review of the *PCMLTFA*, p. 14.

47 Senate Review of the *PCMLTFA*, p. 16.

48 Senate Review of the *PCMLTFA*, p. 16.

8. the federal government, following the development of very clear guidelines about the identification of suspicious attempted transactions and, after thorough consideration of the international experience with the identification and reporting of such transactions, amend the *PCMLTFA* to require the reporting of suspicious attempted transactions;[49]
9. the federal government meet with FINTRAC, the RCMP and other relevant stakeholders in an effort to determine the likelihood, nature and extent of money laundering and terrorist activity financing using such emerging methods of financial services delivery as white label ATMs and internet banking. Appropriate legislative and other actions should be taken once the likelihood, nature and extent of these activities is determined;[50]
10. the federal government examine the extent to which the objective reporting threshold of $10,000 contained in the *PCMLTFA* is appropriate for Canada and consistent with other countries. Should the threshold be found to be inappropriate, the Act should be amended to establish an appropriate objective reporting threshold;[51]
11. the federal government ensure that FINTRAC is adequately funded to fulfill its responsibilities under the *PCMLTFA*. As well, the government should examine the role, if any, that the Office of the Superintendent of Financial Institutions could play in providing FINTRAC with information that would assist it in meeting its compliance obligations under the Act;[52]
12. the federal government collaborate with the Office of the Privacy Commissioner in the development of legislation to amend the *PCMLTFA*, with a view to ensuring that the proposed amendments meet domestic and international requirements without unduly compromising the privacy of Canadians;[53]
13. the federal government amend the *PCMLTFA* to permit FINTRAC to provide information to foreign financial intelligence units only in countries which have privacy legislation consistent with Canada's *Privacy Act*;[54]
14. the federal government amend the *PCMLTFA* to require periodic review of the operations of FINTRAC, with an annual report to Parliament. This review should be undertaken by the Security Intelligence Review Committee (SIRC), which should receive adequate resources to enable it to fulfill this broader mandate;[55]

---

49 Senate Review of the *PCMLTFA*, p. 17.
50 Senate Review of the *PCMLTFA*, p. 18.
51 Senate Review of the *PCMLTFA*, p. 19.
52 Senate Review of the *PCMLTFA*, p. 20.
53 Senate Review of the *PCMLTFA*, p. 21.
54 Senate Review of the *PCMLTFA*, p. 22.
55 Senate Review of the *PCMLTFA*, p. 22.

15. the RCMP make publicly available its rules and regulations regarding information retention and disposal. The rationale underlying the periods of time articulated in any rules and regulations that do not reflect legislated obligations should be justified to the Minister of Public Safety;[56] and that
16. the federal government provide the Royal Canadian Mounted Police with the additional resources needed to pursue investigation of the money laundering and terrorist activity financing cases that it believes are necessary to protect Canadians.[57]

4.1.4 House of Commons Review of the *Anti-terrorism Act*

Section 145 of the *Anti-terrorism Act*[58] (*ATA*) required a comprehensive review of its provisions and operation within three years of Royal Assent.[59]

In March 2007, the House of Commons Standing Committee on Public Safety and National Security[60] published its final report on the review of the *ATA*: *Rights, Limits, Security: A Comprehensive Review of the Anti-terrorism Act and Related Issues*.[61] The report also examined issues relating to all legislation amended or created by the *ATA*, including TF matters covered by the *PCMLTFA* and the *Charities Registration (Security Information) Act*[62] (*CRSIA*). However, TF was not the main issue discussed in that report. Money laundering issues were not considered.

- On topics related to TF, the Commons Committee review recommended that:

---

56 Senate Review of the *PCMLTFA*, p. 23.
57 Senate Review of the *PCMLTFA*, p. 24.
58 S.C. 2001, c. 41.
59 In this case, both chose to conduct a review. The House of Commons recommended that the *Anti-terrorist Act* be amended so that another review would be conducted in 2010-11: House of Commons Canada, Final Report of the Standing Committee on Public Safety and National Security, Subcommittee on the *Review of the Anti-terrorism Act, Rights, Limits, Security: A Comprehensive Review of the Anti-terrorism Act and Related Issues*, March 2007, p. 84, online: Parliament of Canada <http://www2.parl.gc.ca/content/hoc/Committee/391/SECU/Reports/RP2798914/sterrp07/sterrp07-e.pdf> (accessed May 25, 2009) [House of Commons Report on the *ATA*].
60 Subcommittee on the Review of the *Anti-terrorism Act*.
61 House of Commons Report on the *ATA*.
62 S.C. 2001, c. 41, s. 113.

- [16][63] section 83.1 of the *Criminal Code* be amended to exempt legal counsel or law firms when they are providing legal services and not acting as financial intermediaries;[64]
- [17] section 83.08 of the *Criminal Code* be amended to allow for a due diligence defence;[65]
- [18-22] several inconsistencies in the wording of the *Criminal Code* be fixed;[66]
- [23] consideration be given to further integrating the terrorist entity listing regimes established under the *Criminal Code*, the *Regulations Implementing the United Nations Resolution on the Suppression of Terrorism*, and the *United Nations Al Qaida and Taliban Regulations* insofar as the departmental administration, applicable test for inclusion, and legal consequences of listing are concerned;[67]
- [24] section 83.05 of the *Criminal Code* be amended so that, when a listed entity wishes to have an initial decision to list reviewed, it is not required to make an application to the Minister of Public Safety, but may instead apply directly to a court;[68]
- [25] section 83.05 of the *Criminal Code* be amended so that, when a listed entity applies to no longer be a listed entity in accordance with subsections (2) or (8), the Minister of Public Safety and Emergency Preparedness must make a recommendation within 60 days, failing which he or she is deemed to have recommended that the applicant be removed from the list. Furthermore, any recommendation or deemed recommendation on the part of the Minister should expressly be referred to the Governor in Council, which is to make a final decision within 120 days of the entity's application, failing which the entity is deemed to be removed from the list;[69] and

---

63 The numbers in the square brackets are the recommendation numbers.

64 House of Commons Report on the *ATA*, p. 24. [This is not the same requirement as the requirement in the *PCMLTFA* to report suspicious transactions, which is dealt with in a separate section as "the legal profession issue." In the case of the *PCMLTFA*, lawyers would be required to report suspicious transactions. With regard to what is mentioned here in the House of Commons report, there is already a requirement in the *Criminal Code* that "…every person" shall disclose the existence of property in their possession or control that they know is owned or controlled by or on behalf of a terrorist group. This includes lawyers and the House Review proposes to change that. The Senate Review of the *ATA*, on the other hand, disagreed, stating that "The Committee has concluded that no special exemptions need to be created for lawyers when providing legal services to or representing those accused of terrorist offences. Solicitor-client privilege does not appear to be placed in jeopardy by section 83.1 of the *Criminal Code*, and the Crown would be required to prove subjective intent, on the part a lawyer, before he or she could be convicted under sections 83.03 or 83.18.": at p. 56.]

65 House of Commons Report on the *ATA*, p. 24.

66 House of Commons Report on the *ATA*, pp. 25-26.

67 House of Commons Report on the *ATA*, p. 29.

68 House of Commons Report on the *ATA*, p. 30.

69 House of Commons Report on the *ATA*, pp. 31-32.

- [26] section 83.05 of the *Criminal Code* be amended so that, during each two-year review of the list of entities under subsection (9), it be made clear that the Governor in Council has the final decision as to whether or not an entity should remain a listed entity. Furthermore, the decision should be made within 120 days of the commencement of the review, failing which the entity is deemed to be removed from the list.[70]

The Commons committee also made recommendations relating to the *CRSIA*. These are discussed in Chapter VI.

The 2007 Commons Committee report asked the government to table a comprehensive response,[71] which it did in July 2007.[72]

4.1.5 Senate Review of the *Anti-terrorism Act*

In February 2007, the Special Senate Committee on the *Anti-terrorism Act* published its report, *Fundamental Justice in Extraordinary Times: Main Report of the Special Senate Committee on the Anti-terrorism Act*.[73] That report examined issues relating to all legislation amended or created by the *ATA*, including TF matters related to the application of the *PCMLTFA* and the *CRSIA*. However, TF matters were not the main issue reviewed. The Commons Committee report described above and the Senate Committee report arrived at opposite conclusions on some issues, especially due diligence matters and the listing process.

The Senate Committee recommended that:

- [2] the government legislate a single definition of terrorism;[74]
- [10] the government provide written justification for listing each terrorist entity under its three listing regimes;[75]
- [11] the Department of Justice be required to review, and provide an independent evaluation of, the information that security and intelligence agencies provide to the Minister of Public Safety before he or she recommends to Cabinet the addition, retention or removal of a terrorist entity from a list of such entities;[76]
- [25] the government put information-sharing arrangements in relation to national security investigations in writing; ensure that Canadian law enforcement and security agencies attach written caveats regarding the use of shared information; require Canadian

---

70 House of Commons Report on the *ATA*, p. 32.
71 House of Commons Report on the *ATA*, p. 113.
72 The government's response is examined in section 5.3.
73 Online: Parliament of Canada: <http://www.parl.gc.ca/39/1/parlbus/commbus/senate/com-e/anti-e/rep-e/rep02feb07-e.pdf> (accessed January 16, 2009) [Senate Report on the *ATA*].
74 Senate Report on the *ATA*, p. 17.
75 Senate Report on the *ATA*, p. 46. But only when the listing differs from the UN list.
76 Senate Report on the *ATA*, p. 49.

> agencies to make formal complaints to foreign agencies regarding the misuse of shared information; and produce annual reports assessing the human rights records of various countries;[77]
>
> - [38] the government implement more effective oversight of the RCMP, akin to the level and nature of oversight that SIRC performs in relation to CSIS, particularly in terms of access to information and the capacity to audit day-to-day national security functions;[78] and that
> - [39] a standing committee of the Senate, with dedicated staff and resources, be established to monitor, examine and periodically report on matters relating to Canada's anti-terrorism legislation and national security framework.[79]

No recommendations were made about TF. The Committee saw the need for a special advocate in charitable status cases under the *CRSIA*.[80] As well, the Committee concluded that a "due diligence" defence was not necessary to protect individuals who donated to charities or transferred money by way of the informal value transfer system known as "hawala."[81]

4.1.6 Commission of Inquiry Concerning Maher Arar

The Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar ("O'Connor Commission"), in its policy report, *A New Review Mechanism for the RCMP's National Security Activities*,[82] explored not only RCMP activities in national security matters, but also those of other parties, such as CSIS, the Integrated Threat Assessment Centre (ITAC), CSE and the Department of National Defence (DND). The O'Connor Commission also briefly considered TF issues. It recommended a revised review mechanism for the RCMP and also called for independent review of the activities of several other agencies:

> There should be independent review, including complaint investigation and self-initiated review, for the national security activities of the Canada Border Services Agency, Citizenship and Immigration Canada, Transport Canada, the Financial Transactions and Reports Analysis Centre of Canada and Foreign Affairs and International Trade Canada.[83]

---

77 Senate Report on the *ATA*, p. 92.
78 Senate Report on the *ATA*, p. 118.
79 Senate Report on the *ATA*, pp. 122.
80 Senate Report on the *ATA*, pp. 30-31.
81 Senate Report on the *ATA*, pp. 60-61.
82 (Ottawa: Public Works and Government Services Canada, 2006) [*A New Review Mechanism for the RCMP's National Security Activities*].
83 *A New Review Mechanism for the RCMP's National Security Activities*, p. 558.

The report spoke specifically about the impact of the activities of FINTRAC:

> FINTRAC's activities have the potential to significantly affect the lives of individuals. Much of the information it deals with is highly confidential. To the extent that suspected threats to national security or criminal activity are identified and information passed on to the RCMP, CSIS or a foreign agency, there could be further impacts on individual rights and interests. When creating FINTRAC, the government recognized the significant nature of these potential impacts and put in place a number of restrictions on when, to whom and how FINTRAC may disclose information. The sensitive nature of the information that FINTRAC deals with has, for good reason, resulted in an agency whose activities lack transparency. FINTRAC works in co-operation with other national security actors, such as the RCMP, CSIS and the CBSA. In my view, FINTRAC is a prime candidate for independent review.[84]

Justice O'Connor proposed that SIRC be put in charge of the review mechanism for FINTRAC.[85] He also recommended that SIRC's powers be enhanced[86] and that all review mechanisms be able to provide for the "…exchange of information, referral of investigations, conduct of joint investigations and coordination in the preparation of reports."[87] The focus of that recommendation was on an independent review mechanism to examine the propriety of FINTRAC's actions with respect to values such as lawful protections for privacy rather than on its efficacy in terms of contributing to counterterrorism.

4.1.7 2004 SIRC Review of CSIS Terrorist Financing Program

The activities of CSIS are subject to review by the Security Intelligence Review Committee (SIRC) and the Inspector General of CSIS. The SIRC mandate is focused on a review of past operations and does not involve current matters. Reviews of past activities are designed to help Parliament determine if CSIS has complied with the law and whether its activities involved any unreasonable or unnecessary exercise of its powers.[88] The *Canadian Security Intelligence Service Act*[89] (*CSIS Act) gives SIRC* broad access to CSIS information.[90]

---

84 *A New Review Mechanism for the RCMP's National Security Activities*, pp. 567-568. Commissioner O'Connor makes additional comments at pp. 569-573 as to why he recommended independent review for FINTRAC and other agencies.

85 *A New Review Mechanism for the RCMP's National Security Activities*, p. 573.

86 *A New Review Mechanism for the RCMP's National Security Activities*, p. 578.

87 *A New Review Mechanism for the RCMP's National Security Activities*, pp. 580-590.

88 Online: Security Intelligence Review Committee <http://www.sirc-csars.gc.ca/rvwetd/index-eng.html> (accessed April 21, 2009).

89 R.S.C 1985, c. C-23.

90 *Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C-23, s. 39.

In 2004, SIRC conducted a study of the investigation of TF in Canada by CSIS.[91] The conclusion to the study stated that, "…[i]n our review of [a CSIS] terrorist financing investigation, we found that the Service had reasonable grounds to suspect that the activities of targeted individuals and groups posed a threat to the security of Canada."[92]

4.2 International Reviews

According to the EKOS report mentioned above, monitoring the implementation of the AML/ATF Initiative overall is partly done through FATF self- and mutual assessments.[93] Many government officials who testified before the Commission, especially those from the Department of Finance, saw preparation for the 2008 FATF Mutual Evaluation as an important part of their international activities regarding TF. They had no doubt about the importance of the FATF review in providing oversight of Canada's anti-TF program.

4.2.1 The 2008 FATF Mutual Evaluation of Canada

4.2.1.1 Setting

In February 2008, the FATF published its *Third Mutual Evaluation on Anti-Money Laundering and Combating the Financing of Terrorism of Canada*.[94] This evaluation was a review by peers – other member countries of the FATF – to which Canada and all member countries are subject as a condition of joining the FATF.[95]

This evaluation was the third for Canada since joining the FATF, but the first to deal with the FATF's revised 2003 anti-money laundering recommendations and the Nine Special Recommendations on Terrorist Financing.[96] The evaluation itself was conducted mostly during 2007, starting with a questionnaire.[97] An on-site visit to Canada by FATF officials took place in March 2007.[98] The assessment team consisted of individuals with competence in areas such as finance, law enforcement and law,[99] and involved FATF secretariat staff and volunteers from member countries.[100] The assessment team met with many Government of Canada officials responsible for implementing the FATF recommendations, as

---

91 Exhibit P-232, Tab 2: Security Intelligence *Review Committee, Review of the CSIS Investigation of Terrorist Financing Activities in Canada* (SIRC Study 2004-10), August 5, 2005 [SIRC Study 2004-10].
92 SIRC Study 2004-10, p. 23.
93 EKOS Report on Money Laundering and Terrorist Financing, p. 36.
94 The summary was made public on February 29, 2008, and the complete document was made available a few weeks later. The summary is available onlinalso available online: Financial Action Task Force <http://www.fatf-gafi.org/dataoecd/5/3/40323928.pdf> (accessed January 16, 2009) [2008 FATF Mutual Evaluation of Canada].
95 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6779.
96 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6779.
97 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6779.
98 2008 FATF Mutual Evaluation of Canada, para. 1.
99 2008 FATF Mutual Evaluation of Canada, para. 2.
100 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6780.

well as with representatives from the provinces and private sector bodies.[101] A first draft of the evaluation report was prepared and submitted to Canada for comment, leading to further discussions between the FATF and Canada.[102]

A few weeks prior to the FATF plenary session where evaluations are adopted, they are circulated among FATF member countries.[103] There can be discussions about the evaluation before its adoption at the plenary session.[104]

The 2008 FATF Mutual Evaluation of Canada summarized the AML/ATF measures adopted by Canada.[105] More significantly, it provided an assessment of Canada's compliance with the FATF "40 + 9 Recommendations" aimed at money laundering and TF. The report was lengthy and highly technical. It provided a detailed assessment of Canada's level of compliance with all FATF recommendations.

4.2.1.2 Results

The 2008 FATF Mutual Evaluation was critical of Canada's AML/ATF Initiative and of Canada's implementation of the FATF Recommendations.[106] The executive summary stated that, "…[w]ith regard to legal measures (money laundering and TF offences, confiscation, freezing mechanisms), the legal framework is generally in line with the FATF standards; however further steps could be taken to enhance effective implementation."[107] The Evaluation was more severe in the ratings it gave to Canada's performance in meeting each FATF recommendation.

The FATF rates compliance using the following ratings: Compliant (C), Largely Compliant (LC), Partially Compliant (PC) and Non-Compliant (NC). While the FATF explains in detail the reason underlying the ratings for each recommendation,[108] the difference between the ratings can be small. Canadian officials stated that there is not much difference between the two passing ratings (C and LC), but there is between the two failing grades (PC and NC).[109]

In total, the 2008 FATF Mutual Evaluation gave Canada seven Compliant Ratings,[110] twenty-three Largely Compliant Ratings,[111] eight Partially Compliant Ratings[112]

---

101 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6780.
102 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6780.
103 Testimony of Diane Lafleur, vol. 54, September 28, 2007, pp. 6780-6781.
104 Testimony Diane Lafleur, vol. 54, September 28, 2007, p. 6781.
105 2008 FATF Mutual Evaluation of Canada, para. 3.
106 For Canada's response, see section 5.4.
107 2008 FATF Mutual Evaluation of Canada, para. 5.
108 See Table 1 of the 2008 FATF Mutual Evaluation of Canada for a summary of the ratings. They are also scattered throughout the document with their respective explanations.
109 Exhibit P-443: Summary of Meeting between Commission Counsel and Department of Finance, April 10, 2008, p. 1.
110 Of the 7 Compliant ratings, 6 related to the 40 Recommendations and 1 to the 9 Special Recommendations.
111 Of the 23 Largely Compliant ratings, 17 related to the 40 Recommendations and 6 to the 9 Special Recommendations.
112 All related to the 40 Recommendations.

and eleven Non-Compliant Ratings.[113] Although the FATF "40 Recommendations" are generally considered to be directed at money laundering, they can also be considered to apply to TF. As such, the 40 Recommendations are included in the TF assessment process, in addition to the 9 Special Recommendations which deal specifically with TF.

The rating for compliance with Recommendation 26 was of particular interest because the recommendation related to the importance and role of FIUs – in Canada's case, FINTRAC. In the 2008 FATF Mutual Evaluation, FINTRAC received a rating of PC (Partially Compliant).[114] The FATF explained this rating as follows:

1. FINTRAC has insufficient access to intelligence information from administrative and other authorities (especially from CRA, CSIS and Customs);
2. FINTRAC is not allowed by the *PCMLTFA* to gather additional financial information from reporting entities;
3. Effectiveness:

    a. The number of staff dedicated to the analysis of potential money laundering/TF cases is low, especially in comparison with the number of reports coming in, which may have an impact on the number of cases that FINTRAC generates;

    b. Feedback from law enforcement authorities outlines the relatively limited added value of FINTRAC disclosures in law enforcement investigations;

    c. The timeliness of FINTRAC disclosures to law enforcement authorities was raised as an issue at the time of the FATF's visit to Canada;

    d. Eighty per cent of the disclosures made by FINTRAC result from voluntary information received from law enforcement; only 20% result from Suspicious Transaction Reports (STRs), which raises serious concerns with respect to the capability of FINTRAC to generate money laundering/TF cases on the basis of STRs or other reports it receives from the private sector; and

    e. So far, very few, if any, convictions for money laundering or TF have resulted from a FINTRAC disclosure, a fact to be considered in any assessment of the usefulness of FINTRAC's intelligence in criminal investigations and prosecutions.[115]

---

113 Of the 11 Non-Compliant ratings, 9 related to the 40 Recommendations and 2 related to the 9 Special Recommendations.

114 The FATF recently revised the rating on Recommendation 26 to "Compliant."

115 2008 FATF Mutual Evaluation of Canada 2008, Table 1, Recommendation 26.

Canada was given an NC rating concerning FATF's Special Recommendation VI, about money/value transfer services, as well as concerning Special Recommendation VII, about wire transfer rules.

The 2008 FATF Mutual Evaluation criticized Canada for its risk assessment of financial activity sectors.[116] The Evaluation stated that Canada's approach to risk did not reflect FATF's approach. The FATF noted that Canada's approach was to cover an activity sector *only if* there was a proven risk of money laundering or TF. The FATF argued that entities in any area of activity must be covered *unless* there was "a proven low risk" of money laundering or TF. The FATF report also stated that Canada did not have a consistent methodology for evaluating the risk of TF through financial activity sectors.

4.2.2 The 1997 FATF Mutual Evaluation of Canada

The 1997 FATF Mutual Evaluation of Canada occurred before the FATF was assigned responsibility for TF matters and before the enactment of Canada's provisions on TF. The 1997 Evaluation appears to have been largely responsible for the creation of FINTRAC, since Canada did not have an FIU at the time and was criticized on that account. FINTRAC was created in 2000 and the National Initiative to Combat Money Laundering was set in motion.[117]

4.2.3 UN Counter-Terrorism Committee Reviews

UN Resolution 1373 (2001) created the United Nations Counter-Terrorism Committee (UN CTC) and required UN member states, among other things, to prevent and suppress TF, criminalize TF and freeze funds used to support terrorism.[118] All member states have an obligation to report on progress to implement that resolution (as well as on implementation of Resolution 1624 (2005), dealing with prohibition of incitement to commit terrorist acts).[119] The report is in the form of a questionnaire which is completed by member countries.

Canada has provided all the required reports. The Commission examined the 2006 report. The questionnaire for that report dealt with several terrorism-related topics, including TF. The UN CTC was interested in learning about the status of

---

116 2008 FATF Mutual Evaluation of Canada, paras. 630-640.

117 2004 Auditor General Report on Money Laundering, para. 2.8; EKOS Report on Money Laundering and Terrorist Financing, p. 2.

118 See the discussion of Resolution 1373 in Chapter I.

119 The reports submitted by the various member states can be read on the United Nations Security Council Counter-Terrorism Committee website, online: <http://www.un.org/sc/ctc/countryreports/Creports.shtml> (accessed January 15, 2009).

a registry for money services businesses (MSBs),[120] and how alternative money transfer agencies (such as hawalas) and the financial activities of charitable organizations were being monitored.[121] The questionnaire also asked about the lack of prosecutions for terrorist activities.[122]

---

120 UN CTC Report Submitted by Canada pursuant to Security Council resolution 1373 (2001) and resolution 1624 (2005), S/2006/185, Question 1.1: "The Committee acknowledges laws and regulations adopted by Canada in suppressing terrorist financing in accordance with resolution 1373 (2001). The Committee is aware that Canada has mentioned in its fourth report that it is looking at options to establish a registration or licensing system for MSBs. The Committee would be glad to know whether a licensing/registration system has been established. If so, please give the Committee an update as to its functions and legal authority.": online: United Nations Security Council Counter-Terrorism Committee <http://daccessdds.un.org/doc/UNDOC/GEN/NO6/297/90/PDF/NO629790.pdf?OpenElement> (accessed January 15, 2009) [UN CTC 2006 Report by Canada].

121 UN CTC 2006 Report by Canada, Question 1.2: "The Committee may wish to know how Canada monitors alternative money transfer agencies, such as the 'Hawala' which do not work at all through the banking system. How many such informal money transfer agencies do you believe exist? How do the Canadian authorities intend to make sure that these entities would not serve for terrorist purposes?"; Question 1.3: "The Committee is aware also that with respect to the money laundering, Canada has put in place administrative control on the financial institutions: However, the Committee would be grateful to have further clarification on the measures that Canada is employing in order to monitor the financial activities of charitable organizations. How, for example, does Canada make sure that these charitable organizations report their financial activities (donations and disbursements)? How does Canada prevent charities from being a source for misuse of funds that could be diverted to terrorist activities?"

122 UN CTC 2006 Report by Canada, Question 1.4: "Canada has also mentioned in its fourth report that since September 2001, no entities or persons have been prosecuted by the Canadian authorities in relation to terrorist activities. Could Canada please provide the Committee with an updated data relating to persons, entities, non-profit organizations being prosecuted for terrorist activities since September 2001?"

VOLUME FIVE
TERRORIST FINANCING

CHAPTER V: CANADA'S RESPONSE TO REVIEWS OF ITS ANTI-TF PROGRAM

5.1 Legislative Changes

5.1.1 Department of Finance 2005 Consultation Paper

In June 2005, the Department of Finance published a consultation paper, *Enhancing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime*, setting out the Government of Canada's proposals to strengthen the AML/ATF Initiative.[1] The paper had several objectives: meeting FATF obligations[2] generally, preparing for the 2008 FATF Mutual Evaluation, addressing the recommendations of both the EKOS and Auditor General's reports of 2004,[3] responding to the concerns of various stakeholders and, finally, preparing for the parliamentary reviews to be held in 2006-07.[4]

The paper contained proposals on substantive matters such as customer due diligence provisions, correspondent banking, electronic funds transfers, reporting of suspicious attempted transactions, sharing of information between agencies and a registration scheme for MSBs. It also proposed minor legal changes,[5] including some technical amendments.[6] The paper explained the basis for each of the proposals. For example, proposal 4.1, which recommended expanding the information contained in FINTRAC disclosures, cited both the Auditor General and the EKOS recommendations in support.[7] Proposal 3.1 called for the creation of an MSB registration system, as required by FATF's

---

1 The document can be found online: Department of Finance <http://www.fin.gc.ca/activty/pubs/enhancing_e.pdf> (accessed January 15, 2009) [Consultation Paper on AML/ATF Regime]. In the introductory paragraph, both ML and TF are mentioned. The Department states that "…[m]oney laundering is not only a serious threat to the integrity of the financial system, but it funds and creates incentives for further crime." However, it says nothing about the risks associated with TF.

2 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6778. The existing FATF obligations had been somewhat modified in 2003: see Consultation Paper on AML/ATF Regime, p. 6.

3 For example, the EKOS report stated: "However, the FATF recommendations were revised in June 2003 and Canada will now have to amend its legislative and regulatory framework to meet these new recommendations, particularly with respect to client due diligence and record keeping. This indicates a continued need for action on the part of Canada in this area.": EKOS Research Associates Inc., *Year Five Evaluation of the National Initiatives to Combat Money Laundering and Interim Evaluation of Measures to Combat Terrorist Financing* (November 30, 2004), p. 19, online: Department of Finance <http://www.fin.gc.ca/activty/pubs/nicml-incba_e.pdf> (accessed January 16, 2009) [EKOS Report on Money Laundering and Terrorist Financing].

4 Consultation Paper on AML/ATF Regime, p. 1.

5 Consultation Paper on AML/ATF Regime, pp. 39-49.

6 Consultation Paper on AML/ATF Regime, pp. 50-51.

7 Consultation Paper on AML/ATF Regime, p. 34.

Special Recommendation VI.[8] Many submissions were made in response to the consultation paper.[9]

5.1.2 Bill C-25

On October 5, 2006, Bill C-25, *An Act to amend the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and the Income Tax Act and to make a consequential amendment to another Act*, was introduced in the House of Commons.[10] The Bill received Royal Assent on December 14, 2006. Its provisions came into force in stages, over two years, and were all in force by December 2008. Officials told Commission counsel that Parliament adopted a staggered approach to bringing into force various provisions in Bill C-25 because stakeholders needed time to adapt to the changes.[11]

Bill C-25 was designed to implement changes to Canada's AML/ATF Initiative and to prepare for upcoming reviews of the Initiative, including the FATF Mutual Evaluation.[12] For example, both the Auditor General and EKOS reports had recommended that FINTRAC be permitted to increase the detail of the information contained in its disclosures to law enforcement and security intelligence agencies. Bill C-25 amended sections 55(7) and 55.1(3) of the *PCMLTFA* to allow FINTRAC to accomplish this.

Although the report of the Senate committee examining the *PCMLTFA* was published after Bill C-25 received Royal Assent, the Bill reflected several of the committee's ideas. For example, the recommendation that a registration mechanism be created for MSBs,[13] the inclusion of dealers in precious metals, stones and jewellery under the reporting requirements in the *PCMLTFA*[14] and the amendment of the *PCMLTFA* to allow FINTRAC to make fuller disclosures to law enforcement and intelligence agencies[15] – all measures eventually recommended by the Senate committee – were included in Bill C-25.

---

8 Consultation Paper on AML/ATF Regime, p. 29.

9 More than 25 submissions can be found online: Department of Finance <http://www.fin.gc.ca/activty/consult/regime_e.html> (accessed January 15, 2009). It appears that a majority of the submissions were concerned with ML issues.

10 1st Sess., 39th Parl. See online: Parliament of Canada <http://www.parl.gc.ca/LEGISINFO/index.asp?Language=E&Chamber=N&StartList=A&EndList=Z&Session=14&Type=0&Scope=I&query=4832&List=stat> (accessed January 16, 2009).

11 Exhibit P-443: Summary of Meeting between Commission Counsel and Department of Finance, April 10, 2008, p. 6.

12 See, for example, Testimony of Diane Lafleur, vol. 54, September 28, 2007, pp. 6778-6779.

13 Senate of Canada, Interim Report of the Standing Senate Committee on Banking, Trade and Commerce, *Stemming the Flow of Illicit Money: A Priority for Canada, Parliamentary Review of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, October 2006, p. 10, online: Parliament of Canada <http://www.parl.gc.ca/39/1/parlbus/commbus/senate/com-e/bank-e/rep-e/rep09oct06-e.pdf> (accessed January 16, 2009) [Senate Review of the *PCMLTFA*].

14 Senate Review of the *PCMLTFA*, p. 10.

15 Senate Review of the *PCMLTFA*, p. 16. Sections 55(7) and 55.1(7) of the *PCMLTFA* now allow FINTRAC to disclose more information, such as indicators (ss. 55(7)(n), 55.1(3)(n)), the relationships suspected by the Centre on reasonable grounds to exist between any persons or entities referred to in paragraph (a) and any other persons or entities (ss. 55(7)(h), 55.1(3)(h)) and other details.

5.2 Non-legislative Changes

The federal government responded to the Auditor General and EKOS reports through measures other than legislation as well. For instance, the Auditor General's recommendation that an anti-money laundering advisory committee be created was implemented without the need for legislative change.

The EKOS Report had recommended that a "Logic Model" for the Initiative be revisited and updated, and that an evaluation framework be updated to "… establish clear expectations around how the future success of the Initiative will be measured."[16] Diane Lafleur of the Department of Finance testified that officials had been "…working diligently in the wake of the recommendations from the Auditor General, among others, to develop a better performance framework for the initiative and that is ongoing work right now."[17] A document on the topic, *Evaluation Framework for the AML/ATF Regime*, was prepared for the Department of Finance at the end of 2007. It attempted to create a model to evaluate the Initiative.

5.3 Government Response to the *Anti-terrorism Act* Review

The Government of Canada responded to the House of Commons report, *Rights, Limits, Security: A Comprehensive Review of the Anti-Terrorism Act and Related Issues*.[18] The response was in part as follows:[19]

> [16][20] The solicitor-client privilege should not be used to conceal property and, accordingly, the Government rejected Committee's proposal to exempt the legal profession from the requirements of section 83.1 of the *Criminal Code*;[21]
>
> [17] The *mens rea* element as required by section 83.12 of the *Criminal Code* was sufficient and a due diligence defence was not necessary;[22]

16 EKOS Report on Money Laundering and Terrorist Financing, p. 55.

17 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6765.

18 The House of Commons Canada, Final Report of the Standing Committee on Public Safety and National Security, Subcommittee on the Review of the *Anti-terrorism Act, Rights, Limits, Security: A Comprehensive Review of the Anti-terrorism Act and Related Issues*, March 2007, online: Parliament of Canada <http://www2.parl.gc.ca/content/hoc/Committee/391/SECU/Reports/RP2798914/sterrp07/sterrp07-e.pdf> (accessed May 25, 2009) is discussed in section 4.1.4. The request for response is found at p. 113 of the report. The *Response of the Government of Canada to the Final Report of the Standing Committee on Public Safety and National Security, Subcommittee on the Review of the Anti-terrorism Act, Rights, Limits, Security: A Comprehensive Review of the Anti-terrorism Act and Related Issues* is found online: Parliament of Canada <http://cmte.parl.gc.ca/Content/HOC/committee/391/secu/govresponse/rp3066235/391_SECU_Rpt07_GR/391_SECU_Rpt07_GR-e.pdf> (accessed May 25, 2009) [Canada Response to House of Commons Report on the *ATA*].

19 These are the responses which are most relevant to TF matters. Some technical changes, such as the House of Commons Recommendation 32, were accepted by the government and were not reproduced in that listing.

20 The numbers in the square brackets are the recommendation numbers.

21 Canada Response to House of Commons Report on the *ATA*, p. 8.

22 Canada Response to House of Commons Report on the *ATA*, p. 9.

> [23] The Government wished to maintain the current listing system, with multiple lists, because each listing complements the others and because several other countries, such as Australia, the US and the UK, maintain separate listing systems;[23]
>
> [24] Enabling an entity to make a direct application for judicial review to challenge a listing under the *Criminal Code* listing process without first applying to the Minister of Public Safety would run counter to the goal of effective and timely decision-making;[24] and
>
> [26] The creation of an automatic "delisting" system that would de-list individuals or entities after a set period of time could result in Canada failing to comply fully with its international obligations.[25]

5.4 Government Response to the 2008 FATF Mutual Evaluation of Canada

On February 29, 2008, the Minister of Finance issued a news release stating that "…[w]hen the actions the Government has taken recently are fully implemented, Canada will be compliant with virtually all of the FATF's Recommendations."[26]

After the FATF's on-site visits to various Canadian agencies in the course of conducting its evaluation, Canadian officials were shown a copy of the draft of the FATF Mutual Evaluation for comment. A series of discussions followed between Canadian and FATF officials, leading up to the FATF plenary meeting in February 2008, where the Evaluation was adopted. During these discussions, Canadian officials made their case about several of the FATF's proposed ratings, a common practice. Representatives from the Canadian agencies responsible for Canada's response to the FATF Mutual Evaluation, including law enforcement and FINTRAC officials, attended the February plenary.

Some descriptions of the anti-TF program that Canadian stakeholders gave to FATF during its on-site visits were outdated by the time of the FATF plenary meeting, since legislative and other changes had been made to the Canadian program in the interval. This was one reason for the concern of Canadian officials about the criticisms. For example, the FATF Evaluation stated that, "…[a]t the time of the on-site visit, the feedback provided by some organizations that receive FINTRAC disclosures was generally negative (unsatisfactory timelines for disclosures, relatively limited added value of FINTRAC disclosures

---

23 Canada Response to House of Commons Report on the *ATA*, p. 12.
24 Canada Response to House of Commons Report on the *ATA*, p. 12.
25 Canada Response to House of Commons Report on the *ATA*, p. 12.
26 "Canada Makes Progress in Combatting Money Laundering and Terrorist Financing" (February 29, 2008), online: Department of Finance <http://www.fin.gc.ca/news08/08-023e.html> (accessed January 15, 2009) ["Canada Makes Progress in Combatting Money Laundering and Terrorist Financing"].

in law enforcement investigations, FINTRAC disclosures positively contributed to existing investigations but rarely generated new ones)."[27] The FATF did not appear to take into account the implementation of provisions from Bill C-25, which increased the amount of information that FINTRAC must disclose to law enforcement and security intelligence agencies.[28]

Table 3 of the FATF Mutual Evaluation, "Authorities' Response to the Evaluation,"[29] summarizes Canada's response. Canada commented on each recommendation for which Canada received a rating of Non-Compliant (NC), and on almost all recommendations for which Canada received a Partially Compliant (PC) rating. Canada's response was often to cite upcoming legislative changes and their date of coming into force and contained the following general statement:

Legislative amendments to the *PCMLTFA* passed in December 2006 and associated regulations enacted in June 2007 and December 2007 will address a substantial number of deficiencies identified in this report. Please see Annex 1 for a detailed list of legislative and regulatory amendments to Canada's AML/CFT regime that came into force after June 2007 and have not been considered in this evaluation. Canada's regulations allow a period of time between enactment and coming into force to provide an opportunity for businesses and sectors to modify systems.[30]

The Annex referred to in Canada's response is reproduced immediately below.

---

27 Financial Action Task Force, *Third Mutual Evaluation on Anti-Money Laundering and Combating the Financing of Terrorism, Canada*, February 29, 2008, para. 21, online: Financial Action Task Force <http://www.fatf-gafi.org/dataoecd/5/3/40323928.pdf> (accessed April 1, 2009) [2008 FATF Mutual Evaluation of Canada].

28 "Canada Makes Progress in Combatting Money Laundering and Terrorist Financing."

29 2008 FATF Mutual Evaluation of Canada, pp. 308-310.

30 2008 FATF Mutual Evaluation of Canada, p. 308.

ANNEX 1

Legislative and regulatory Changes to the Canadian AML/CFT regime

Amendment	Legislation Enacted	Regulations Enacted	Measure Fully In Force
Extending record retention time period for FINTRAC	Dec 14, 2006	n/a	Feb 10, 2007
Enhanced information sharing on non-profit organisations	Dec 14, 2006	n/a	June 30, 2007
Enhanced FINTRAC disclosure information	Dec 14, 2006	June 27, 2007	June 30, 2007
Prohibition against correspondent relationships with shell banks	Dec 14, 2006	June 27, 2007	June 30, 2007
Correspondent banking due diligence requirements	Dec 14, 2006	June 27, 2007	June 30, 2007
Explicit prohibition on opening accounts for unidentified customers	Dec 14, 2006	n/a	June 23, 2008
Application to foreign branches or subsidiaries	Dec 14, 2006	n/a	June 23, 2008
Non-face-to-face CDD measures	n/a	June 27, 2007	June 23, 2008
Use of an agent or mandatary for customer identification (clarifying provision)	n/a	June 27, 2007	June 23, 2008
Beneficial owner requirements	n/a	June 27, 2007	June 23, 2008
Enhancing CDD and Record Keeping	Dec 14, 2006	June 27, 2007	June 23, 2008
PEPs requirement for financial institutions	Dec 14, 2006	June 27, 2007	June 23, 2008
Special attention to complex and unusual transactions (*i.e.* risk assessment)	Dec 14, 2006	June 27, 2007	June 23, 2008
Reporting suspicious attempted transactions	Dec 14, 2006	June 27, 2007	June 23, 2008
Special attention to business from countries of risk (*i.e.* risk assessment)	Dec 14, 2006	June 27, 2007	June 23, 2008
MSB registration	Dec 14, 2006	June 27, 2007	June 23, 2008
Wire transfers travel rule	Dec 14, 2006	June 27, 2007	June 23, 2008
Enhancing measures for casinos, accountants and real estate, including: • Enhanced CDD and record-keeping. • Non face to face measures. • Use of agent and mandatary. • Special attention to transactions.	Dec 14, 2006	June 27, 2007	June 23, 2008
Inclusion of Lawyers, BC Notaries and Jewellers, including measures on: • CDD and record-keeping. • Non face to face measures. • Use of agent and mandatary. • Special attention to transactions. • Triggers for STR reporting (except lawyers). • Coverage by FINTRAC to ensure compliance.	Dec 14, 2006	Dec 2007	Dec 2008
Administrative Monetary Penalties provisions	Dec 14, 2006	Dec 2007	Dec 2008
Application to businesses and professions at risk (real estate developers)	n/a	Feb 2008	Feb 2009

As an example, the FATF gave Canada a Non-Compliant rating for its failure to comply with Special Recommendations dealing with money services businesses (MSBs) and wire transfers. The Annex showed that MSB registration regulations would come into force in June 2008 (to comply with Special Recommendation VI)[31] as would regulations concerning wire transfers (to comply with Special Recommendation VII).[32]

Many FATF recommendations were similar to those flowing from domestic reviews of the anti-TF program. Several recommendations took an approach similar to the following: "Canada should ensure that the new provisions enacted in June 2007 are fully in line with the FATF requirements and ensure that reporting entities implement measures that meet the FATF standards."[33] This showed the FATF's awareness that several deficiencies had been remedied by more recent legislative changes.

After the plenary meeting adopted the Mutual Evaluation of Canada in February 2008, Canada requested one year to show that it was in fact complying with many of the obligations about which it had received criticism. Since the last of Bill C-25's changes to the anti-TF program came into force in December 2008, Canada will be able to state clearly the extent to which it complies in practice, and not merely theoretically, with FATF recommendations. Even so, the NC and PC ratings given in the 2008 Evaluation will not change since the FATF does not have a procedure for modifying these ratings.

5.5 Conclusion

International and domestic reviews of Canada's anti-TF program have led to improvements in the program. These reviews have shown the government and Canadian agencies, with the Department of Finance in the lead, to be willing to correct deficiencies. However, the length of time required to restructure the anti-TF program remains a significant concern. The process that led to the introduction of Bill C-25 in October 2006 began after EKOS and the Auditor General identified deficiencies in late 2004. In 2005, the Department of Finance issued a consultation paper about the AML/ATF Initiative, albeit with more emphasis on money laundering issues. Consultations with various stakeholders occurred during 2005 and 2006. Bill C-25 received Royal Assent in December 2006. Its provisions came into force over a two-year period, with the last provisions coming into effect in December 2008, more than four years after the EKOS and Auditor General reports.

---

31 2008 FATF Mutual Evaluation of Canada, p. 309.
32 2008 FATF Mutual Evaluation of Canada, p. 309.
33 2008 FATF Mutual Evaluation of Canada, p. 302.

VOLUME FIVE
TERRORIST FINANCING

CHAPTER VI: THE LINKS BETWEEN THE CHARITABLE SECTOR AND TERRORIST FINANCING

6.1 Charities and Terrorist Financing Generally

Charities and not-for-profit organizations (NPOs)[1] around the world can be misused to facilitate TF, either with or without the knowledge of those operating or contributing to the organizations. Among the many ways that charities and NPOs can be misused are the following:

1. Their apparent legitimacy allows charities and NPOs to raise funds in many different areas of the world, especially those plagued by conflict;[2]
2. Transferring funds to other countries may make it easier for charities and NPOs to avoid accountability for the use of those funds;[3]
3. Charities and NPOs have a long history of important work and are seen as vital parts of society. Organizations interested in raising funds for terrorism can gain credibility simply by calling themselves charities or NPOs, or by becoming registered with government authorities as charities. This credibility helps these organizations to raise funds;[4]
4. Some charities and NPOs can reach large numbers of donors to raise funds;
5. The activities of charities and NPOs are often cash-intensive, making it difficult for authorities to track uses of the funds;[5]
6. Registered charities can issue tax receipts, thus allowing donors to reduce the cost to themselves of giving to the charity;[6]
7. Registered charities and NPOs may receive tax benefits[7] which leave them with additional funds to support terrorism; and
8. Charities and NPOs may be able to launder money to hide its intended improper uses.[8]

---

1 The differences in Canada between NPOs and registered charities are described below.
2 Financial Action Task Force, *Terrorist Financing*, February 29, 2008, p. 8, online: Financial Action Task Force <http:/www.fatf-gafi.org/dataoecd/28/43/40285899.pdf> (accessed February 12, 2009) [FATF Report on Terrorist Financing]; Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6863.
3 Testimony of Kenneth Dibble, vol. 59, October 9, 2007, p. 7297.
4 Testimony of Maurice Klein, vol. 57, October 3, 2007, p. 7121.
5 FATF Report on Terrorist Financing, p. 11.
6 At the hearings, the Commissioner expressed doubt that an individual inclined to finance terrorist organizations would be deterred by the lack of a tax receipt: Transcripts, vol. 54, September 28, 2007, p. 6809.
7 Testimony of Maurice Klein, vol. 57, October 3, 2007, p. 7122.
8 Testimony of Nikos Passas, vol. 53, September 27, 2007, p. 6579.

The international community is well aware of the misuse of charitable or non-profit status for TF. When the Financial Action Task Force (FATF) expanded its mission in 2001 to include TF, it issued a special recommendation on NPOs (Special Recommendation VIII) as part of its "Nine Special Recommendations on Terrorist Financing." Special Recommendation VIII spoke of non-profit organizations (which would include charities in the context of the recommendation) being "particularly vulnerable" to abuse:

> Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Non-profit organisations are particularly vulnerable, and countries should ensure that they cannot be misused:
>
> - by terrorist organisations posing as legitimate entities;
> - to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; and
> - to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.[9]

Some charitable organizations in Canada and elsewhere have long been suspected of helping terrorists[10] by raising and helping to move funds. However, as with the extent of TF in general, it is difficult to determine the extent of TF involving charities and NPOs.

Donna Walsh, Director of the Review and Analysis Division in the Charities Directorate of the Canada Revenue Agency (CRA), testified that it was not possible to state how many registered charities could be or are involved in TF.[11] However, some rough indications were available. In its 2006 Annual Report, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) reported that a third of its disclosures of "designated information" to law enforcement

---

9 "9 Special Recommendations (SR) on Terrorist Financing (TF)," VIII: Non-profit organisations, online: Financial Action Task Force <http://www.fatf-gafi.org/document/9/0,3343,en_32250379_32236920_34032073_1_1_1_1,00.html#VIIINonprofit> (accessed February 12, 2009) [FATF Special Recommendation VIII: Non-profit organisations].

10 For example, see the discussion of fundraising in chapter 2 of Senate of Canada, Special Committee on Security and Intelligence, "The Report of the Special Senate Committee on Security and Intelligence" (January 1999), online: Parliament of Canada <http://www.parl.gc.ca/36/1/parlbus/commbus/senate/com-e/secu-e/rep-e/repsecintjan99part2-e.htm#Fundraising> (accessed March 3, 2009).

11 Testimony of Donna Walsh, vol. 57, October 3, 2007, p. 7127. Similar remarks appear in Testimony of Kenneth Dibble, vol. 59, October 9, 2007, p. 7294. "Registered charities" are those charities that have been granted charitable status by the CRA.

and intelligence agencies related to a charity or NPO in some capacity.[12] RCMP Superintendent Rick Reynolds testified that "a significant number" of major TF investigations in Canada involved a charity or NPO "…in some context…. [p]erhaps not in fundraising but in some context…either wittingly or unwittingly … and some of them may be very minor in nature…."[13]

Professor David Duff of the Faculty of Law at the University of Toronto testified that there were a number of allegations that money from some Canadian Sikh temples was improperly diverted during the 1990s for terrorist purposes.[14] The Babbar Khalsa, which both CSIS and the RCMP believed to be centrally implicated in the Narita and Air India bombings and terrorist acts and plots in both Canada and India, managed to obtain charitable status in the early 1990s, although its charitable status was revoked in 1996.[15]

Blake Bromley, a Canadian lawyer practising exclusively on charities issues, testified that concern long ago about funds from Canadian charities being used for political causes in India led that country to enact laws to restrict the flow of funds:

> …Indian legislation aimed at restricting the flow of charitable funds to finance terrorism was passed a quarter century before the post 9/11 global war on terrorism, and it was aimed specifically at Canadian donors supporting the political cause espoused by the bombers of Air India flight 182. India was worried about donations coming from Canadian charities to fund the political struggle in Khalistan. Nine years before the bombing of Air India flight 182, India passed the *Foreign Contributions (Regulation) Act*, 1976 to regulate the acceptance and utilization of charitable contributions from foreign countries.[16]

---

12 Financial Transactions and Reports Analysis Centre of Canada, *FINTRAC 2006 Annual Report*, p. 19, online: Financial Transactions and Reports Analysis Centre of Canada <http://www.fintrac.gc.ca/publications/ar/2006/AR-eng.pdf> (accessed February 12, 2009). This assessment was based on a review of 120 disclosures of suspected terrorist activity financing and other threats to the security of Canada. Some 32 per cent of the NPOs were found to be registered Canadian charities, 7 per cent were Canadian NPOs not registered as charities and 61 per cent were foreign NPOs.

13 Testimony of Rick Reynolds, vol. 55, October 1, 2007, pp. 6864-6865. The *Royal Canadian Mounted Police Departmental Performance Report for the period ending March 31, 2006* also stated at p. 62 that "Furthermore, it is important to note that the majority of terrorist financing involves registered charities": online: Treasury Board of Canada Secretariat <http://www.tbs-sct.gc.ca/dpr-rmr/0506/RCMP-GRC/rcmp-grc-eng.pdf> (accessed February 24, 2009) [2005-06 RCMP Departmental Performance Report].

14 Testimony of David Duff, vol. 85, November 29, 2007, p. 10890.

15 Testimony of David Duff, vol. 85, November 29, 2007, p. 10890; David G. Duff, "Charities and Terrorist Financing: A Review of Canada's Legal Framework" in Vol. 2 of Research Studies: Terrorism Financing Charities and Aviation Security, p. 201 [Duff Paper on Charities and Terrorist Financing].

16 Blake Bromley, "Funding Terrorism and Charities," October 26, 2007, p. 3, online: Benefic Group <http://www.beneficgroup.com/files/getPDF.php?id=120> (accessed May 12, 2009) [Bromley Paper on Funding Terrorism and Charities].

> Charitable organizations have been identified as supporting terrorism in some American TF prosecutions, notably those involving the Benevolence International Fund and the Holy Land Foundation.

The 9/11 Commission reported that, before the 9/11 attacks, Al Qaida relied on diversions of funds from Islamic charities and on financial facilitators who gathered money from witting and unwitting donors located primarily in the Arabian Gulf region.[17]

One witness from the UK, Kenneth Dibble of the England and Wales Charity Commission, stated that "...with over 190,000 registered charities [in the UK], the incidence of terrorist abuse for charities is very, very low."[18]

6.2 Overview of the Charitable Sector in Canada[19]

In Canada, the federal government encourages charitable giving by allowing registered charities to issue income tax receipts to donors and by exempting charities from the obligation to pay certain taxes. Because these measures reduce government revenues, the government has an interest in ensuring that benefits accrue only to organizations that truly qualify as charities under Canadian law. In a paper prepared for the Commission, Professor Duff concluded that the federal government had foregone $2 billion in revenue in 2003 because of the tax benefits arising from donations to registered charities. He estimated that foregone revenues could increase to about $2.5 billion in 2008.[20] The federal interest in charities also increasingly flows from another concern – that some charities may be involved in TF.

There are about 83,000 registered charities in Canada.[21] Their annual revenues total more than $US5.5 billion.[22] The 2008 Financial Action Task Force (FATF) Mutual Evaluation of Canada reported that 95 per cent of the value of all donations made to the non-profit organization (NPO) sector in Canada goes to registered charities.[23]

---

17 National Commission on Terrorist Attacks Upon the United States, *Monograph on Terrorist Financing*, pp. 19-21, online: National Commission on Terrorist Attacks Upon the United States <http://govinfo.library.unt.edu/911/staff_statements> (accessed February 20, 2009).

18 Testimony of Kenneth Dibble, vol. 59, October 9, 2007, p. 7300.

19 For an in-depth review of Canada's regime as it relates to charitable organizations, see Duff Paper on Charities and Terrorist Financing.

20 Duff Paper on Charities and Terrorist Financing, pp. 206-207. Duff quotes the Department of Finance, *Tax Expenditures and Evaluations* (Ottawa: Her Majesty the Queen in Right of Canada, 2006), pp. 17, 26 as the source of this information.

21 Testimony of Donna Walsh, vol. 57, October 3, 2007, p. 7099; Testimony of David Duff, vol. 85, November 29, 2007, p. 10893.

22 Financial Action Task Force, *Third Mutual Evaluation on Anti-Money Laundering and Combating the Financing of Terrorism*, Canada, February 29, 2008, para. 1412, online: Financial Action Task Force <http://www.fatf-gafi.org/dataoecd/5/3/40323928.pdf> (accessed March 2, 2009) [2008 FATF Mutual Evaluation of Canada].

23 2008 FATF Mutual Evaluation of Canada, para. 1412.

Registered charities in Canada range from large, often international, groups with Canadian operations, to smaller community charities. The majority have five or fewer employees, receive less than $100,000 in annual revenues[24] and depend on volunteer work.[25] Most charities in Canada do not carry out international activities.

6.3 The Vulnerability of the Canadian Charitable Sector to Being Used for Terrorist Financing

Canada has made efforts to assess the vulnerability of the charitable sector to being used for TF.[26] Bromley told the Commission that he saw "…a potential problem with charities funding terrorism which needs to be brought out in the open and discussed with the communities that are most vulnerable."[27] Kenneth Dibble explained that there was a fine line between giving money to a charity for humanitarian purposes and giving for ideological purposes. Donors may give to a charity expecting it to alleviate poverty, only to have part of the funds go to terrorists. Some charities, he said, may be the only aid organizations in a particular part of the world, and terrorists themselves might benefit from the hospitals and other services that the charities provide. Dibble spoke of the need for clarity in the rules for charities to prevent terrorist groups from benefiting from the funds held by charities.[28]

6.4 Regulating the Charitable Sector in Canada

Canada relies heavily on the federal government to monitor charities. Historically, the provinces have done little to regulate charities despite their clear constitutional role. Under section 92(7) of the *Constitution Act*, 1867,[29] provinces may exclusively make laws for the establishment, maintenance and management of charities. However, very few have done so. Even among those that regulate charities in some way, there is no uniform approach.

Professor Duff described the constitutional situation:

> [P]rovincial legislatures in Canada are granted exclusive authority to make laws in relation to: "The Establishment, Maintenance, and Management of … Charities, and Eleemosynary [pertaining to charity] Institutions in and for the Province." In addition, provinces have exclusive jurisdiction over "Property and Civil Rights in the Province" – allowing them

24 Testimony of David Duff, vol. 85, November 29, 2007, p. 10891.
25 Duff Paper on Charities and Terrorist Financing, p. 207.
26 See 2008 FATF Mutual Evaluation of Canada, paras. 1413-1414 for a brief summary of the efforts in this regard.
27 Bromley Paper on Funding Terrorism and Charities, p. 24.
28 Testimony of Kenneth Dibble, vol. 59, October 9, 2007, pp. 7293, 7297.
29 (U.K.), 30 & 31 Vict., c. 3, reprinted in R.S.C. 1985, App. II, No. 5.

> to regulate the transfer and use of property for charitable purposes. Federal jurisdiction over charities, on the other hand, is limited to the incidental powers that the Parliament of Canada derives from its taxation power. To the extent that the [*Income Tax Act*] confers special tax benefits on charities and their contributors, supervision and regulation of charities in order to ensure that they satisfy the terms on which these benefits are conferred constitutes a legitimate exercise of this federal power. While provincial governments have broad powers to regulate charities and charitable property, therefore, federal jurisdiction to supervise and regulate charities is limited to conferral of fiscal benefits under the *ITA*.[30] [References to footnotes omitted]

6.4.1 The Federal Government as the De Facto Regulator

Because of constitutional limits on Parliament's powers, the CRA's regulatory jurisdiction over charities is more limited than that of the provinces.[31] Despite this, the federal government over time became the *de facto* primary regulator of charities.[32] The CRA has regulated charities in Canada since the process for registering as a charity was established in 1967.[33] It has done this through its taxation power,[34] in recent years sometimes denying or revoking charitable status in part due to suspicions that the organization was involved with TF.

The CRA has begun an initiative and established working groups on charity-related matters with the provinces, but TF is not being addressed.[35] One impediment to cooperation with the provinces arises from CRA's obligation to comply with confidentiality provisions, primarily those in the *Income Tax Act*[36] (*ITA*), that limit the disclosure of some types of information about charities.[37]

6.4.2 The Provincial Role in Dealing with Charities

The provinces have the exclusive right under the *Constitution Act*, *1867* to make laws to establish, maintain and manage charities. Professor Duff noted that only Ontario has enacted specific legislation:

> Notwithstanding their constitutional authority to regulate charities and charitable donations, most provinces have either chosen not to exercise this jurisdiction, or have done

---

30 Duff Paper on Charities and Terrorist Financing, p. 203. For more on the constitutional framework, see generally, Duff Paper on Charities and Terrorist Financing.
31 Duff Paper on Charities and Terrorist Financing, pp. 203-204.
32 Testimony of David Duff, vol. 85, November 29, 2007, p. 10894.
33 Testimony of David Duff, vol. 85, November 29, 2007, p. 10895; Exhibit P-236, Tab 4: Canada Revenue Agency Presentation: "Canada's Charities and Anti-terrorism Measures," October 3, 2007 [CRA Presentation on Canada's Charities and Anti-terrorism Measures].
34 *Constitution Act*, 1867 (U.K.), 30 & 31 Vict., c. 3, s. 91(3).
35 Testimony of Terry de March, vol. 57, October 3, 2007, pp. 7160-7161.
36 R.S.C. 1985, c. 1 (5th Supp.).
37 Testimony of Terry de March, vol. 57, October 3, 2007, p. 7161.

> so only sparingly.[38] Although a few provinces have enacted legislation regarding charitable fundraising, and provincial Attorneys-General have the right and duty to supervise and assist charities under their *parens patriae* jurisdiction as representatives of the Crown, only Ontario has enacted specific legislation regulating the operation of charitable organizations and the use of charitable property in the province.[39]

A recent Ontario government discussion paper explains the origins of Ontario's regulation of charities:

> In Ontario the Attorney General's powers were codified and expanded with the enactment of the *Charities Accounting Act* in 1915. In 1919 with the enactment of the *Public Trustee Act*, the *Charities Accounting Act* was amended to give the statutory supervisory authority to the Public Trustee, renamed the Public Guardian and Trustee in 1995.[40] [References omitted.]

However, the Ontario Public Guardian and Trustee is not a regulator of charities. It has very little power to make decisions in this area. It has no registration listings and does not grant charitable status.[41] Still, it has authority over all charitable property, no matter who or what entity holds the property.[42]

The Ontario *Charities Accounting Act*[43] is primarily concerned with standing and procedure rather than with substantive legal standards for the proper administration of charitable property.[44] Unlike the UK system, where a charities commission operates as a quasi-judicial body, the Ontario model is "court-centred."[45]

The provincial Crown also has a *parens patriae* jurisdiction for supervising charitable property, but that power is seldom exercised. Thus, the provincial Crown has had a longstanding right and duty to supervise and come to the assistance of charities.[46] However, a 1996 Supreme Court decision held that

---

38 Duff mentions the *Charitable Fund-raising Act*, R.S.A. 2000, c. C-9 (Alberta), *The Charities Endorsement Act*, C.C.S.M. c. C60 (Manitoba) and *The Charitable Fund-raising Businesses Act*, S.S. 2002, c. C-6.2 (Saskatchewan): Duff Paper on Charities and Terrorist Financing, p. 203, note 18.

39 Duff Paper on Charities and Terrorist Financing, p. 203.

40 Exhibit P-384, Tab N: Ken Goodman, "Discussion Paper: Mandate of the Public Guardian and Trustee" (Ontario), January 2004, p. 2 [Discussion Paper on Mandate of the Ontario Public Guardian and Trustee].

41 Discussion Paper on Mandate of the Ontario Public Guardian and Trustee, pp. 3-4.

42 Discussion Paper on Mandate of the Ontario Public Guardian and Trustee, p. 4.

43 R.S.O. 1990, c. C.10.

44 Discussion Paper on Mandate of the Ontario Public Guardian and Trustee, p. 10.

45 Discussion Paper on Mandate of the Ontario Public Guardian and Trustee, pp. 2, 10. For a more thorough overview of the British, American and Australian regimes relating to the regulation and supervision of charities, see Mark Sidel, "Terrorist Financing and the Charitable Sector: Law and Policy in the United Kingdom, the United States, and Australia" in Vol. 2 of Research Studies: Terrorism Financing Charities and Aviation Security [Sidel Paper on Terrorist Financing and the Charitable Sector].

46 Discussion Paper on Mandate of the Ontario Public Guardian and Trustee, pp. 1-2.

the *parens patriae* concept does not exist as such in Quebec, since the concept emanates from the common law.[47]

Corporate registries (provincial or federal) also exercise very limited control over the activities of incorporated charities. These registries do not investigate TF issues. For the most part, they receive annual returns and related forms from registered corporate bodies. These forms provide limited information.

6.5 Canada's Efforts to Curb the Misuse of Registered Charities for Terrorist Financing

6.5.1 The Charities Directorate of the Canada Revenue Agency

The CRA is the federal agency that oversees registered charities in Canada as part of its mandate to implement Canada's tax system. Its Charities Directorate was created to deal with registered charities, especially regarding the benefits and tax treatment they receive. Through the Directorate, CRA registers qualifying organizations as charities and provides technical advice on their operation. It also undertakes audit and compliance activities.[48]

The 2008 FATF Mutual Evaluation of Canada found that the compliance program of the Charities Directorate is largely based on information from annual returns from charities, internal analysis of trends in the charitable sector, complaints from the public and tips from informants.[49]

Before 9/11, there was no counterterrorism function in the Directorate or in the CRA as a whole.[50] In 2004, the Review and Analysis Division (RAD) was created within the Charities Directorate and charged mainly with TF issues.[51] A senior position was later added to the RAD to deal with terrorism issues – Senior Advisor, Anti-terrorism and Charities Directorate.

The Charities Directorate has made an effort to hire staff with diverse backgrounds, such as defence intelligence, law enforcement, security intelligence and law, and with experience from international agencies and FINTRAC.[52] Many employees also have credentials in forensic investigation and are able to speak other languages, including Farsi, Arabic, Spanish and Urdu.[53]

Maurice Klein, Senior Advisor, Anti-terrorism and Charities Directorate, testified about the challenges inherent in identifying TF done by charities:

---

47 *W.(V.) v. S.(D.)*, [1996] 2 S.C.R. 108 at para. 59.
48 Canada Revenue Agency, "Charities and Giving," online: Canada Revenue Agency <http://www.cra-arc.gc.ca/tx/chrts/menu-eng.html> (accessed March 3, 2009).
49 2008 FATF Mutual Evaluation of Canada, para. 1419.
50 Testimony of Donna Walsh, vol. 57, October 3, 2007, p. 7109.
51 Testimony of Donna Walsh, vol. 57, October 3, 2007, p. 7098.
52 Testimony of Donna Walsh, vol. 57, October 3, 2007, p. 7115.
53 Testimony of Donna Walsh, vol. 57, October 3, 2007, p. 7115.

> [T]he enormous amounts of money that are donated to charities each year, combined with the fact that we have 83,000 registered charities currently operating in Canada, make the diversion of relatively smaller amounts of funds more difficult to detect.[54]

Charities in Canada can be monitored or investigated in at least three ways. First, individuals linked with charities, or the charities themselves, can be monitored by law enforcement and security intelligence agencies. Second, FINTRAC may receive reports of activities relating to charities. FINTRAC, in turn, might conclude that it must send designated information to law enforcement and security intelligence bodies or to the CRA, which may then conduct further monitoring or investigations. Finally, CRA might decide on its own that a registered charity or applicant for charitable status could have ties to terrorism.

6.5.2 The Legal Regime Governing Registered Charities

The CRA, in dealing with registered charities, is guided by three statutes: the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*[55] (*PCMLTFA*), the *Charities Registration (Security Information) Act*[56] (*CRSIA*) and the *ITA*.[57] CRA defines its approach in fighting TF as being to "…change the risk equation" and "…[take] away 'enabling conditions.'"[58] CRA considers that it has "…a responsibility to mitigate and manage the risk of terrorist involvement in the registration system."[59] A CRA briefing document explains several ways in which the CRA can help counterterrorism efforts and limit TF:

- identifying linkages between individuals and organizations;
- identifying charities operating in countries or regions of concern regarding terrorist activities;
- identifying "money trails";
- countering the ability of terrorist supporters to take over existing legitimate charities; and
- discovering predictive patterns and indicators of risk.[60]

In addition, the CRA's power to deny charitable status allows it (and government as a whole) to dissociate itself from, and denounce, charities that may be involved in TF. Denial of charitable status amounts at least to symbolic disapproval by

---

54 Testimony of Maurice Klein, vol. 57, October 3, 2007, pp. 7121-7122.
55 S.C. 2000, c. 17.
56 S.C. 2001, c. 41, s. 113.
57 Testimony of Donna Walsh, vol. 57, October 3, 2007, p. 7105.
58 CRA Presentation on Canada's Charities and Anti-terrorism Measures, slides 9, 20.
59 Exhibit P-236, Tab 9: Canada Revenue Agency, "Managing and Mitigating Risk of Terrorist Involvement," p. 1 [CRA Document on Managing and Mitigating Risk of Terrorist Involvement].
60 CRA Presentation on Canada's Charities and Anti-terrorism Measures, slide 18.

government and can be a signal to potential supporters of a charity to distance themselves from it.[61]

6.5.2.1 Limitations on Disclosure by CRA

The CRA must obey stringent rules about the confidentiality of taxpayer information. It can disclose information only in limited cases. These limitations are set out in the *ITA* and *PCMLTFA* and have limited even the information available to this Commission.[62] These confidentiality rules do not, however, limit the ability of the CRA to *receive* information from intelligence and law enforcement agencies.

Some information held by CRA can be disclosed publicly, such as information regarding applications for registered status, annual returns of charities, directors' names, financial statements and letters revoking charitable status.[63] This information may relate to current or former registered charities and is accessible either on the CRA's website or, for financial information about a specific charity, on request to CRA.[64]

6.5.2.2 Becoming a Registered Charity: Application and Registration Processes

A major part of the CRA's work to counter TF occurs during the review of applications for registered charity status. Ms. Walsh told the Commission that the CRA had committed additional resources to ensure "…early detection through specialized screening and analysis."[65] She said, however, that the CRA was not the first defence against terrorism, but that its work does help to support other agencies such as the RCMP and CSIS.[66]

Section 248(1) of the *ITA* defines "registered charity" as follows:

> (a) a charitable organization, private foundation or public foundation, within the meanings assigned by subsection 149.1(1), that is resident in Canada and was either created or established in Canada, or
>
> (b) a branch, section, parish, congregation or other division of an organization or foundation described in paragraph (a), that is resident in Canada and was either created or established in Canada and that receives donations on its own behalf,

---

61 See p. 166 of the Sidel Paper on Terrorist Financing and the Charitable Sector for a discussion of how the UK Charity Commission was able to remove Abu Hamza from the Finsbury Park Mosque.

62 The matter was discussed before the Commission on October 3, 2007. However, CRA officials prepared several "sanitized" cases for the Commission to help it understand CRA's work.

63 CRA Presentation on Canada's Charities and Anti-terrorism Measures, slide 8.

64 Testimony of Donna Walsh, vol. 57, October 3, 2007, pp. 7102-7103. Exceptions are the home addresses, telephone numbers and dates of birth of the charity's directors.

65 Testimony of Donna Walsh, vol. 57, October 3, 2007, p. 7114.

66 Testimony of Donna Walsh, vol. 57, October 3, 2007, p. 7187.

that has applied to the Minister in prescribed form for registration and that is at that time registered as a charitable organization, private foundation or public foundation.

The Act requires that charitable organizations and charitable foundations be exclusively charitable and that their resources be used for charitable activities or for charitable purposes.[67] Professor Duff wrote that Canadian courts have generally sought guidance in the common law of trusts to interpret the terms "charitable activities" and "charitable purposes." Specifically, the purposes of the organization must fall within one or more of the following categories, known as the "Pemsel" categories (from a 19th century House of Lords case of that name[68]):

- the relief of poverty;
- the advancement of education;
- the advancement of religion; or
- other purposes beneficial to the community in a way the law regards as charitable.[69]

Seeking to achieve political purposes generally renders an applicant ineligible for charitable registration. A CRA document explains this more fully:

> The courts have decided that organizations seeking to achieve political purposes, in whole or in part, cannot be recognized as a registered charity. Political purposes include:
>
> - furthering the aims of a political party;
> - promoting a political doctrine;
> - persuading the public to adopt a particular view on a broad social question; and
> - attempting to bring about or oppose changes in the law or government policy.
>
> Purposes that are so broad as to allow for unlimited political activity, or organizations with unspecified political purposes, will not qualify for charitable registration. In addition, the Act specifically prohibits a registered charity from engaging in any

67 Duff Paper on Charities and Terrorist Financing, pp. 207-212.

68 *Commissioners for Special Purposes of the Income Tax v. Pemsel*, [1891] A.C. 531.

69 Canada Revenue Agency, "Summary Policy," Ref. No. CSP-C01, online: Canada Revenue Agency <http://www.cra-arc.gc.ca/tx/chrts/plcy/csp/csp-c01-eng.html> (accessed March 3, 2009). See Canada Revenue Agency, "Registering a Charity for Income Tax Purposes," T4063(E) Rev. 08, p. 8, online: Canada Revenue Agency <http://www.cra-arc.gc.ca/E/pub/tg/t4063/t4063-08e.pdf> (accessed March 3, 2009) ["Registering a Charity for Income Tax Purposes," T4063(E) Rev. 08] for a description of each category.

> partisan political activity. A partisan political activity is one that involves direct or indirect support of, or opposition to, any political party or candidate for public office.[70]

Although the CRA document sets out this general prohibition on engaging in political activities, it also states that organizations can engage in limited, non-partisan, political activity in some circumstances:

> Under the [Income Tax Act], a registered charity that is established exclusively for charitable purposes can engage, to a limited extent, in **non-partisan political** "**activities**" that directly help accomplish the charity's purposes.
>
> For example, a registered charity with a charitable purpose to provide for the welfare of children can engage in activities that take a public position about certain legislation in the field of child welfare, provided the activities are within [the limits described above]. However, an organization established solely for purposes of pressuring for a change in the legislation affecting the welfare of children cannot be registered as a charity.[71]

To be registered as a charity, an organization must also pass a public benefit test. The organization must show that its "…activities and purposes provide a tangible benefit to the public" and that "…those people who are eligible for benefits are either the public as a whole, or a significant section of it, in that they are not a restricted group or one where members share a private connection, such as social clubs or professional associations with specific membership."[72]

Applicants complete form T2050 to apply as a registered charity.[73] The 14-page form includes questions about the name of the organization and its directors, its structure, financial information and information about its activities. Ms. Walsh stated that, once the form is submitted, "…[e]ach application is subject to a risk-based evaluation which takes into account the potential risk that the organization could be used to support terrorist activities."[74]

With the substantial changes introduced by Bill C-25,[75] the CRA can disclose new classes of information to other agencies. In addition, information that was

---

70 "Registering a Charity for Income Tax Purposes," T4063(E) Rev. 08, p. 5. See also Testimony of Donna Walsh, vol. 57, October 3, 2007, p. 7168; Duff Paper on Charities and Terrorist Financing, pp. 211-212; *Income Tax Act*, R.S.C. 1985, c. 1 (5th Supp.), ss. 149.1(6.1)-(6.2) [*Income Tax Act*].

71 "Registering a Charity for Income Tax Purposes," T4063(E) Rev. 08, p. 5.

72 "Registering a Charity for Income Tax Purposes," T4063(E) Rev. 08, p. 7.

73 A blank form was entered into evidence: see Exhibit P-236, Tab 6: Application to Register a Charity under the *Income Tax Act*.

74 Testimony of Donna Walsh, vol. 57, October 3, 2007, p. 7101.

75 *An Act to amend the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and the Income Tax Act and to make a consequential amendment to another Act*, S.C. 2006, c. 12 [Bill C-25].

already shared for the administration and enforcement of the *CRSIA* can now be used for investigations. Walsh testified that "…the impediments [for sharing information with other agencies] were too high"[76] before these changes:

> [E]ven with the passage of the *CRSIA* there were still significant restrictions upon information sharing between the CRA and other agencies mandated to counter terrorist financing. For one thing, there was still no legislative authority for the CRA to give or receive information from FINTRAC or to FINTRAC. For another, information that the CRA provided to CSIS and the RCMP could not be used in their own investigations. Its use was restricted to the administration and enforcement of the *CRSIA*.[77]

Bill C-25 added a new subsection to section 241 of the *ITA* to accomplish this improved flow of information. Section 241(9) allows the CRA to do the following:

> . . . provide, to an official of the Canadian Security Intelligence Service, of the Royal Canadian Mounted Police or of the Financial Transactions and Reports Analysis Centre of Canada,
>
> (a) publicly accessible charity information;
>
> (b) designated taxpayer information, if there are reasonable grounds to suspect that the information would be relevant to
>
> (i) an investigation by the Canadian Security Intelligence Service of whether the activity of any person may constitute threats to the security of Canada, as defined in section 2 of the *Canadian Security Intelligence Service Act*,
>
> (ii) an investigation of whether an offence may have been committed under
>
> (A) Part II.1 of the *Criminal Code*, or
>
> (B) section 462.31 of the *Criminal Code*, if that investigation is related to an offence under Part II.1 of that *Act*, or
>
> (iii) the prosecution of an offence referred to in subparagraph (ii); and

76 Testimony of Donna Walsh, vol. 57, October 3, 2007, p. 7165.
77 Testimony of Donna Walsh, vol. 57, October 3, 2007, p. 7110.

> (c) information setting out the reasonable grounds referred to in paragraph (b), to the extent that any such grounds rely on information referred to in paragraph (a) or (b).[78]

Only CSIS, the RCMP and FINTRAC can receive publicly accessible charity information and designated taxpayer information.

Designated taxpayer information consists of a wider range of information than publicly accessible charity information.[79] Designated taxpayer information is defined as taxpayer information — other than designated donor information — of a registered charity, or of a person who has at any time made an application for registration as a registered charity, that is:

> (a) in respect of a financial transaction
>
> > (i) relating to the importation or exportation of currency or monetary instruments by the charity or applicant, or
> >
> > (ii) in which the charity or applicant has engaged a person to whom section 5 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* applies,
>
> (b) information provided to the Minister by the Canadian Security Intelligence Service, the Royal Canadian Mounted Police or the Financial Transactions and Reports Analysis Centre of Canada,
>
> (c) the name, address, date of birth and citizenship of any current or former director, trustee or like official, or of any agent, mandatory or employee, of the charity or applicant,
>
> (d) information submitted by the charity or applicant in support of an application for registration as a registered charity that is not publicly accessible charity information,
>
> (e) publicly available, including commercially available databases, or

---

78 The amendment was introduced by s. 45(2) of Bill C-25.

79 The *Income Tax Act* defines "taxpayer information" in s. 241(10). It provides in s. 241(3.2) that "An official may provide to *any person* the following taxpayer information relating to another person *that was at any time a registered charity* (in this subsection referred to as the "charity")." The phrases "publicly accessible charity information" and "designated taxpayer information" are used in s. 241(9). "Publicly accessible charity information" is defined in s. 241(10) as "taxpayer information that is (a) described in subsection (3.2), or that would be described in that subsection if the words 'that was at any time a registered charity' were read as '*that has at any time made an application for registration as a registered charity*', (b) information -- other than designated donor information -- submitted to the Minister with, or required to be contained in, any public information return filed or required to be filed under subsection 149.1(14), or (c) information prepared from information referred to in paragraph (a) or (b)." [Emphasis added.]

> (f) information prepared from publicly accessible charity information and information referred to in paragraphs (a) to (e)....[80]

As a result of the Bill C-25 amendments, the CRA can now provide the basic information – publicly accessible charity information – to CSIS, the RCMP and FINTRAC about an application, and can also provide designated taxpayer information if further conditions set out in section 241(9)(b) are met.

During each of fiscal years 2005-06 and 2006-07, the CRA received approximately 4,000 applications for registration.[81] In 2006-07, registrations for welfare and religious purposes were the most popular, each representing 29 per cent of overall new registrations. Applications for education and benefit to the community purposes stood at 19 and 15 per cent respectively. These proportions appear to have been consistent over the last five years.[82]

The CRA registration process is explained in a document submitted to the Commission as an exhibit, "Managing and Mitigating Risk of Terrorist Involvement."[83] The risk assessment comes into play when the initial screening of an application raises concerns about terrorist involvement. The CRA may then request further information from the applicant through a Request for Information (RFI) . Ms. Walsh testified that the CRA often has a "very highly developed case" already if it is requesting more information.[84]

Professor Duff observed that the Federal Court of Appeal has characterized the registration of charities as a "strictly administrative function," and that the Court has found no obligation on the Minister to notify the applicant and invite representations or conduct a hearing before refusing its application for charitable status.[85] Nonetheless, the CRA currently does allow representations. After assessing an application, CRA will send an Administrative Fairness Letter (AFL) to the applicant explaining the reasons for denying charitable status. The AFL gives the applicant 90 days to respond.[86] The CRA can refuse the application by way of a Final Determination (FD), also described as a Final Turn Down (FTD),[87] or it may decide to register the applicant (REG).

In response to registration applications received in 2006-07, the CRA issued 326 FDs, compared to 52 in 2005-06. CRA attributes this to the implementation of

---

80 *Income Tax Act*, s. 241(10).

81 Exhibit P-236, Tab 10: Assessment, Determinations & Monitoring (ADM) Division, Year End Report 2006/2007, Charities Directorate, Legislative Policy and Regulatory Affairs Branch, p. 4 [ADM 2006/2007 Report].

82 ADM 2006/2007 Report, p. 8.

83 CRA Document on Managing and Mitigating Risk of Terrorist Involvement.

84 Testimony of Donna Walsh, vol. 57, October 3, 2007, p. 7133.

85 Duff Paper on Charities and Terrorist Financing, pp. 212-213.

86 Duff Paper on Charities and Terrorist Financing, p. 212, citing Canada Revenue Agency, *Registered Charities Newsletter*, No. 25 (Fall 2005), p.3, online: Canada Revenue Agency <http://www.cra-arc.gc.ca/E/pub/tg/charitiesnews-25/charitiesnews25-e.pdf> (accessed March 3, 2009).

87 The CRA Document on Managing and Mitigating Risk of Terrorist Involvement uses the acronym "FD"; the ADM 2006/2007 Report uses "FTD."

new procedures.[88] The principal categories of reasons for denials of registration, in 2006-07, were: (i) broad/vague objects, (ii) lack of information and (iii) non-charitable activities.[89] The chart below shows the results of the CRA's "risk mitigation effort" over several years for cases originally evaluated as having some element of risk for support for terrorism:

Fiscal Period	RFI	AFL	FD	REG	Total
April 1, 2007 - Sept 21, 2007	8	12	2	2	24
April 1, 2006 - March 31, 2007	12	12	6	3	33
April 1, 2005 - March 31, 2006	4	13	1	2	20
April 1, 2004 - March 31, 2005	4	5	0	7	16
April 1, 2003 - March 31, 2004	10	6	0	3	19
April 1, 2002 - March 31, 2003	17	15	5	1	38
April 1, 2001 - March 31, 2002	7	7	0	2	16
Total	62	70	14	20	

Exhibit P-236, Tab 9

Ms. Walsh testified that some registration applications had been denied in part because of terrorist involvement, including TF.[90] However, she could not identify the exact number of organizations denied charitable status for this reason, since a given organization might make several applications. In addition, CRA may have several reasons (including those not related to terrorism) to deny registration. In some cases it may be impossible for CRA to attribute a denial of registration solely to terrorism or TF factors, although statistics on when concerns about TF were one of the grounds for denying charitable status would obviously be valuable.[91] The above chart shows that from 2001 until the time of the Commission's hearings on this subject, the CRA denied registration in 14 cases that had some terrorism connection.[92] In addition, the RCMP reported that in 2005-06, three organizations were denied charitable registration because they had links to terrorist activities or groups.[93]

---

88 ADM 2006/2007 Report, p. 5.
89 ADM 2006/2007 Report, p. 9.
90 Testimony of Donna Walsh, vol. 57, October 3, 2007, pp. 7171-7172.
91 Testimony of Donna Walsh, vol. 57, October 3, 2007, pp. 7170-7171; ADM 2006/2007 Report, p. 9.
92 CRA Document on Managing and Mitigating Risk of Terrorist Involvement, p. 2; Testimony of Donna Walsh, vol. 57, October 3, 2007, pp. 7172-7173.
93 RCMP 2005-06 Departmental Performance Report, p. 62.

Ms. Walsh stated that CRA "probably" examines the background of directors and trustees listed on an application for charitable status to determine whether the organization is going to be operated wholly for charitable purposes and activities: " information of any sort that is relevant to making that determination is information that we could look at."[94] Furthermore, the names of directors and trustees can now be shared with CSIS and the RCMP.[95]

For confidentiality reasons, no specific examples of registration applications were provided to the Commission, but the CRA did offer several "sanitized" real examples to illustrate the work done in assessing applications:

> [Example 1] A Canada-based organization applied for registered charitable status. Research revealed that the organization provided propaganda and financial support to promote the ideology and the agenda of a proscribed terrorist organization abroad that was seeking to undermine the stability of another country. The applicant's political activities in Canada and its support for a terrorist entity overseas disqualified it from obtaining Canadian registration as a charity. The application was denied.[96]
>
> [Example 2] An organization's application to CRA for registered charitable status did not provide sufficient information to allow the federal government to understand how it intended to conduct or protect its activities in an active combat zone overseas. The onus is on the applicant to substantiate that its purposes and activities are charitable in the legal sense. In addition, the organization proposed to conduct its work in areas under the control of groups listed by Canada and the United Nations as terrorist entities. The documents provided by the organization indicated that it intended to work with these groups. The application was denied.[97]
>
> [Example 3] This application for registration was seen to be problematic because of the wide span of the applicant organization's objects, which would not restrict it to pursuing exclusively charitable goals. Of major concern was that the organization was not responsible for running the programs that it supported. Instead, the organization's financial and material resources were provided to non-qualified recipients who operated in conflict zones controlled by groups listed by Canada as terrorist entities. The information provided by the applicant organization indicated that it did not have adequate mechanisms in place to prevent its resources from being made

94 Testimony of Donna Walsh, vol. 57, October 3, 2007, p. 7169.
95 See para. (c) of the definition of "designated taxpayer information" in the *Income Tax Act*, s. 241(10).
96 Exhibit P-236, Tab 8: "CRA Case Summaries," Case 5 [CRA Case Studies].
97 CRA Case Summaries, Case 8.

> available to those terrorist entities. In addition, the applicant operated under the auspices of another organization whose objects and activities were political in nature and were aimed at providing benefits to a specific segment of the community.[98]

These examples show that denials of registration occur because of various deficiencies, possibly including TF.

Professor Duff suggested that a more demanding regulatory regime in recent years may have reduced the number of organizations that would otherwise have obtained registered status. He described a sizeable decrease in the number of applications approved for registered charity status – from 90 per cent of applications in 1995-96 to about 65 per cent in 1996-97 – after the revocation of the charitable status of Babbar Khalsa in 1996.[99] He also described the decrease in applications for charitable status between 1999 and 2002 following the attacks of September 11, 2001, and the enactment of the *CRSIA* later that year. He concluded:

> Although the explanation for these shifts is not clear, they suggest that the CRA may have become more rigorous in its assessment of applications for registered status after the Babbar Khalsa Society's charitable status was revoked, which – together with the subsequent enactment of the *CRSIA* – may have led to fewer applications for registered status. If so, a more demanding regulatory regime may have reduced the number of organizations that would otherwise have obtained charitable status.[100]

Duff suggested that current provisions for the exchange of information would have made it doubtful that the Babbar Khalsa could register as a charity today.[101] The CRA can be more thorough in reviewing registration applications, given its increased investigative powers and the resulting decrease in registrations.

6.5.2.3 The Monitoring and Audit Processes

The CRA's powers include the power to inspect, audit and examine the books, records and property of a taxpayer (including a registered charity), as well as the power to enter premises and to be given reasonable assistance in such cases.[102]

Once a charity is registered with CRA, it is subject to regular monitoring. Monitoring is part of the ongoing audit process, which occurs on both a random

---

98 CRA Case Summaries, Case 12.
99 Duff Paper on Charities and Terrorist Financing, pp. 213-214.
100 Duff Paper on Charities and Terrorist Financing, p. 214.
101 Duff Paper on Charities and Terrorist Financing, p. 238.
102 *Income Tax Act*, s. 231.1(1); Duff Paper on Charities and Terrorist Financing, pp. 227-229.

and a targeted basis.[103] This audit process is separate from the audit program for regular taxpayers.[104] The charities audit process is risk-based, and the risk indicators are constantly evolving.[105] Terry de March, Acting Director General of the Charities Directorate, testified that "…at different times the money leaving the country for foreign activities has been a focus of our audit program."[106]

An audit can occur even before registration.[107] CRA conducts field audits of about 800 registered charities each year – about one per cent of all registered charities.[108]

Registered charities are subject to multiple requirements to maintain their charitable status. These include the following:

- filing an annual information return and a public information return within six months of the end of their taxation year;[109]
- maintaining books and records in Canada;[110] and
- not becoming involved in commercial activities.[111]

A registered charity must file an annual Registered Charity Information Return (form T3010). This form requires information such as a summary of the year's activities, changes to governing documents, directors' names and personal information, information on international activities, information about sources and uses of funds, financial statements and the charity's web site address.[112]

There is no automatic mechanism or process for CRA to be advised of changes in the annual return information between annual filings. The only tools at CRA's disposal to deal with such changes are the audit process (but only about one per cent of charities are audited every year), information supplied to CRA by other agencies and publicly available information.

A survey of the information collected in 2005 from these forms appears in the CRA document "Assessment, Determinations & Monitoring (ADM) Division."[113] It shows that 13,326 charities reported charitable activities outside Canada (17 per cent of all charities) and that 44,108 charities reported annual revenue of $100,000 or less (56 per cent of all charities). The document surveyed the top reporting "flags" – cases where charities had not provided all the requested

---

103 Testimony of Terry de March, vol. 57, October 3, 2007, p. 7125.
104 Testimony of Terry de March, vol. 57, October 3, 2007, pp. 7125-7126.
105 Testimony of Terry de March, vol. 57, October 3, 2007, p. 7126.
106 Testimony of Terry de March, vol. 57, October 3, 2007, p. 7125.
107 Testimony of Terry de March, vol. 57, October 3, 2007, p. 7126.
108 2008 FATF Mutual Evaluation of Canada, para. 1425.
109 *Income Tax Act*, s. 149.1(14).
110 *Income Tax Act*, s. 230(2); CRA Presentation on Canada's Charities and Anti-terrorism Measures, slide 4.
111 The prohibition is on an unrelated business: *Income Tax Act*, s. 149.1(2)(a); Duff Paper on Charities and Terrorist Financing, p. 215, note 73.
112 CRA Presentation on Canada's Charities and Anti-terrorism Measures, slide 6.
113 ADM 2006/2007 Report, pp. 10-13.

information – and found 28,640 charities (36 per cent)[114] did not provide a Basic Information Sheet as part of their annual return.

6.5.2.4 Intermediate Sanctions

Before 2005, the only option available to the CRA in the case of a non-compliant charity was to revoke the charity's registration. Since then, several intermediate measures have been introduced to provide greater flexibility in enforcement.[115] These include monetary penalties and the suspension of a charity's power to issue tax receipts for donations. The penalties can be appealed.[116]

Professor Duff testified that intermediate measures let a charity know that it has to "shape up," and let the public know that a charity is having difficulty complying with its legal obligations.[117] Such measures might also help those who seek to regain control of charities which are experiencing governance problems[118]:

> To the extent that existing and potential supporters are given notice of the charity's failings through [suspension of power to issue tax-receipts], they may be in a position to persuade the charity to take remedial measures including the removal and replacement of directors or trustees, which the federal government could not accomplish directly given the constitutional limits of its jurisdictional authority.[119]

The CRA does not have a power like that of the Charity Commission of England and Wales to suspend or remove trustees and take measures to protect charities in difficulty. In his paper prepared for the Commission, Professor Mark Sidel detailed how this power was used in the UK to remove Abu Hamza from the Finsbury Park Mosque in London even before he was convicted of inciting murder and hatred in the United Kingdom and indicted on terrorism support charges in the United States.[120] In Canada, direct interventions to remove directors or trustees would fall under provincial jurisdiction. However, the creative use of intermediate sanctions by the CRA could indirectly produce some of the same results. For example, it might be possible to suspend an organization's charitable status temporarily. This would alert trustees, directors and donors to problems in the organization. They might themselves then take remedial actions that are not open to federal authorities because of a lack of federal jurisdiction.

---

114 ADM 2006/2007 Report, p. 11.
115 Testimony of David Duff, vol. 85, November 29, 2007, p. 10896. See pp. 238-239 of Duff Paper on Charities and Terrorist Financing for more on intermediate penalties.
116 See Duff Paper on Charities and Terrorist Financing, pp. 219-221.
117 Testimony of David Duff, vol. 85, November 29, 2007, p. 10896.
118 Testimony of David Duff, vol. 85, November 29, 2007, p. 10903.
119 Duff Paper on Charities and Terrorist Financing, p. 220.
120 Sidel Paper on Terrorist Financing and the Charitable Sector, p. 166.

Since these intermediate sanctions have been allowed only since 2005, empirical evidence about their value is scarce. However, as Professor Duff argues, it must surely be a factor in the decrease in the number of revocations since 2005.

6.5.2.5 Revocation of Charitable Status

A charity has 90 days to file an objection after the CRA issues a revocation notice, and appeals may also be involved.[121] Even after revoking a charity's registration, the CRA continues to collect information about the charity.[122]

Year	Revocations by Request	Revocations for Failure to File Information Return	Revocations for Cause	Total Revocations
2002	800	1,599	5	2,404
2003	788	1,127	6	1,921
2004	709	1,261	8	1,978
2005	438	963	11	1,412

The above chart[123] shows that most revocations are due to a request by a charity or failure to file an information return. There have been very few revocations for cause – ranging from 5 to 11 annually – between 2002 and 2005. Professor Duff testified that the small number might mean either that the charitable sector is healthy or that improper activities are not being caught, but that it was impossible to know which reason applied.[124]

The 2008 FATF Mutual Evaluation of Canada described several types of conduct that have caused registrations to be revoked:

> Recent experience suggests that, on average, about 10 charities a year lose their registrations as a result of serious non-compliance issues, including dubious fund-raising schemes, political activities, lack of proper books and records, and improper personal benefit. In addition, registered charities that have failed to demonstrate sufficient control over their foreign operations have been de-registered.[125]

In the end, it is difficult to determine from justifications for revoking registrations if the revocations occurred partly or wholly because of links with terrorism or TF.

6.5.2.6 The Charities Registration (Security Information) Act (CRSIA) Process

Following 9/11, the role of the Charities Directorate changed substantially. This was, in large part, a result of the enactment of the *Charities Registration (Security*

---

121 See p. 217 of Duff Paper on Charities and Terrorist Financing for further details.
122 Testimony of Donna Walsh, vol. 57, October 3, 2007, p. 7103.
123 Duff Paper on Charities and Terrorist Financing, p. 218.
124 Testimony of David Duff, vol. 85, November 29, 2007, p. 10901.
125 2008 FATF Mutual Evaluation of Canada, para. 1425.

Information) Act (*CRSIA*). The Department of Justice summarizes the purpose of *CRSIA* as follows:

> *CRSIA* makes possible the use of classified information in determining whether organizations can register as charities under the *Income Tax Act* or whether, previously having been registered, they can retain this status. Before the passage of *CRSIA*, all decisions on charitable registration were subject to appeal in an open court, and thus only information that could be disclosed publicly could be used in reaching these decisions.[126]

A CRA document similarly spoke of the importance of being able to rely on classified information in making the case for denying or revoking registration:

> Regular rules and procedures under the *Income Tax Act* are used to deny or revoke registration where publicly available information combined with information an organization is required to provide to the CRA is sufficient to make the case that an organization is not exclusively dedicated to charitable purposes. But the option to undertake the certificate process authorized by the [*CRSIA*] also is an important tool for cases where it is necessary to rely on classified information to substantiate an organization's ties to terrorism.[127]

The Government of Canada described the *CRSIA* as an administrative process which includes an administrative measure with an administrative remedy.[128]

Section 2(1) of the *CRSIA* explains the Act's formal purpose:

> 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

126 Department of Justice, Fact Sheet, "Outline of the *Charities Registration (Security Information) Act*," online: Department of Justice <http://www.justice.gc.ca/eng/antiter/sheet-fiche/CRSIA-LEOBRS.HTML> (accessed April 17, 2009).

127 CRA Document on Managing and Mitigating Risk of Terrorist Involvement, p. 1.

128 *Response of the Government of Canada to the Final Report of the Standing Committee on Public Safety and National Security, Subcommittee on the Review of the Anti-terrorism Act, Rights, Limits, Security: A Comprehensive Review of the Anti-terrorism Act and Related Issues*, p. 14, online: Parliament of Canada <http://cmte.parl.gc.ca/Content/HOC/committee/391/secu/govresponse/rp3066235/391_SECU_Rpt07_GR/391_SECU_Rpt07_GR-e.pdf> (accessed May 25, 2009) [Canada Response to House of Commons Report on the *ATA*].

> are made available only to organizations that operate exclusively for charitable purposes.[129]

Section 2(2) requires the Act to be carried out "in recognition of, and in accordance with," the following principles:

> (a) maintaining the confidence of taxpayers may require reliance on information that, if disclosed, would injure national security or endanger the safety of persons; and
>
> (b) the process for relying on the information referred to in paragraph (a) in determining eligibility to become or remain a registered charity must be as fair and transparent as possible having regard to national security and the safety of persons.

Professor Duff testified that the spirit of the *CRSIA* predated 9/11 since its provisions existed in draft form before then. After 9/11, the draft provisions were integrated with the bill that became the *ATA*.[130] Ms. Walsh stated that the enactment of the *CRSIA* was important "…because it created the foundation for an intelligence-assisted compliance effort that we did not have previously."[131]

The *CRSIA* permits the Minister of Public Safety and the Minister of National Revenue to issue a certificate stating that it is their opinion, based on information, that there are reasonable grounds to believe[132]:

> that an applicant or registered charity has made, makes or will make available any resources, directly or indirectly, to an entity that is a listed entity as defined in subsection 83.01(1) of the *Criminal Code*;
>
> that an applicant or registered charity made available any resources, directly or indirectly, to an entity as defined in subsection 83.01(1) of the *Criminal Code* and the entity was at that time, and continues to be, engaged in terrorist activities as defined in that subsection or activities in support of them; or
>
> that an applicant or registered charity makes or will make available any resources, directly or indirectly, to an entity as defined in subsection 83.01(1) of the *Criminal Code* and the entity engages or will engage in terrorist activities as defined in that subsection or activities in support of them.[133]

---

129 See also Testimony of Donna Walsh, vol. 57, October 3, 2007, p. 7106; CRA Presentation on Canada's Charities and Anti-terrorism Measures, slide 11.

130 Testimony of David Duff, vol. 85, November 29, 2007, p. 10897.

131 Testimony of Donna Walsh, vol. 57, October 3, 2007, p. 7109.

132 The *Charities Registration (Security Information) Act*, S.C. 2001, c. 41, s. 113 [*CRSIA*] uses the "reasonable grounds to believe" standard rather than the criminal law standard of proof. See Testimony of Donna Walsh, vol. 57, October 3, 2007, p. 7110.

133 *CRSIA*, s. 4(1).

Both ministers assess the available intelligence before signing a certificate. To facilitate this, the RCMP and CSIS analyze relevant information and provide their recommendation to the Minister of Public Safety. The CRA performs a similar assessment and provides advice to the Minister of Revenue.

The following chart summarizes the CRSIA certificate process:[134]

IDENTIFICATION OF CASE

- CSIS or the RCMP, with CRA identify, and initially assess the case for a security certificate

CONSULTATION

- CSIS/RCMP and CRA to consult and share information to the extent possible related to potential certificate.

DECISION TO PROCEED

- CSIS/RCMP and CRA determine whether to pursue action under *CRSIA*
- Security Intelligence Report (SIR) prepared by CSIS or RCMP

INTERNAL APPROVAL

- SIR verified by RCMP or CSIS legal counsel
- SIR approved by the Director of CSIS/Commissioner of the RCMP
- Following sign off, SIR delivered to Deputy Minister (DM) of Public Safety and the Commissioner of the Canada Revenue Agency

NOTIFICATION OF INTERDEPARTMENTAL COMMUNITY

- DM of Public Safety convenes DM-level meeting of relevant departments.
- Submission is reviewed and recommendation to Ministers confirmed

ADVISING THE MINISTER OF PUBLIC SAFETY

- Unsigned security certificate and SIR forwarded to the Minister of Public Safety.
- If the Minister of Public Safety signs the certificate, it is provided to the Minister of National Revenue for signature

SUBSEQUENT PROCESS

- Public Safety Canada provides implicated organization with a copy of the certificate once both Ministers have signed
- The certificate is filed in the Federal Court not earlier than seven days later
- If upheld by the court, the certificate is published in the *Canada Gazette*

134 Exhibit P-383, Tab 11: Public Safety Canada's Submission to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, October 24, 2007, p. 3.

If the certificate is issued, it is then sent to the charity or applicant for charitable status with a notice that the certificate will be referred to the Federal Court.

A Federal Court judge may receive into evidence anything that, in the judge's opinion, is reliable and appropriate, even if it is probably inadmissible as evidence in a court of law, and may base the decision on that information.[135] The judge must hear all or part of the information or evidence in the absence of the applicant or registered charity named in the certificate and their counsel if, in the judge's opinion, its disclosure would be injurious to national security or endanger the safety of any person.[136] The judge must then provide a summary of that evidence to the applicant or registered charity to enable it to be reasonably informed of the circumstances giving rise to the certificate. This summary must not include anything that the judge concludes would be injurious to national security or endanger a person if disclosed.[137] The judge must also give an opportunity for the applicant or registered charity to be heard.[138] After completing this process, the judge must determine whether the certificate is reasonable, and must quash it if of the opinion that it is unreasonable.[139]

A determination by the judge that the certificate of review is reasonable is conclusive proof that the applicant is ineligible to become a registered charity or, in the case of a registered charity, that it does not comply with the requirements to continue to be a registered charity.[140] The judge's determination is final and is not subject to appeal or judicial review.[141] That determination can be reviewed only through an application to the Minister of Public Safety on the basis of a "material change in circumstances" since the determination was made.[142] Unless cancelled sooner, the certificate is valid for seven years.[143]

No certificate had been issued under the *CRSIA* as of January 2009.[144] This may be in part because support for terrorist activities would also violate *ITA* requirements for charitable status. It is likely simpler for the CRA to revoke or deny charitable status because of a failure to satisfy the *ITA* than it is to undertake the *CRSIA* certificate process to achieve the same result. The CRA continues to operate on

---

135 *CRSIA*, s. 6(j).
136 *CRSIA*, s. 6(e).
137 *CRSIA*, s. 6(h).
138 *CRSIA*, s. 6(i).
139 *CRSIA*, s. 7.
140 *CRSIA*, s. 8(1).
141 *CRSIA*, s. 8(2).
142 *CRSIA*, s. 10(1).
143 *CRSIA*, s. 13.
144 House of Commons Canada, Final Report of the Standing Committee on Public Safety and National Security, Subcommittee on the Review of the *Anti-terrorism Act, Rights, Limits, Security: A Comprehensive Review of the Anti-terrorism Act and Related Issues*, March 2007, p. 34, online: Parliament of Canada <http://www2.parl.gc.ca/content/hoc/Committee/391/SECU/Reports/RP2798914/sterrp07/sterrp07-e.pdf> (accessed March 3, 2009) [House of Commons Report on the *ATA*]; The Senate of Canada, Special Senate Committee on the *Anti-terrorism Act, Fundamental Justice in Extraordinary Times: Main Report of the Special Senate Committee on the Anti-terrorism Act*, February 2007, p. 60, online: Parliament of Canada <http://www.parl.gc.ca/39/1/parlbus/commbus/senate/Com-e/anti-e/rep-e/rep02feb07-e.pdf> (accessed March 3, 2009) [Senate Report on the ATA].

the premise that it is preferable to deal with TF issues under the *ITA* because the process under the *ITA* is more transparent.[145]

If a registered charity or an organization applying for registration is included in either of the UN terrorist entity lists or in the *Criminal Code* list, the CRA evaluates the organization and takes action under either the *CRSIA* or the *ITA*.[146]

In his paper, Professor Duff suggested that the onus of proof under the *ITA* may make it a more attractive vehicle than the *CRSIA* in revoking charitable status:

> [S]ince the onus of proof under an ordinary revocation proceeding falls on the charity to disprove the assumptions of fact on which the decision to revoke is based, it may be easier to revoke registered status on this basis than under the *CRSIA*, notwithstanding the "reasonable belief" standard on which revocation under the *CRSIA* may be based.[147]

Although no certificate has yet been issued under the *CRSIA*, Ms. Walsh, Director of the Review and Analysis Division in the Charities Directorate of the Canada Revenue Agency (CRA), stated that the certificate process constitutes a prudent reserve power.

The Commission heard concerns that the *CRSIA* might deter legitimate charities from doing good works abroad. In his paper, Terrance Carter, a lawyer specializing in charities law, argued that "the immediate practical concern for charities is not that they will be prosecuted … but that they may be vulnerable to de-registration under [*CRSIA*]."[148] As well, he described several possible deficiencies in the *CRSIA* procedure for obtaining a certificate denying or revoking charitable registration.[149] Professor Duff also suggested that there were several deficiencies in the *CRSIA*:

- The grounds on which charitable status may be denied or revoked are extremely broad;
- There is no due diligence defence or, in the alternative, a requirement of intent;
- The level of secrecy surrounding the proceedings is very high, such that it may create insurmountable hurdles for a registered charity or applicant that wants to mount an adequate defence; and

---

145 Testimony of Donna Walsh, vol. 57, October 3, 2007, p. 7157.

146 Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (Ottawa: Public Works and Government Services Canada, 2006), p. 190.

147 Duff Paper on Charities and Terrorist Financing, p. 227.

148 Terrance S. Carter, "The Impact of Anti-terrorism Legislation on Charities in Canada: The Need For an Appropriate Balance," October 26, 2007, p. 18, online: Carters Professional Corporation <http://www.carters.ca/pub/article/charity/2007/tsc1026.pdf> (accessed May 12, 2009) [Carter Paper on Impact of Anti-terrorism Legislation on Charities in Canada].

149 Carter Paper on Impact of Anti-terrorism Legislation on Charities in Canada, pp. 38-39.

- There is a lack of provision for intermediate penalties (as an alternative to the outright revocation of status or denial of an application) in *CRSIA* certificate proceedings.[150]

In March 2007, the House of Commons Standing Committee on Public Safety and National Security[151] made several recommendations relating to the *CRSIA*, among them that:

- [27] the *CRSIA* be amended so that a Federal Court judge to whom a certificate is referred shall not find the certificate to be reasonable where an applicant or registered charity has established that it has exercised due diligence to avoid the improper use of its resources under section 4(1);[152]
- [28] in consultation with the charitable sector, the Canada Revenue Agency develop and put into effect best practice guidelines to provide assistance to applicants for charitable status and registered charities in their due diligence assessment of donees;[153]
- [29] section 8(2) of the *CRSIA* be amended to allow for an appeal to the Federal Court of Appeal of a decision by a Federal Court judge that a referred certificate is reasonable;[154] and
- [33] subsections 5(3) and (4) of the *CRSIA* be repealed and the Act be amended so that, beginning from the time that an applicant or registered charity is being investigated for allegedly making resources available to a terrorist entity, its identity cannot be published or broadcast, and all documents filed with the Federal Court in connection with the reference of the certificate must be treated as confidential, unless and until the certificate is found to be reasonable and published under section 8.[155]

The Government of Canada responded to the aspects of the House of Commons report dealing with charities as follows:[156]

- [27-28] The Government wished to maintain the *status quo* in the system under the *ITA* and *CRSIA* for the registration of charities and the revocation of registration because doing otherwise would mean that organizations with links

150 Duff Paper on Charities and Terrorist Financing, pp. 240-241.
151 Subcommittee on the Review of the *Anti-terrorism Act*.
152 House of Commons Report on the *ATA*, p. 36.
153 House of Commons Report on the *ATA*, p. 36.
154 House of Commons Report on the *ATA*, p. 37.
155 House of Commons Report on the *ATA*, p. 40.
156 Canada Response to House of Commons Report on the *ATA*, pp. 14-15. The numbers in square brackets refer to the recommendations in the House of Commons Report on the *ATA*.

to terrorism could possibly learn about Canadian counter-terrorism measures and structure their affairs to create a defence against *CRSIA* measures. The changes to the law proposed by the Commons report would also weaken Canada's conformity with its international obligations;[157]

- [29] In considering the possible value of judicial appeals under the *CRSIA*, further study was necessary to assess the implications of the judicial consideration of provisions governing access to appeals under the *Immigration and Refugee Protection Act* security certificate scheme;[158] and
- [33] Adding to the *CRSIA* a provision prohibiting the publication of information in relation to a charity that was under investigation, and a general confidentiality ban on documents filed in Federal Court, would depart from the principle of openness in court proceedings and would run a serious risk of contravening the *Charter*.[159]

In February 2007, the Special Senate Committee on the *Anti-terrorism Act* published its report, *Fundamental Justice in Extraordinary Times: Main Report of the Special Senate Committee on the Anti-terrorism Act*.[160] The report contained a general recommendation about the need for a special advocate in charitable status cases.[161]

The Commons and Senate reports both addressed the due diligence and *mens rea* issues, but came to different conclusions. The Commons report recommended adding a due diligence defence to the certificate proceedings triggered by section 4(1) of the *CRSIA*.[162] The Senate report concluded that adding a due diligence defence to the *CRSIA* "…could have the unintended effect of making

---

157 Canada Response to House of Commons Report on the *ATA*, p. 14. Furthermore, the government stated that "…[t]o require in the *CRSIA* that an organization 'knew or ought to have known' could, in some circumstances, effectively result in the Government of Canada providing a tax subsidy for resources tied to terrorism."

158 Canada Response to House of Commons Report on the *ATA*, p. 15.

159 Canada Response to House of Commons Report on the *ATA*, p. 15.

160 Senate Report on the *ATA*.

161 Senate Report on the *ATA*, p. 60: "The Committee is also satisfied that the appointment of a special advocate, by specifically addressing problems inherent in the judicial review process, would help to address witness anxiety about the 'chill' effect of the *CRSIA* on charitable giving or work. The special advocate would test the evidence raised against charitable organizations in security and intelligence reports, and better enable them to respond to allegations that they have made, made or will make resources available to terrorist groups or in support of terrorist activities. The availability of a special advocate during judicial review would therefore restore balance to the processes under the *CRSIA*, helping to ensure that charities are treated fairly."

162 See Recommendation 27 in House of Commons Report on the *ATA*, p. 36.

charities more vulnerable to being used as front organizations for terrorists."[163] Carter also called for a due diligence defence and for a *mens rea* element in *CRSIA* certificate proceedings.[164] Duff argued that the current broad provisions for denial or revocation of registration under the *CRSIA*, along with the absence of a due diligence defence or requirement of intent, might create uncertainty that could deter well-meaning charities from pursuing activities abroad, especially in conflict zones.[165] Duff recommended that a *mens rea* requirement of "intent" be included in section 4(1) of the *CRSIA*[166] for the certificate proceedings permitted by the Act to come into play. He also recommended a due diligence defence. The due diligence defence could be explained in a "made-in-Canada" best practices paper that would guide charities.[167]

6.5.2.7 Collection and Use of Information from Various Sources

The *PCMLTFA* requires FINTRAC to disclose "designated information" to the CRA in some situations. If FINTRAC has reasonable grounds to suspect that designated information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence, it must disclose information to the CRA:

> if [FINTRAC] also determines that the information is relevant to an offence of obtaining or attempting to obtain a rebate, refund or credit to which a person or entity is not entitled, or of evading or attempting to evade paying [certain taxes or duties];[168] or
>
> if [FINTRAC] also has reasonable grounds to suspect that the information is relevant to determining (i) whether a registered charity…has ceased to comply with the requirements of [the *ITA*] for its registration as such, or (ii) whether a person or

---

163 Senate Report on the *ATA*, p. 60. The report also stated: "The Committee is also satisfied that the appointment of a special advocate, by specifically addressing problems inherent in the judicial review process, would help to address witness anxiety about the 'chill' effect of the *CRSIA* on charitable giving or work. The special advocate would test the evidence raised against charitable organizations in security and intelligence reports, and better enable them to respond to allegations that they have made, made or will make resources available to terrorist groups or in support of terrorist activities. The availability of a special advocate during judicial review would therefore restore balance to the processes under the *CRSIA*, helping to ensure that charities are treated fairly. Having said this, however, the Committee urges the government to use its powers to deny or revoke charitable status under the *CRSIA* with caution, in order to ensure that charities are not penalized for legitimate aid activities that might occasionally tangentially benefit terrorist organizations or groups": pp. 60-61.

164 Carter Paper on Impact of Anti-terrorism Legislation on Charities in Canada, p. 55.

165 Duff Paper on Charities and Terrorist Financing, p. 241.

166 This is the provision allowing the Minister of Public Safety and Minister of National Revenue to sign a certificate stating that it is their opinion that there are reasonable grounds to believe that an applicant or charity has made, is making or will make resources available to a listed entity as defined in s. 83.01(1) of the *Criminal Code*.

167 Duff Paper on Charities and Terrorist Financing, p. 241.

168 *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, s. 55(3)(b) [*PCMLTFA*].

> entity that [FINTRAC] has reasonable grounds to suspect has applied to be a registered charity…is eligible to be registered as such.[169]

CRA may use this information from FINTRAC to start a new enforcement action or support an ongoing action.[170]

As well, the *PCMLTFA* allows the CRA to apply for a judge's order requiring FINTRAC to provide additional information about an investigation of an offence that was the subject of a FINTRAC disclosure made under section 55(3)(b) (which deals with improper refunds or evading taxes).[171]

The CRA receives intelligence reports from, and has liaison arrangements with, both the RCMP and CSIS.[172] The Charities Directorate also has its own pool of information. In particular, the CRA has considerable investigative powers under the *ITA*.[173] As well, the CRA actively monitors the media and the Internet and it reviews case law, academic papers and texts.[174] Two staff members are dedicated to the collection of information.[175] As well, "…[r]esources are … devoted to the collection and analysis of program-derived and publicly available information specifically relating to the use of social, community, religious, and humanitarian organizations to provide cover and legitimacy for international terrorism."[176]

6.5.2.8 Information Sharing Between CRA and Other Agencies

As noted earlier, Bill C-25 amended the *ITA* to allow the CRA to disclose information to CSIS, the RCMP and FINTRAC.[177]

The CRA has the discretion to decide whether or not to share information with the RCMP or CSIS. Ms. Walsh testified that the CRA usually discloses information to both agencies.[178] However, there was no set procedure for those agencies to report back to CRA on whether the information had led to a successful prosecution. Ms. Walsh said that this information would be useful and that CRA was seeking such information from other agencies as part of CRA's performance evaluation framework.[179]

The system is now focused on a more extensive sharing of information about registered charities. Still, as Ms. Walsh testified, the new information-sharing

---

169 *PCMLTFA*, s. 55(3)(c).
170 Exhibit P-227, Tab 3: Department of Finance Memorandum of Evidence on Terrorist Financing, February 28, 2007, p. 37 [Department of Finance Memorandum of Evidence on Terrorist Financing].
171 *PCMLTFA*, s. 60.3.
172 CRA Document on Managing and Mitigating Risk of Terrorist Involvement, p. 1.
173 Testimony of David Duff, vol. 85, November 29, 2007, p. 10898.
174 Testimony of Donna Walsh, vol. 57, October 3, 2007, pp. 7127-7129.
175 Testimony of Donna Walsh, vol. 57, October 3, 2007, p. 7128.
176 CRA Document on Managing and Mitigating Risk of Terrorist Involvement, p. 1.
177 Department of Finance Memorandum of Evidence on Terrorist Financing, p. 38.
178 Testimony of Donna Walsh, vol. 57, October 3, 2007, p. 7116.
179 Testimony of Donna Walsh, vol. 57, October 3, 2007, pp. 7120-7121.

powers were so recent that CRA officials did not yet know how well they were working and what shortcomings might appear.[180]

6.5.2.9 Oversight and Review

The CRA's work is subject to several forms of oversight – by the Auditor General, the Treasury Board, the Office of the Privacy Commissioner of Canada (under the *Privacy Act*[181]), the Office of the Information Commissioner of Canada (under the *Access to Information Act*[182]) and the courts. The CRA's annual public report[183] also contains an evaluation of the work of the CRA. As well, CRA activities are examined during parliamentary reviews of the *ATA*, which can touch on the *CRSIA*, and during the FATF mutual evaluation process.

Still, there is no equivalent for the CRA to the review performed by the Security Intelligence Review Committee (SIRC) of CSIS activities. CRA's stringent protection of taxpayer information could make such a review difficult. Unless the law were changed, only taxpayer information such as defined in section 241(3.2) of the *ITA* (information relating to registered charities) would be available for review. Such restrictions applied when the CRA was reviewed by the FATF in 2007-2008, as well as during parliamentary and other reviews of the anti-TF program.

Commissioner O'Connor did not recommend oversight of the CRA in his report of the Arar Inquiry.[184] Commissioner O'Connor focused on the review of the propriety of conduct, including the effect that actions could have on privacy values.

6.6 Not-for-profit Organizations (NPOs)

There may be confusion among members of the public about the distinction between registered charities and not-for-profit organizations (NPOs).[185] Terrance Carter, a lawyer specializing in charities law, testified that even "…the FATF and the international best practice refers to both as well, both non-profit organizations and charities are all in the same document."[186]

NPOs are defined in the *ITA*. In essence, they are clubs, societies and similar organizations:

> (i) that can be created for any purpose except profit;

---

180 Testimony of Donna Walsh, vol. 57, October 3, 2007, p. 7165.
181 R.S.C. 1985, c. P-21.
182 R.S.C. 1985, c. A-1.
183 Final Submissions of the Attorney General of Canada, Vol. III, February 29, 2008, para. 173; Testimony of Maurice Klein, vol. 57, October 3, 2007, p. 7155.
184 Testimony of Maurice Klein, vol. 57, October 3, 2007, pp. 7155-7156.
185 Testimony of Donna Walsh, vol. 57, October 3, 2007, pp. 7174-7175.
186 Testimony of Terrance Carter, vol. 67, October 26, 2007, p. 8375.

> (ii) with no distribution of any profits to members or shareholders (that means that all profits, if any, are kept within the organization for its purposes); and
>
> (iii) which are not charities in the opinion of the minister.[187]

Like registered charities, NPOs pay no income tax.[188] Unlike charities, NPOs cannot issue tax receipts for donations. Most NPOs are registered with a provincial corporate or other registry.

Terry de March, Acting Director General of the Charities Directorate, told the Commission that there are about 80,000 NPOs in Canada and 83,000 registered charities.[189]

A not-for-profit organization that does not seek to become a registered charity can nonetheless qualify for tax-exempt status with the CRA as an NPO. An NPO's lack of authority to issue a tax receipt may not deter donors who are committed to the NPO's cause. In his paper, Blake Bromley gave the following example, based on his experience with Sikh charities, of a situation where charitable tax receipts are not important to donors:

> Sikhs generally give anonymously by placing their offerings in a large locked box so that no one knows how much is given and by whom. Tax receipts are not generally issued, because many worshippers are recent immigrants who are not used to receiving tax benefits for religious donations. However, if a gurdwara receives most of its donations from donors who are not claiming tax benefits, then the gurdwara suffers no disadvantage from being an NPO rather than a charitable organization. In fact, given the problems that gurdwaras face in obtaining charitable status if they carry on cultural and language programs, we advise some of these organizations that it would be a waste of money to apply for registered charity status.[190]

Many organizations that may be prepared to support TF may not see issuing tax receipts as a priority. Creating a "legitimate" vehicle to raise funds and move them abroad is the main objective. Incorporation provides legitimacy to terrorist organizations that need a respectable public face.[191] Furthermore, an NPO can call itself a charity, even if it is not a registered charity. Professor Duff testified that an NPO "…can certainly obtain funds and present [itself] and gain

---

187 *Income Tax Act*, s. 149.1(1). See also Testimony of Donna Walsh, vol. 57, October 3, 2007, pp. 7174-7175 and Testimony of Ron Townshend, vol. 57, October 3, 2007, p. 7196.
188 Bromley Paper on Funding Terrorism and Charities, p. 13.
189 Testimony of Terry de March, vol. 57, October 3, 2007, pp. 7161-7162.
190 Bromley Paper on Funding Terrorism and Charities, p. 14.
191 Testimony of Ron Townshend, vol. 57, October 3, 2007, pp. 7197, 7208.

the legitimacy of being a charity by passing [itself] off as such."[192] Even if an NPO does not call itself a charity, simply being an NPO can give it legitimacy in the mind of the public.

Ron Townshend, Registrar with BC Registry Services, testified that legislation regulating NPOs in most provinces is similar.[193] He also spoke about the almost complete lack of oversight of NPOs:

> ...I questioned my fellow Registrars across the country on this because I was interested in finding out how much time they spend working with their non-profit organizations. Some spend some time but most of them spend very little time, actually. They basically say it's not their mandate and they let the [NPOs] work internally or go to court or whatever.[194]

The role of a provincial registrar includes ensuring that NPOs comply with relevant provincial legislation and providing registration assistance.[195] Townshend explained that his office has four full-time staff members responsible for handling NPOs.[196] As Registrar, he reviews the applications and constitutions, but not the bylaws, of NPOs seeking registration in the provincial corporate registry.

Not all provinces require NPOs to submit their bylaws to their registrar.[197] Townshend did not believe that it was his role to become involved in an NPO's internal affairs.[198] The BC Registrar has very limited authority to investigate NPOs.[199] The Registrar can issue a certificate confirming that an NPO is in good standing in meeting its filing requirements, although this does not necessarily mean that the NPO is in good standing in respect of its conduct.[200] Responses from all jurisdictions to a questionnaire about oversight showed no evidence of greater scrutiny or control of NPOs in other provinces and territories.

Townshend explained that there is "…a fair amount of confusion" in BC in the discussion of NPOs,[201] which might be unincorporated or incorporated, provincial or extra-provincial:

> I have to say that there is a fair amount, at times, of confusion that goes on with the public and others around the role of the

---

192 Testimony of David Duff, vol. 85, November 29, 2007, p. 10910.
193 Testimony of Ron Townshend, vol. 57, October 3, 2007, p. 7205.
194 Testimony of Ron Townshend, vol. 57, October 3, 2007, p. 7199.
195 Testimony of Ron Townshend, vol. 57, October 3, 2007, p. 7197.
196 Testimony of Ron Townshend, vol. 57, October 3, 2007, p. 7195.
197 Testimony of Ron Townshend, vol. 57, October 3, 2007, pp. 7198-7199.
198 Testimony of Ron Townshend, vol. 57, October 3, 2007, p. 7199.
199 Testimony of Ron Townshend, vol. 57, October 3, 2007, p. 7199. Townshend believed that he was going further than his predecessors in this regard.
200 Testimony of Ron Townshend, vol. 57, October 3, 2007, p. 7197.
201 Testimony of Ron Townshend, vol. 57, October 3, 2007, p. 7200.

> Registrar and what all these different kinds of societies and charitable status really mean.[202]

The confusion arises in part because there is no single department or government source in BC for complete information about NPOs.[203] Provincial governments in general are content simply to confirm registration.

Townshend testified that some 658 extra-provincial NPOs were operating in BC, of which 375 were federally registered and 150 were registered in other provinces. The remaining NPOs originated abroad.[204] Generally speaking, foreign NPOs can choose whether to register in BC For example, a charity or NPO from Japan can operate in BC without registering there. Townshend said that, as Registrar, he had the power to force extra-provincial NPOs to register, but had never done so.[205]

Townshend described NPOs as a "maze."[206] He said that when an NPO wants to register as a charity, it is referred to the CRA. That same NPO may later register with the BC Corporate Registry as a provincial NPO.[207] Even if the CRA revokes the charitable registration of the NPO, it can remain registered as a provincial NPO[208] and can still call itself a charity (although it cannot issue tax receipts).

There is no single common identifier for NPOs in Canada that would allow a cross-Canada search to identify existing NPOs. However, some provinces were using the federal business identifier numbering system (for federally incorporated bodies) for NPOs. Such an approach will apparently be considered for use on a wider scale.[209] Townshend noted that the Charities Directorate has approached BC Registry officials to explore a joint filing process for NPOs that are seeking registered charity status.[210] That would alleviate at least some of the confusion surrounding the status and registration of NPOs.

Townshend said he was vaguely familiar with the processes for listing of terrorist entities but had not worked with the lists.[211] He testified that this Commission was the first body to ask him, as Registrar, about TF issues.[212] He said that "… for the most part it's not something we get involved in, or have at least at this point."[213] He also stated that corporate registrars across the country were part of

---

202 Testimony of Ron Townshend, vol. 57, October 3, 2007, pp. 7197-7198.
203 Testimony of Ron Townshend, vol. 57, October 3, 2007, p. 7198.
204 Testimony of Ron Townshend, vol. 57, October 3, 2007, pp. 7200-7201.
205 Testimony of Ron Townshend, vol. 57, October 3, 2007, p. 7201.
206 Testimony of Ron Townshend, vol. 57, October 3, 2007, p. 7201.
207 Testimony of Ron Townshend, vol. 57, October 3, 2007, p. 7204.
208 Testimony of Ron Townshend, vol. 57, October 3, 2007, p. 7216.
209 Testimony of Ron Townshend, vol. 57, October 3, 2007, p. 7203.
210 Testimony of Ron Townshend, vol. 57, October 3, 2007, p. 7206.
211 Testimony of Ron Townshend, vol. 57, October 3, 2007, p. 7212.
212 Testimony of Ron Townshend, vol. 57, October 3, 2007, p. 7207.
213 Testimony of Ron Townshend, vol. 57, October 3, 2007, p. 7208.

a close-knit group which met annually but that, to that point, TF had not been discussed.[214]

Townshend had assisted RCMP investigators with inquiries about particular NPOs.[215] He expressed a clear willingness to become involved in TF issues if asked by the province.

Remaining an NPO reduces government oversight of the organization's activities and also reduces controls on how the funds obtained by the NPO can be disbursed. For example, NPOs can have political or other purposes that are not permitted of registered charities. Bromley made similar points in his testimony:

> …[When] there is no tax receipt given, there is much less regulatory supervision on how the funds are then distributed out of the non-profit and I don't think that's unreasonable but the reality is that they then can make unrestricted grants by simply writing a cheque to any non-proprietary organization internationally and they don't have to worry about agency agreements. They don't have to worry about the same accountability for those funds and there aren't the limitations on them actually being charitable. Anything that is [a] public good in the broadest sense, you know, qualifies.[216]

In his paper prepared for the Commission, Bromley expressed concerns about the lack of attention to NPOs in anti-TF efforts:

> In my opinion, the collective discussion on how Canada's legal framework might facilitate terrorist financing has put too much emphasis on the favoured tax position of registered charities and not enough emphasis on the position of the non-profit organizations.[217]

Professor Duff called for more extensive federal-provincial cooperation in regulating both NPOs and charities:

> Since federal regulation applies only to charities that seek or obtain registered status, moreover, not charities that do not apply for registered status, nor other nonprofit and voluntary organizations, federal and provincial governments should also consider what joint initiatives might be taken to establish a more extensive regulatory regime for charities and other

214 Testimony of Ron Townshend, vol. 57, October 3, 2007, p. 7209.
215 Testimony of Ron Townshend, vol. 57, October 3, 2007, pp. 7207-7208.
216 Testimony of Blake Bromley, vol. 67, October 26, 2007, pp. 8431-8432.
217 Bromley Paper on Funding Terrorism and Charities, p. 13.

> nonprofit and voluntary organizations, irrespective of their registered status under the *ITA*.[218]

Several months after Townshend testified, a report in *The Globe and Mail* said that his office had begun to vet organizations to check for links to terrorism: "We're starting to monitor organizations that are getting incorporated over whether or not they have been identified by the United Nations or the federal government as a terrorist organization."[219]

6.7 The Findings of the 2008 FATF Mutual Evaluation of Canada about the Charitable Sector

The FATF's 2004 Special Recommendations on Terrorist Financing called for countries to review the adequacy of laws and regulations that relate to entities that can be used for TF.[220] The 2008 FATF Mutual Evaluation of Canada reviewed Canada's regulation of the charitable sector[221] and gave Canada a rating of "Largely Compliant." The FATF explained how the Canadian regime functions, identified the treatment of NPOs as a potential gap, and made the following recommendations:

> Canada has taken considerable steps to implement SR VIII [the FATF's Special Recommendation VIII on non-profit organizations] in relation to registered charities, which it considers to be the sector most at risk, based on the risk assessment studies it has done. A large segment of the NPO population is not covered by the current measures using the risk based approach, but Canada should continue to monitor the risks in these other sectors. Canada should improve the existing co-ordination mechanisms between competent authorities, especially between the CRA and the parties responsible for listing and freezing applications. Again, Canada should review the capacity of CRA and FINTRAC to share information with law enforcement authorities related to the non-profit sector.[222]

---

218 Duff Paper on Charities and Terrorist Financing, p. 239.

219 Robert Matas, "Provinces to watch charities for links to terror groups," *The Globe and Mail* (February 5, 2008), online: The Globe and Mail <http://www.theglobeandmail.com/servlet/Page/document/v5/content/subscribe?user_URL=http://www.theglobeandmail.com%2Fservlet%2Fstory%2FLAC.20080205.BCREGISTERY05%2FTPStory%2FNational&ord=3350358&brand=theglobeandmail&force_login=true> (accessed March 3, 2009).

220 FATF Special Recommendation VIII: Non-profit organisations.

221 2008 FATF Mutual Evaluation of Canada, paras. 1411-1441.

222 2008 FATF Mutual Evaluation of Canada, para. 1442. See also p. 306 of the same document.

6.8 Criticisms and Challenges Relating to Canada's Approach to Fighting Terrorist Financing in the Charitable Sector

6.8.1 The System May Overreach

Bromley and Carter both testified that charitable registrations are more difficult to obtain now, due to new requirements imposed by the CRA.

Carter testified about the interpretive notes to FATF's Special Recommendation VIII, noting the provision that anti-TF legislation should not disrupt or discourage legitimate charitable activities.[223] In his paper prepared for the Commission, he made similar comments:

> [W]hile Canada's anti-terrorism legislation is very much a product of a complex array of international initiatives, conventions and multilateral agreements that establish daunting requirements for charities, these same international requirements at least acknowledge the need to strike a balance between efforts to thwart terrorist financing and ensuring that legitimate charitable programs can continue to operate. Specifically, the Financial Action Task Force ("FATF"), in a key policy document concerning the oversight of the non-profit organizations sector internationally, reminds its member countries to ensure that "(m)easures adopted by countries to protect the NPO sector from terrorist abuse should not disrupt or discourage legitimate charitable activities" and also that those measures "should to the extent reasonably possible avoid any negative impact on innocent and legitimate beneficiaries of charitable activity".[224]

6.8.2 The Status and Legal Framework of the CRA Itself

The Commission heard a range of views, both in testimony and in papers, about the suitability of having charities regulated by the CRA. Bromley criticized having the CRA as regulator of charities. The CRA is, at its core, the regulator of Canada's taxation system. This model can be described as the "fiscal regulator" model. In contrast, the Charity Commission of England and Wales is set up expressly to regulate charities. The Charity Commission has more extensive powers than the CRA to regulate, monitor and impose sanctions on charities that breach the law. The Canadian fiscal regulator (tax-based) model has other deficiencies as well:

---

223 Testimony of Terrance Carter, vol. 67, October 26, 2007, p. 8376.
224 Carter Paper on Impact of Anti-terrorism Legislation on Charities in Canada, pp. 2-3.

- It may allow fiscal considerations to trump the charities' best interests and may create distrust of government; and
- The need for confidentiality can impede the work of the regulator and reduce the effectiveness of measures to reduce TF.

However, Kenneth Dibble of the England and Wales Charity Commission testified that a tax-based model that provides fiscal relief (such as Canada's) had some advantages over the Charity Commission model, including the ability to revoke registration and removing tax benefits.[225]

The Charities Directorate, as part of the CRA, has no choice but to operate under the general rules and approaches of that fiscal regulator. Bromley, in his paper, not only expressed doubts that CRA was the appropriate regulator of charities[226] but noted that this could weaken relationships with charities:

> CRA also has difficulty building strong relationships with charities because it is a tax collection agency, which understands that in regulating the charitable sector its 'mandate is to protect the tax base.'[227]

The Commission's hearings explored the differing functions of regulators. Professor Duff testified about the considerable trust that exists between the UK charitable sector and the UK Charity Commission:

> I think the UK Charity Commission generally is regarded as having a fair bit of trust from the charitable sector, and I don't blame anyone at the CRA, but they're kind of the gatekeepers on the fiscal benefits.... they're going to always have a more adversarial relationship...[with the charitable sector.][228]

Mark Sidel made similar points in a paper prepared for the Commission. The paper contains an extensive analysis of the positive experience that the United Kingdom has had with its Charity Commission.[229]

Duff's paper went on to elaborate on the limited role that the CRA can play because of the federal division of powers:

---

225 Testimony of Kenneth Dibble, vol. 59, October 9, 2007, p. 7328. Dibble stated that "…[o]ne significant difference is one you touched on before about the removal of registration or the removal of status as a compliance remedy, and … many people have said to me why can't the commission remove this charity from the register because of what it's done. And you can argue this is a weakness in our system. And the North American model, where there is a sort of an ability to remove the tax advantages or perhaps even de-registration of a non-compliant organization, is a shorter more effective and more resource-effective way of actually dealing with the problem."

226 Bromley Paper on Funding Terrorism and Charities, p. 7.

227 Bromley Paper on Funding Terrorism and Charities, p. 19.

228 Testimony of David Duff, vol. 85, November 29, 2007, p. 10908.

229 Sidel Paper on Terrorist Financing and the Charitable Sector, pp. 162-175.

> [B]ecause federal jurisdiction over charities is incidental to its taxing power, federal regulatory efforts in this area have tended to emphasize monitoring and investigation in order to assess eligibility for tax benefits, rather than advice and support in order to assist charities to carry out their activities in a manner consistent with their legal obligations and charitable purposes.[230]

Professor Duff argued that there has been a growing emphasis in recent years on federal initiatives to provide advice and support to charities, such as the Charities Partnership and Outreach Program.[231] Nonetheless, the risk remained that the CRA could lean towards enforcing its fiscal rules rather than towards assisting charities.

However, Terry de March, the Acting Director General of CRA's Charities Directorate, denied that the CRA had been pressured to recoup fiscal benefits rather than allowed to help charities comply with the legislation.[232] For example, the amounts identified by Statistics Canada as "foregone revenue" from tax deductions were never used as a benchmark by the Charities Directorate in its work.

6.8.2.1 The Fiscal Regulator Model and Confidentiality

Bromley argued in his paper that the confidentiality provisions binding a fiscal regulator such as the CRA can make its fight against TF, less effective.[233]

Despite the expanded disclosure now allowed under the *ITA* because of amendments introduced by Bill C-25, the *ITA* still prevents the CRA from disclosing some information that may be relevant to fighting TF. In contrast, the Charity Commission of England and Wales discloses on its website examples of cases where the Commission has investigated registered charities for various matters, including alleged involvement in terrorism. There were 20 reports on the Commission's website as of June 2008. In a 2008 report about one investigation, the Charity Commission released information that included the name and general description of the charity, the source of the Commission's concern, when the Commission initiated its inquiry, the issues at stake, the time scale of the inquiry, the findings, the regulatory action taken, the impact of the Commission's intervention, the resources applied to the investigation, the action required of the charity's trustees and, finally, "lessons for other charities."[234]

---

230 Duff Paper on Charities and Terrorist Financing, p. 204.
231 Duff Paper on Charities and Terrorist Financing, p. 204.
232 Testimony of Terry de March, vol. 57, October 3, 2007, p. 7182.
233 Bromley Paper on Funding Terrorism and Charities, p. 16.
234 As an example, see the Newham Foursquare Church, online: United Kingdom Charity Commission <http://www.charity-commission.gov.uk/investigations/inquiryreports/newham4.asp> (accessed June 6, 2008).

The *ITA* limits the information that can be disclosed to any person about a charity to the following:

> (a) a copy of the charity's governing documents, including its statement of purpose;
>
> (b) any information provided in prescribed form to the Minister by the charity on applying for registration under [the *ITA*];
>
> (c) the names of the persons who at any time were the charity's directors and the periods during which they were its directors;
>
> (d) a copy of the notification of the charity's registration, including any conditions and warnings;
>
> (e) if the registration of the charity has been revoked or annulled, a copy of the entirety of or any part of any letter sent by or on behalf of the Minister to the charity relating to the grounds for the revocation or annulment;
>
> (f) financial statements required to be filed with an information return referred to in subsection 149.1(14);
>
> (g) a copy of the entirety of or any part of any letter or notice by the Minister to the charity relating to a suspension under section 188.2 or an assessment of tax or penalty under [the *ITA*] (other than the amount of a liability under subsection 188(1.1)); and
>
> (h) an application by the charity, and information filed in support of the application, for a designation, determination or decision by the Minister under subsection 149.1(6.3), (7), (8) or (13).[235]

6.8.2.2 Fewer Sanctions or Means of Redress are Available to the CRA

Because charities in many respects fall under provincial jurisdiction, the CRA cannot remove a charity's trustees or appoint managers. In this respect, it has fewer powers than the England and Wales Charity Commission. However, the CRA now has more sanctions available to it than before. Several intermediate sanctions were introduced in 2005, giving the CRA more flexibility in dealing with charities thought to be delinquent, including those found to be involved in terrorism or TF.

---

235 *Income Tax Act*, s. 241(3.2).

6.8.2.3 A New Charities Regulator

Some parties before the Commission called for a new charities regulator in Canada. The Air India Victims' Families Association recommended that Canada should consider adopting the Charity Commission model:

> The federal government should work cooperatively with the provinces and territories, to consider reforming the Canadian regulatory framework for charitable and non-profit sectors, in order to adopt where possible, the jurisdiction, structure, powers, and modus operandi of the Charity Commission of England and Wales.[236]

Professor Sidel summarized the advantages of the UK model when he wrote about how "…the Charities Commission employs a broad range of investigative and regulatory responses to concerns that charities have links with terrorism."[237] As well, the IN-AICCA[238] submitted that the federal government, "…in conjunction with the provincial regulatory authorities, adopt the approach of the Charities Commission of the U.K. with respect to charities in order to provide a broad range of investigative and regulatory responses."[239]

Professor Duff addressed the constitutional problems associated with regulating charities in Canada in his paper for the Commission, arguing that the federal government and the provinces could jointly delegate their powers to a regulatory agency and thereby avoid a bedevilling division of responsibility:

> [F]ederal and provincial governments should consider alternative arrangements to facilitate a more robust regulatory regime for charities, involving at the very least the exchange of information about charities and more ambitiously the possible delegation of federal and provincial authority over charities to an administrative agency that could exercise broad supervisory and regulatory powers."[240]

Professor Duff also called for measures that will treat charities and NPOs as allies against terrorism:

> [T]he other policy objective, I think, is to provide support to charities and other voluntary organizations so that they can

---

236 *Where is Justice?*, AIVFA Final Written Submission to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, February 29, 2008, p. 159.
237 Sidel Paper on Terrorist Financing and the Charitable Sector, p. 196.
238 Submissions of the Family Members of the Crew Victims of Air India Flight 182 and Indian Nationals, Air India Cabin Crew Association, Sanjay Lazar and Aleen Quraishi [IN-AICCA Submission].
239 IN-AICCA Submission, p. 46.
240 Duff Paper on Charities and Terrorist Financing, p. 239.

> function appropriately and I think that they should be viewed ... as allies in the struggle against terrorism for the most part rather than potential enemies or suspects in the struggle against terrorism; allies in many respects that they build social solidarity.[241]

The CRA has explored reform of the charity sector as part of CRA's Voluntary Sector Initiative (VSI) process,[242] which included a brief consideration of the UK model.

6.8.3 The Need for Charities to Receive Practical Guidance

Some Canadian charities believe that they are being left to fend for themselves in an environment which they do not always fully understand.

In his paper, Carter argued that registered charities could unwittingly be affected by new legislation aimed at fighting terrorism and TF. He described the *Criminal Code* provisions dealing with terrorism and TF as producing a "Super *Criminal Code*." Almost any charity, particularly one conducting overseas operations, could find itself caught by the provisions.[243] Carter also suggested that the "learning curve" for charities to understand the anti-TF regime was very high.[244] He had not encountered any charity whose officials knew of the requirements for charities carrying out international activities.[245]

Professor Sidel commented in his paper about the difficulties that many charities face in complying with American best practices. He explained how the US Treasury was required to withdraw guidelines drafted in 2002 because of widespread concerns that they created unrealistic standards. New guidelines were issued in 2005, but the nonprofit community "…remained deeply concerned that these so-called 'voluntary best practices' were in fact stealth law."[246]

There is some support for new guidelines for Canadian charities. For example, Carter recommended as follows:

---

241 Testimony of David Duff, vol. 85, November 29, 2007, p. 10891.

242 Treasury Board of Canada Secretariat, "Voluntary Sector Initiative," online: Treasury Board of Canada Secretariat <http://www.tbs-sct.gc.ca/rma/eppi-ibdrp/hrdb-rhbd/archive/vsi-isbc/description_e.asp> (accessed March 3, 2009). See also Testimony of Blake Bromley, vol. 67, October 26, 2007, p. 8448.

243 Carter Paper on Impact of Anti-terrorism Legislation on Charities in Canada, pp. 6-24.

244 Testimony of Terrance Carter, vol. 67, October 26, 2007, p. 8397.

245 These requirements are set out in the US Department of the Treasury paper on best practices for US-based charities and have been incorporated by reference into the CRA's requirements for charities in Canada. Testimony of Terrance Carter, vol. 67, October 26, 2007, p. 8401; *U.S. Department of the Treasury Anti-Terrorist Financing Guidelines: Voluntary Best Practices for U.S. – Based Charities*, online: US Department of the Treasury <http://www.treasury.gov/offices/enforcement/key-issues/protecting/docs/guidelines_charities.pdf> (accessed March 3, 2009).

246 Sidel Paper on Terrorist Financing and the Charitable Sector, p. 180.

> In consultation with the charitable sector, the Canada Revenue Agency [should] develop and put into effect "made-in-Canada" best practice guidelines to provide assistance to applicants for charitable status and registered charities in their due diligence initiatives.[247]

The House of Commons Subcommittee on the Review of the *Anti-terrorism Act* made a very similar recommendation:[248]

> Such best practice guidelines would be based on the experience of Canadian applicants and registered charities in carrying out due diligence assessments in the Canadian context, especially when such organizations have limited resources and expertise to carry out such examinations. These best practice guidelines should suggest both general policies and checklists that could be administered by applicants and registered charities in carrying out their due diligence assessments.[249]

6.8.4 CRA Outreach and Education

The CRA has relationships with both national and international charities. As a result, it is in a unique position to acquire information to help in the fight against terrorism and TF. There appear to be no legislative constraints preventing the Charities Directorate from conducting further outreach activities in vulnerable communities and helping to strengthen existing bonds.

Even though the Charities Directorate, due to constitutional limitations, does not have a broad range of tools, it could, as is the case with the Charity Commission of England and Wales, become more involved at the "ground level," and possibly be seen more as an ally that can provide appropriate and timely information to the public. A "hands-on" outreach program, especially in communities that are more vulnerable to TF and to possible exploitation, might lessen the chances of community members being co-opted to assist extremists.[250]

6.8.5 More Extensive Disclosure by the CRA

At present, section 241(3.2) of the *ITA* permits the CRA to publish certain information about current or previously registered charities. Duff suggested that it would be appropriate for information about applicants for charitable status to be disclosed.[251] The CRA could then publish, on its website or elsewhere, the

---

247 Carter Paper on Impact of Anti-terrorism Legislation on Charities in Canada, p. 43.
248 See Recommendation 28 in House of Commons Report on the *ATA*, p. 36.
249 House of Commons Report on the *ATA*, p. 36.
250 See Bromley Paper on Funding Terrorism and Charities, p. 17.
251 Testimony of David Duff, vol. 85, November 29, 2007, p. 10906.

same information about applicants for charitable status that it now publishes about registered charities. This would make more information available to the public and to overseas communities in Canada. In turn, individuals and communities, not only the CRA, could then monitor applicants for charitable status, just as they are now able monitor registered charities.

VOLUME FIVE
TERRORIST FINANCING

CHAPTER VII: RESOLVING THE CHALLENGES OF TERRORIST FINANCING

7.1 Introduction

Suppressing terrorism by attacking the financing efforts behind it is an uphill battle. Terrorist acts themselves may cost very little. The direct costs of the actual bombing of Air India Flight 182 that claimed 329 lives have been estimated at under $10,000, although the costs of maintaining the conspiracy that led to the bombing would have been higher. The cost of the 2004 Madrid train bombings that claimed 191 lives was estimated at €15,000, not including significant organizational costs.

Terrorist financing (TF) is also complex. There are many sources of the relatively small sums needed to finance terrorism, including open fundraising, extortion, use of charities, contributions from legitimate employment and business income, proceeds of organized crime and direct state support. There are also many hard-to-detect ways to move funds to their destination. The 9/11 Commission concluded that "…trying to starve the terrorists of money is like trying to catch one kind of fish by draining the ocean."[1]

It is impossible to obtain a clear picture of the extent of TF in Canada. In 2006-07 alone, FINTRAC disclosed to other agencies 33 cases involving $200 million of suspicious transactions that may have involved TF or other threats to the security of Canada. In addition, it disclosed eight cases involving suspicious transactions that may have involved money laundering and TF or threats to the security of Canada. The dollar value of the disclosures in these eight cases was $1.6 billion.[2] Even if only a small percentage of those suspicious transactions turned out in fact to involve TF, the dollar value would be significant.

Terrorist groups can respond quickly to efforts to suppress TF in one sector, such as financial institutions, by moving to another, such as informal value transfer systems. Revoking the registration of a charity that has been associated with TF may simply result in the organization becoming a not-for-profit body that continues to funnel funds to terrorists. Professor Martin Rudner suggested

---

1 National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, p. 382, online: National Commission on Terrorist Attacks Upon the United States <http://www.9-11commission.gov/report/911Report.pdf> (accessed September 23, 2009).

2 Financial Transactions and Reports Analysis Centre of Canada, *FINTRAC 2007 Annual Report*, p. 8, online: Financial Transactions and Reports Analysis Centre of Canada <http://www.fintrac.gc.ca/publications/ar/2007/ar-eng.pdf> (accessed June 3, 2009).

that an operating assumption behind any financial intelligence strategy "… must surely be that criminal and terrorist (mis-)behavior is almost infinitely adaptable."[3]

Much of Canada's anti-TF effort is based on an anti-money laundering model that focuses on transactions of $10,000 or more. Although there is some overlap, the money laundering model is not easily transferred to TF, which often involves smaller sums and "clean" money – money not derived from the proceeds of crime. The small sums needed to finance terrorist acts are not likely to be discovered through routine collection and processing of information by FINTRAC and the CRA in compliance with their governing laws. Legislation is only one of several approaches needed to combat TF. Current and accurate intelligence about terrorists is also necessary because many transactions involving TF may not otherwise attract attention.

In dealing with TF, Canada does not make the best use of its resources. Neither FINTRAC nor the CRA are sufficiently integrated into the flow of intelligence to maximize their efforts at detecting TF. Nor can they easily provide the best financial intelligence about TF cases to CSIS and the RCMP.

In Canada, there has been only one TF conviction – the Khawaja[4] case – and that case came to light through security intelligence and police investigations, not through the anti-TF work of FINTRAC.

Deficiencies in Canada's TF regime have been identified by many external reviews, conducted both domestically and by international bodies such as the Financial Action Task Force (FATF). Such reviews serve to underline the importance of subjecting all counterterrorism activities to ongoing review of their effectiveness.

Even improved anti-TF efforts will not always succeed. It needs to be recognized that the criminals who surreptitiously gather and disburse funds to terrorists are cunning and ideologically-driven. No single effort by government can defeat them. Constant vigilance and a cooperative approach among agencies are necessary.

Initiatives to counter TF should be seen as one part of a comprehensive strategy to counter terrorism. Even if they cannot stop the flow of funds, these initiatives can produce financial intelligence that in turn can show links among terrorists – links that might otherwise not be discovered. Anti-TF measures can also produce evidence for TF prosecutions which can disrupt terrorist plans and punish terrorists well before a plot is carried out.

TF prosecutions, like terrorism prosecutions in general, will be very challenging. However, they will be more manageable with the improvements to the

3 Martin Rudner, "Using Financial Intelligence Against the Funding of Terrorism" (2006) 19(1) International Journal of Intelligence and Counterintelligence 32 at 50 [Rudner Article on Using Financial Intelligence].

4 *R. v. Khawaja*, [2008] O.J. No. 4244 (Sup. Ct.) at para. 133.

prosecution system recommended in Volume Three of this report: expert prosecutors serving under a Director of Terrorism Prosecutions and fairer and more efficient means to decide when the disclosure of intelligence is necessary for a fair trial.

7.2 Current and Potential Performance Indicators for Canada's Anti-TF Program

7.2.1 The Need for Better Mechanisms to Review Performance

"Performance" or "result" indicators facilitate assessing programs or systems.[5] However, it is not always easy to show concrete results against terrorism or TF.

There is a shortage of evidence that the anti-TF program has produced concrete results. Federal government officials stressed the difficulty of doing performance assessments about activities that involve preventing some future event or deterring crime.[6] Accurately evaluating a system to combat a covert phenomenon is invariably difficult. As Keith Morrill of DFAIT testified, "… [n]obody notices a war that is averted…."[7] Diane Lafleur of the Department of Finance made similar remarks about assessing the AML/ATF Initiative as a whole. She did, however, suggest that some performance indicators existed:

> [I]t's hard to measure what hasn't happened as a result of the actions that you've taken, but there are other indicators that you can look to; statistics, for example; [the] number of FINTRAC disclosures; [the] number of seizures by Canada Border Services Agency…prosecutions, arrests, et cetera, that eventually, I think, will be able to paint a much better picture of the success of the initiative.[8]

In his paper, Professor Nikos Passas stated that one advantage of using anti-money laundering measures for TF purposes was the acquisition of statistics and numbers that could be provided as evidence of the value of work done by the authorities:

> Some advantages of [using anti-money laundering measures for TF purposes] were also that quantitative measures of action and success could be provided: one could cite the numbers of designated suspected terrorists, accounts closed, amounts or

5 For the remainder of this chapter, these will be called "performance" indicators.
6 Testimony of Keith Morrill, vol. 54, September 28, 2007, pp. 6721-6722; Testimony of Donna Walsh, vol. 57, October 3, 2007, pp. 7152-7153.
7 Testimony of Keith Morrill, vol. 54, September 28, 2007, p. 6721.
8 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6765.

assets frozen, the growing number of countries following the lead, etc.[9]

However, not all these types of statistics are collected in Canada. At best, the development of quantitative measures is a work in progress.[10] The 2008 FATF Mutual Evaluation of Canada gave a "Largely Compliant" rating for Canada's efforts to collect statistics, but the FATF also identified several areas where Canada needs to improve.[11]

More comprehensive statistics would give a better understanding of the anti-TF program and facilitate regular international and domestic assessments of its performance. As was mentioned during the Commission hearings, further information that can be used to assess performance will be collected in the work leading up to the completion of the Performance Evaluation Framework, work led by Finance Canada.

7.2.2 Number of Prosecutions or Convictions

Disrupting and preventing terrorist activities are important objectives, but the public may understandably measure "success" by the number of TF prosecutions or convictions. As of January 2009, more than seven years after the enactment of the *Anti-terrorism Act*[12] (*ATA*), there has been only one successful conviction in Canada in a case that included TF charges, although a few other prosecutions are now under way and may lead to convictions.

The current number of prosecutions and convictions in Canada does not appear to show that the anti-TF program has achieved significant success. This lack of prosecutions can be blamed only in part on the inherent challenges of TF prosecutions or on the relative infancy of the anti-TF program.[13]

---

9 Dr. Nikos Passas, "Understanding Terrorism Financing," Report prepared for the Major Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 in Vol. 2 of Research Studies: Terrorism Financing Charities and Aviation Security, p. 77 [Passas Report on Terrorism Financing].

10 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6765; Testimony of Donna Walsh, vol. 57, October 3, 2007, p. 7153.

11 Financial Action Task Force, *Third Mutual Evaluation on Anti-Money Laundering and Combating the Financing of Terrorism, Canada*, February 29, 2008, p. 289, online: Financial Action Task Force <http://www.fatf-gafi.org/dataoecd/5/3/40323928.pdf> (accessed January 27, 2009) [2008 FATF Mutual Evaluation of Canada].

12 S.C. 2001, c. 41.

13 In a paper prepared for the Commission, Professor Robert Chesney of Wake Forest University commented on the efficacy of TF charges. In the United States, such charges are usually pursued through charges of material support for terrorism. Chesney observed that "…even if the government has insufficient evidence to prosecute the suspect for a past act of violence or, more to the point, for an anticipated act of violence, it may yet have the option of pursuing a support charge in the spirit of preventive charging": Robert M. Chesney, "Terrorism and Criminal Prosecutions in the United States" in Vol. 3 of Research Studies: Terrorism Prosecutions, p. 91 [Chesney Paper on Terrorism and Criminal Prosecutions]. This is sometimes described as the "Al Capone" method of charging. The appendices to Chesney's paper reveal the aggressive efforts of American officials with respect to TF charges and indicate that the United States has far more experience with TF prosecutions than Canada: see Chesney Paper on Terrorism and Criminal Prosecutions, pp. 121-148.

In the one successful prosecution to date that involved TF charges – the Khawaja case – the indictment listed several terrorism-related charges, namely offences relating to the facilitation of terrorism and the preparation of explosive devices to perpetrate a terrorist attack. Khawaja was also charged with two offences related to TF. The first TF charge stemmed from instructing an individual to "… open a bank account and conduct financial transactions on [Khawaja's] behalf for the benefit of a terrorist group." The second charge related to providing, inviting a person to provide and making available property and financial services intending or knowing that they would be used for the purpose of facilitating or carrying out a terrorist activity or for the purpose of benefiting others who were facilitating or carrying out terrorist activity.[14]

In October 2008, Khawaja was found guilty of five of the original seven counts charged, including both counts that had TF elements, and not guilty on two counts (although he was found guilty of included offences with respect to those two counts). He was subsequently sentenced to ten-and-a-half years' imprisonment, in addition to the five years he had already spent in custody awaiting trial.[15]

In early 2009, another terrorism prosecution with TF elements was still underway – the "Toronto 18."[16] In both the Khawaja and "Toronto 18" prosecutions, TF charges were among others relating to terrorism. However, Canada's approach in general continues to reflect an emphasis on "chasing the bomber."

TF prosecutions can be expensive and time-consuming. Because of this, they should be used strategically to disrupt groups that pose the greatest risk. As discussed in Chapter II of Volume Three of this report, there should be mechanisms within government, including the National Security Advisor, to facilitate decisions about whether it is appropriate to refer TF matters to police or prosecutors or to use them as an ongoing source of intelligence. If a decision is made to prosecute, the Director of Terrorism Prosecutions – a new position that the Commission recommends – should facilitate the process.

In the Khawaja case, the evidence of TF was not the product of financial intelligence provided by FINTRAC or another agency.[17] Rather, it was the product of traditional intelligence and investigative techniques.

After the Commission's hearings, another RCMP investigation resulted in TF charges against an individual. The charges involved allegations of financing the Liberation Tigers of Tamil Eelam (LTTE) in Canada through the recently "listed" World Tamil Movement (WTM). This was the first Canadian prosecution based

---

14 Contravening s. 83.03(a) of the *Criminal Code*, R.S.C. 1985, c. C-46.

15 The Reasons for Sentence can be found online: The Globe and Mail <http://images.theglobeandmail.com/v5/content/pdf/ReasonsforSentences0312.pdf> (accessed September 24, 2009).

16 The informal name of the case has changed several times, from the "Toronto 18" to the "Toronto 13" to the "Toronto 11," as some charges were dropped against various defendants. The term "Toronto 18" will be used here.

17 The Commission was not privy to all the facts of the Khawaja investigation. It has relied on what has been made public and on informal discussions with the lead prosecutor.

primarily on TF charges since the *Anti-terrorism Act* came into force. It would be inappropriate to comment on the merits of the case, but it is proper to note that the LTTE has been suspected for years of being one of the main actors in TF in Canada.

Federal officials stated that building strong TF cases is a lengthy process, with many dead ends and variables. Other countries appear to face similar problems. RCMP Superintendent Reynolds described TF investigations as "an extremely complex type of investigation."[18] He noted that investigations can very easily extend up to three years.[19] It takes time, he said, to put resources in place and gather intelligence once new legislation comes into force.[20] This adds to the length of investigations. He added that the disclosure requirements imposed on the Crown by the Supreme Court of Canada in *R. v. Stinchcombe*[21] often create additional hurdles and lengthen terrorism investigations. Other issues (for example, dealing with national security claims under the *Canada Evidence Act*[22]) further complicate investigations.

Mark Potter, Assistant Director for Government Relationships at FINTRAC, made a similar observation about the length of time it takes to bring a TF case to court: "…[S]o many of these investigations take a long time and, to get to the stage of a prosecution from when we provided intelligence, the investigation can take several years."[23]

In his testimony before the Commission, John Schmidt, a senior financial intelligence analyst seconded from FINTRAC to the Integrated Threat Assessment Centre (ITAC), described the complex nature of TF: "[T]he terrorist financing or resourcing trail is not like a piece of string one can follow from its beginning to its end, but more like a river system with many tributaries and outflows, many obstructions and alternative routes, many different things floating along its course…."[24]

A 2007 Court of Quebec decision involving an investigation of the alleged financing of the LTTE by the WTM demonstrates the potential complexity of TF investigations.[25] The investigation began in 2003. Search warrants issued in April 2006 led to the seizure of documents and various types of multimedia, such as CDs, DVDs and videotapes. In 2007, the RCMP asked for a court order under section 490(3) of the *Criminal Code*[26] to allow the continued detention of items seized during the investigation.

---

18 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6819.
19 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6820.
20 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6819.
21 [1991] 3 S.C.R. 326. These disclosure requirements are discussed in Chapter V of Volume Three.
22 R.S.C. 1985, c. C-5. For more on the subject, see Testimony of Rick Reynolds, vol. 55, October 1, 2007, pp. 6843-6847. The *Canada Evidence Act* is discussed more extensively in Volume Three.
23 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6998.
24 Testimony of John Schmidt, vol. 53, September 27, 2007, p. 6655.
25 *Boudreau v. World Tamil Movement* (May 31, 2007), Montreal District, 500-01-017300-044 (C.Q. (Crim & Pen. Div.)), Villemure, Q.C.J.
26 R.S.C. 1985, c. C-46.

Most of the documents seized were in Tamil. Of almost 5,000, more than 3,400 needed translation. In addition, 18 computer hard drives containing files written in Tamil were seized. The case involved 63 suspects and international transfers of funds. The investigation required forensic accountants, computer technicians and lawyers. From the time of the seizure in April 2006 to the time of the application to continue the detention of items seized, eight police officers, a civilian and an interpreter worked full time on the investigation. The judge concluded that detention of the items seized for a further year was justified. In April 2008, the case was the subject of a 184-page affidavit, another indicator of its complexity.[27]

Investigations of TF by law enforcement authorities may not always lead to TF prosecutions. They may, however, lead to the disruption of terrorist plans or activities and unearth previously unknown links among terrorists. In the end, a TF investigation may help prosecute a non-TF offence. TF investigations may also help authorities understand wider terrorist networks. It may be worthwhile to forego prosecution of minor TF players to obtain, over the long term, intelligence and evidence about more important figures. For this reason, measuring the success of anti-TF measures by looking at the number of TF prosecutions might not capture the true value of the work.

7.2.3 The Value of Intelligence Obtained

Obtaining further intelligence from a TF investigation can be an indicator of the value of anti-TF operations, although the impact of this intelligence is difficult to assess.

7.2.4 Number of Entities "Listed" under the *Criminal Code*

The various listing processes in Canada were described in Chapter II of this volume. Listing is an important component of the TF tool kit since reporting entities are required to determine whether their accounts and services involve listed entities.[28] Any transaction linked to one of the listed entities will be reported to FINTRAC as a suspicious transaction. Listed entities also become prime targets for any agency with a role in the fight against terrorism generally.

It could be argued that the increasing number of listed entities is an indication that Canada is making progress in the fight against terrorism and TF.[29] Furthermore, the listings under the *Criminal Code* – unlike the listings under UN Resolution 1267[30] – are made using a Canadian process.

---

27 Affidavit of Shirley Davermann, April 1, 2008.

28 *Criminal Code*, R.S.C. 1985, c. C-46, ss. 83.08-83.12.

29 Since each listing is revised at regular intervals, this should weed out any entities that are no longer involved in terrorism. Any increase in the number of entities listed would therefore not be due to entities remaining on the list after their terrorist activities have ceased.

30 The listing process is explained in section 2.4.

7.2.5 Number and Monetary Value of Frozen Accounts

The value of funds held in frozen bank accounts belonging to listed entities changes over time, since funds may be forfeited or released. A total of $186,335 was held frozen in 10 accounts in Canadian financial institutions as of November 2006.[31] As of April 2008, $69,625 was held frozen in nine accounts.[32] These numbers simply show the total funds that may belong to a listed entity, held by Canadian financial institutions at a given time. There is nothing to indicate what portion of those funds, if any, was linked to terrorism.

7.2.6 FINTRAC Performance Indicators

FINTRAC's performance was a prominent topic before the Commission. In many ways, FINTRAC is the centerpiece of the Canada's anti-TF program. For this reason, FINTRAC receives a large portion of the resources available for this purpose. However, FINTRAC's effectiveness has often been questioned. There has been little evidence of value in FINTRAC's contribution to TF investigations, prosecutions or convictions. In addressing privacy concerns relating to FINTRAC operations, the Office of the Privacy Commissioner of Canada criticized FINTRAC for failing to demonstrate results:

> [T]he Centre has compiled a detailed database on individual Canadians and their finances, maintaining these records for a decade or more in some cases. And from this regime has come little discernable benefit.[33]

That is not to say that FINTRAC is not doing its work as it should. Existing performance evaluation mechanisms simply may not yet fully capture the value of FINTRAC's work. Furthermore, concrete results in complex financial investigations could be long in coming and so may not reflect the true value in the short term.

FINTRAC publishes an annual report, a performance report and a report on plans and priorities each year.[34] FINTRAC officials argued that several performance indicators are already available. As a starting point, according to Mark Potter of FINTRAC, the number of its disclosures can be considered an indication of value.[35] These numbers are its most commonly mentioned indicators in media reports and are featured in annual reports. However, questions remain about

---

31 Final Submissions of the Attorney General of Canada, Vol. III, February 29, 2008, para. 165.

32 Exhibit P-443: Summary of Meeting between Commission Counsel and Department of Finance, April 10, 2008, p. 5.

33 Exhibit P-278, Tab 5: Office of the Privacy Commissioner of Canada, Submission in Response to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, "Canada's Financial Monitoring Regime," September 2007, p. 2 [OPC Submission on Canada's Financial Monitoring Regime]. A senior official of the OPC stated that this opinion may change once the OPC completes its audit of FINTRAC: see Testimony of Carman Baggaley, vol. 71, November 6, 2007, p. 9095.

34 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6972.

35 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6951.

what those numbers prove. In the 2005-06 reporting period, for example, FINTRAC made disclosures of suspected TF and other threats to the security of Canada valued at $256 million, but how much, if any, of that amount was related to TF is not clear.[36] One RCMP official questioned the $256 million figure in his testimony:

> I can only comment from the perspective of the RCMP and our investigation and we don't – we can't see that – we're not seeing that level of funding that we can attribute to terrorist financing. So I don't know how [FINTRAC is] attributing that.[37]

Decreases in the dollar value of disclosures in a given year may be because (i) the program is working, (ii) TF cases are more difficult to identify or (iii) FINTRAC is not effective. It is difficult to view the dollar value of disclosures as a performance indicator.

Professor Anita Anand criticized the use of the number of disclosures as a performance indicator: "…I think there's a gap in the legal regime at that very point that if FINTRAC is reporting a suspicious activity and that is supposed to be evidence of its efficacy, in my mind that is insufficient for us to draw that conclusion."[38]

Potter stated that the fact that FINTRAC had received 15 million financial transaction reports during the 2005-06 fiscal year (the number rose to 21.6 million for the 2007-08 fiscal year[39]) showed that the deterrence aspect of its work was effective.[40] However, the Office of the Privacy Commissioner of Canada suggested that entities might simply "over-report" to ensure compliance with reporting requirements and to avoid penalties for failing to report.[41]

As Professor Anand suggested in her paper for the Commission, a cost-benefit analysis is needed, especially since much of the cost of FINTRAC's reporting requirements are borne by private sector reporting entities.[42]

The routine collection of transaction reports should continue, as required by the *Proceeds of Crime (Money laundering) and Terrorist Financing Act*[43] (*PCMLTFA*),

---

36 Financial Transactions and Reports Analysis Centre of Canada, *FINTRAC 2006 Annual Report*, p. 8, online: Financial Transactions and Reports Analysis Centre of Canada <http://www.fintrac.gc.ca/publications/ar/2006/ar-eng.pdf> (accessed June 3, 2009).

37 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6868.

38 Testimony of Anita Anand, vol. 85, November 29, 2007, p. 10936.

39 Financial Transactions and Reports Analysis Centre of Canada, *FINTRAC 2008 Annual Report,* p. 16, online: Financial Transactions and Reports Analysis Centre of Canada <http://www.fintrac.gc.ca/publications/ar/2008/ar-eng.pdf> (accessed February 24, 2009).

40 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6952

41 OPC Submission on Canada's Financial Monitoring Regime, p. 4.

42 Anita Indira Anand, "An Assessment of the Legal Regime Governing the Financing of Terrorist Activities in Canada" in Vol. 2 of Research Studies: Terrorism Financing Charities and Aviation Security [Anand Paper on Legal Regime Governing Terrorist Financing].

43 S.C. 2007, c. 17.

but the focus of performance measures should shift to end results such as prosecutions and the distribution of valuable intelligence to other agencies. FINTRAC's performance should not be measured mainly by how many transaction reports it receives.

7.3 Lack of Adequate Performance Indicators and Assessment Mechanisms Generally

Most, if not all, current performance assessments do not show whether Canada is winning or losing the fight against TF. It may simply be that appropriate data is not available or is not being used to assess Canada's performance.

The lack of relevant statistics to help measure Canada's performance in TF matters is not a recent problem. Others noted the deficiency even before the Commission began its investigation of TF. The Auditor General of Canada made the following observation in 2004:

> The Treasury Board requires that departments and agencies measure program performance, relate it to program objectives, and report on results achieved. Indicators by which to measure performance are to go beyond activities and outputs to outcomes. Weighed against these requirements, the information on the [AML/ATF] Initiative that has been collected and reported to date is limited.[44]

It would help evaluations of the anti-TF program if federal agencies were required to compile statistics about the program's workings.

Diane Lafleur of the Department of Finance stated that Canada has "…been working diligently in the wake of recommendations from the Auditor General, among others, to develop a better performance framework for the [AML/ATF] initiative, and that is ongoing work right now."[45] The federal government now has a plan to prepare future assessments of the AML/ATF Initiative. The Department

---

44 *Report of the Auditor General of Canada to the House of Commons*, November 2004, Chapter 2: "Implementation of the National Initiative to Combat Money Laundering," para. 2.86, online: Office of the Auditor General of Canada <http://www.oag-bvg.gc.ca/internet/docs/20041102ce.pdf> (accessed January 24, 2009) [2004 Auditor General Report on Money Laundering]. This lead to the recommendation, in para. 2.92, that: "The government should establish effective mechanisms for monitoring the results of disclosures, including the extent to which disclosures are used and the impact they have on the investigation and prosecution of money-laundering and terrorist-financing offences. It should report summary information on these results to Parliament regularly."

45 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6765. See also Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6951, where he said that "…there are certainly efforts under way to strengthen results management, to strengthen the evaluation framework for the regime, so that all partners involved in combating money laundering and terrorist financing are able to provide information that contributes to a better way of measuring our overall results, which is getting at the very end point of how many people are convicted."

of Finance has retained an external consulting firm to prepare a performance evaluation framework.[46] The framework has several objectives:

- Describe the objectives, activities, outputs and expected outcomes of the Regime;
- Summarize the roles and responsibilities of each of the partner departments and agencies;
- Identify the principal evaluation issues that should be addressed during the full evaluation of the Regime; and
- Identify the performance indicators for each of these issues and assess data requirements to support analysis of these indicators, including responsibility for collecting the data and frequency.[47]

The continuing lack of a viable performance evaluation program is not acceptable. The framework described above should facilitate future assessments of the Initiative. Review of the effectiveness of all anti-TF measures should be ongoing.

The framework document being prepared should be implemented as quickly as possible, and should be made public except where national security or operational interests forbid. Such a framework should be nuanced enough to avoid focusing simply on qualitative measures, and should assess how well the anti-TF program supports Canada's overall anti-terrorism strategy.

7.4 Challenges Relating to FINTRAC

7.4.1 Privacy

FINTRAC collects significant personal information about individuals who carry out financial transactions. It keeps that information for up to 15 years, depending on the nature of the information.[48]

In Canada, privacy considerations play a major role in shaping policies and laws on TF. Mark Potter of FINTRAC testified that privacy considerations appear to have been accorded greater weight in Canada than in some other countries.[49] Satisfying privacy concerns in light of the needs of the anti-TF program, the complex nature of TF and Canada's international TF obligations, presents significant challenges.

The Office of the Privacy Commissioner of Canada described its concerns about intrusiveness of the main legislative tool of the anti-TF program, the *PCMLTFA*:

---

46 The document was shown to Commission Counsel. At the request of Department of Finance officials, the document has not been made public.

47 Exhibit P-439: Department of Finance Response to Supplementary Questions of the Commission, Question 2 [Department of Finance Response to Supplementary Questions of the Commission].

48 *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, ss. 54(d), (e) [*PCMLTFA*].

49 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6967.

> [T]he *PCMLTFA* regime has created a mandatory reporting scheme allowing government to access personal information for investigatory purposes *without* judicial authorization and *without* satisfying the standard requirement of reasonable and probable grounds but with sharp penalties for organizations and individuals who fail to report. As Stanley Cohen (General Counsel, Department of Justice) remarked before a Senate Committee reviewing C-25, such a *mandatory* reporting of suspicious transactions tests the limits of constitutional authority in Canada.[50]

The Office of the Privacy Commissioner also raised concerns about the expansion of the reporting program – the increase in the range of private sector entities required to report to FINTRAC – that Bill C-25[51] introduced into the *PCMLTFA*.[52]

Mark Potter of FINTRAC testified that the limits contained in the *Charter* and privacy laws were "simply the reality in Canada." Furthermore, he said, the changes introduced by Bill C-25 responded to law enforcement's desire for more information from FINTRAC while still "...maintaining that balance of *Charter* and privacy rights in what we are allowed to provide."[53]

The federal government appears to have gone a considerable way towards addressing privacy concerns in legislation dealing with TF. FINTRAC cannot divulge certain information to private sector reporting entities. In addition, FINTRAC cannot compel private sector entities to provide information about a specific transaction that has been identified to FINTRAC in a Voluntary Information Record (VIR) – for example, a VIR from the RCMP. This should satisfy some *Charter* privacy concerns about unreasonable search or seizure.

The government appears to have understood the specific privacy considerations attached to the information that comes under the purview of FINTRAC. In addition, Bill C-25 has added another review mechanism for the AML/ATF Initiative – the Privacy Commissioner of Canada. Every two years, the Privacy Commissioner must "…review the measures taken by [FINTRAC] to protect information it receives or collects" under the *PCMLTFA*.[54] The review will focus on the privacy measures and how personal information is protected and handled by FINTRAC. It will not consider the substantive work and mandate of FINTRAC. The Privacy Commissioner, Jennifer Stoddart, testified that her Office would not have an oversight role: "We're simply going to be looking at…[FINTRAC's] information handling procedures and processes through our audit."[55]

---

50 OPC Submission on Canada's Financial Monitoring Regime, pp. 4-5, 7.
51 *An Act to amend the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and the Income Tax Act and to make a consequential amendment to another Act* [Bill C-25].
52 OPC Submission on Canada's Financial Monitoring Regime, pp. 2-4.
53 Testimony of Mark Potter, vol. 56, October 2, 2007, pp. 6966-6967.
54 *PCMLTFA*, s. 72(2).
55 Testimony of Jennifer Stoddart, vol. 72, November 6, 2007, p. 9006.

Reviews of the effectiveness of FINTRAC should occur alongside privacy audits. Effectiveness is not entirely divorced from privacy considerations because privacy intrusions are more easily justified if shown to be effective in preventing TF and acts of terrorism.

FINTRAC is described in the *PCMLTFA* as an independent agency that "…acts at arm's length from law enforcement agencies and other entities to which it is authorized to disclose information." [56] It was positioned this way because reporting entities must report a broad range of financial transactions to FINTRAC. The drafters of the *PCMLTFA* thought that it would constitute an unacceptable privacy intrusion to allow FINTRAC freely to give information about an individual's financial transactions, or even an analysis based on that information, to law enforcement. Privacy concerns also explain in part why the O'Connor Commission recommended that FINTRAC be subject to review by the Security Intelligence Review Committee (SIRC).

The 2008 FATF Mutual Evaluation of Canada described the justification offered for the arm's-length relationship:

> The decision to provide police and other recipients with designated information only when FINTRAC reaches its threshold, rather than to provide unrestricted access to FINTRAC's data holdings, reflects the fact that FINTRAC receives a large amount of varied financial information on persons and entities, the vast majority of which is legitimate and not relevant to any investigation or prosecution.[57]

Janet DiFrancesco, Assistant Director for Macro-Analysis and Integration within the Operations Sector at FINTRAC, testified that being at arm's length from other bodies is an advantage:

> [O]ur regime is -- was created to be consistent with the Charter of Rights, and it does of course consider privacy laws but I think one of the advantages that FINTRAC does have, having been created at arm's length, is that we are also able to collect what we call more objective reports, prescribed transactions in terms of international wire transfers and large cash transaction reports.[58]

It has been suggested that FINTRAC's arm's-length relationship with other agencies is necessary to ensure compliance with the right to protection against

---

56 *PCMLTFA*, s. 40(a).
57 2008 FATF Mutual Evaluation of Canada, para. 382.
58 Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, pp. 6967-6968.

unreasonable search or seizure guaranteed by section 8 of the *Charter*.[59] Both TF and money laundering laws might be challenged as violating Charter rights; in the absence of any judicial guidance, this remains an open question dependent on the circumstances and on the exceptions in the *Charter*.

The "arm's-length" concept originated in money laundering and does not necessarily fit with the state's more compelling interests with respect to TF. Although the arms-length arrangement is designed to ensure that the FINTRAC system respects privacy values and does not allow law enforcement or security intelligence agencies unimpeded access to the vast amount of financial information that FINTRAC has collected without warrant, the arrangement has disadvantages.

The most significant disadvantage is that the arm's-length concept could encourage FINTRAC to operate in its own silo. FINTRAC might be reluctant to pull information into it, and other agencies might be reluctant to give information to FINTRAC. Instead, CSIS, the RCMP, CBSA, CSE and other agencies should all be encouraged to share information with FINTRAC, and FINTRAC should actively seek intelligence from these agencies to help guide its work.

As well, the arm's-length metaphor is misleading to the extent that it suggests that FINTRAC cannot receive or even provide information to law enforcement and security intelligence agencies. The *PCMLTA* does not prevent FINTRAC from receiving information from the RCMP, CSIS and other agencies, and Bill C-25 has significantly expanded the range of information that FINTRAC can disclose to other agencies.

The arm's-length relationship between FINTRAC and the recipients of its disclosures should be re-examined in light of the need for more extensive sharing of information among agencies in TF matters.

Even if moving away from an arm's-length relationship did violate the *Charter* provision against unreasonable search or seizure in section 8, there may be sufficient flexibility in section 1 of the Charter to justify such an infringement. The Supreme Court of Canada concluded in *Hunter v. Southam*[60] that a lower standard could be justified to authorize searches in the national security context than in ordinary criminal cases. This possibility has largely been left unexplored. Courts might rely on *Hunter v. Southam* to accept lower standards for searches dealing with TF than with money laundering. A national security justification, coupled with the need to meet Canada's international commitments with respect to TF, makes the government's case for justifying limits on privacy and other Charter rights much stronger in TF matters than in the money laundering context. As a result, more extensive information-sharing arrangements may be constitutionally acceptable in terrorism and TF matters than in "ordinary" criminal money laundering cases.

---

59 Stanley A. Cohen, *Privacy, Crime and Terror: Legal Rights and Security in a Time of Peril* (Markham: LexisNexis, 2005), pp. 266-272.

60 *Hunter v. Southam*, [1984] 2 S.C.R. 145.

7.4.2 The Critical Importance of Voluntary Information Records in FINTRAC's Terrorist Financing Work

The smaller amounts that are typically involved in TF cases than in money laundering cases impede attempts by FINTRAC to generate TF leads on its own. Fortunately, FINTRAC is empowered to receive information volunteered by anyone. As noted in Chapter III, the RCMP, CSIS, CSE, ITAC, CBSA, CRA, DFAIT and other agencies can voluntarily provide information to FINTRAC by way of a form entitled a Voluntary Information Record (VIR). Foreign FIUs and individuals can also volunteer information,[61] although they would not use a VIR to do so. Private sector reporting entities provide Suspicious Transaction Reports (STRs) to FINTRAC, in addition to reports about transactions that exceed a given monetary threshold.

The VIR process is vital to the success of FINTRAC's work on TF. As noted in Chapter III, about 90 per cent[62] of the possible TF cases that come to FINTRAC's attention do so because FINTRAC has received law enforcement or CSIS VIRs. This illustrates the importance of shared intelligence to help identify targets. It is not surprising that VIRs from CSIS or the RCMP are better at identifying targets than the millions of transaction reports that financial institutions routinely make to FINTRAC each year.

Once FINTRAC receives a VIR, its TF Unit determines whether it can produce an analysis for the submitting agency. FINTRAC should also, in appropriate cases, provide that same analysis to other relevant agencies, a step that at present can be inhibited by caveats attached by the agency submitting the VIR. Where appropriate, FINTRAC should seek exceptions to the caveats to allow further dissemination of the intelligence that the originating agency provided.

There are limits to the effectiveness of transaction reports. The solution is not always to add inflexible financial controls that may adversely affect legitimate activities and impose substantial costs on private sector partners. The key is to take an approach to sharing information and identifying targets flexible enough to respond to the ways that terrorists adapt to changing regulations. As Professor Passas stressed, "…[w]e have to clearly identify our main problems and targets, collect and analyze critically the evidence on their modus operandi, motives, aims, financing and support, and then focus on carefully planned and consistently applied policies that are instrumental to our goals and minimize the externalities and adverse effects."[63] Furthermore, "…the objectives and functions of financial controls must be well understood, and particularly the point that

---

61 *PCMLTFA* s. 54(a). CSIS provides more VIRs to FINTRAC than any other agency.

62 Testimony of Janet DiFrancesco, vol. 56, October 2, 2007 at p. 6956. Mark Potter could not give a number for the operations of FIUs in other countries: see Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6965.

63 Passas Report on Terrorism Financing, p. 106.

intelligence gathering and investigative leads are the key goals, rather than 'drying up' the financial resources of terrorism, which is an impossible task."[64]

As noted in Chapter III, FINTRAC had rarely identified cases on its own in recent years,[65] yet the FATF criticized FINTRAC for excessive reliance on voluntary reports.[66] The Commission does not share FATF's negative view of FINTRAC's reliance on leads and intelligence provided by other agencies. Such reliance is consistent with an approach that uses intelligence to help identify targets. The amounts of money at issue in TF, typically smaller than in money laundering cases, make it difficult for FINTRAC to generate leads on its own. This is further demonstration of the limits of using the money laundering model for TF matters.

7.4.3 Limits on FINTRAC's Disclosures of Designated Information

As discussed in greater detail in Chapter III, even after the Bill C-25 amendments, some limits remain on the information that FINTRAC can disclose to agencies such as the RCMP and CSIS. If an agency wants information beyond "designated information" – for example, FINTRAC's own analysis that led to its decision to disclose – a production order from a judge is required. The 2008 FATF Mutual Evaluation of Canada stated that 14 production orders had been sought to that point by law enforcement. It is not known whether any of these orders related to TF. The main point is the relatively small number of orders. The FATF Mutual Evaluation identified two possible explanations for this:

> Law enforcement authorities cite two basic reasons for the reluctance to apply for production orders. One is that the legislative threshold is high, the same as for a search warrant: the applicant must satisfy the court that there are "reasonable grounds to believe" an offence has been committed. A search warrant is preferable because it provides direct access to target information that could be used as evidence. Second, the information contained in [a] FINTRAC disclosure is generally considered below the legislative threshold [of evidence] that a production order requires.[67]

---

64 Passas Report on Terrorism Financing, p. 90. Passas also states at p. 79 that there are risks that inadequate or ill-thought CFT measures may: drive networks and transactions underground, losing the opportunity to monitor, prevent, better understand and design long-term strategies; cause collateral damage and unnecessary economic disruptions; alienate ethnic groups; undermine our own legitimacy; induce superficial (paper) compliance by various countries or agencies, thereby having an ineffective international CFT regime (i.e. rules and laws may be in place, but they are of little use if they go un-enforced); neglect of more serious problems (regarding terrorist financial vulnerabilities or other serious crimes); produce more grievances and provide more fertile ground for the recruitment of new militants. Moreover, if the root causes of terrorism are ignored, the problems the international community faces will remain in place despite apparent successes: that is, even if designated individuals or groups are arrested or killed in action, other groups or secular radicalism may follow.

65 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6920.

66 2008 FATF Mutual Evaluation of Canada, para. 21.

67 2008 FATF Mutual Evaluation of Canada, para. 387.

The lack of authority in the *PCMLTFA* for FINTRAC to disclose information beyond designated information, including its own analysis of the basic financial data, is a significant deficiency. If FINTRAC's analysis were automatically included in its disclosures of designated information, recipients could make better and more timely use of the disclosure, and the links between FINTRAC and its counterterrorism partners would be strengthened.

One solution could be to amend the *PCMLTFA* to require FINTRAC to include its analysis in disclosures if it had "reasonable grounds to *believe*," for example, that information would be relevant to investigating or prosecuting a TF offence, a more stringent precondition than "reasonable grounds to *suspect*." A "reasonable grounds to believe" provision would result in a less serious privacy intrusion. Any privacy concerns that remained could be somewhat allayed by limiting the requirement to disclose to TF cases. It should be easier under the *Charter* to justify infringements of privacy to counter terrorism than to counter money laundering.[68]

7.4.4 FINTRAC Priorities

FINTRAC gives priority to possible TF cases regardless of the size of the operation.[69] However, there may be cases where money laundering increases the wealth and power of criminal organizations, in turn facilitating violent activities that could rival the violence associated with terrorism. For this reason, FINTRAC should not automatically give priority to TF investigations, although it may normally be appropriate to do so. In some cases, FINTRAC may want to consult with the RCMP and CSIS in deciding its priorities.

7.4.5 Adding New Reporting Sectors

Under the *PCMLTFA*, reporting entities must report certain financial transactions to FINTRAC. These entities include federally-regulated banks, provincially-regulated caisses populaires and credit unions, money services businesses and securities dealers. The *PCMLTFA* also makes it possible to add other types of entities or individuals to the list of reporting entities.

Although FINTRAC monitors various sectors to determine if they should be added as reporting entities, Canada was reprimanded in the 2008 FATF Mutual Evaluation of Canada for not following appropriate risk-management techniques in this regard.[70] The ability to add new financial sectors is important since those who finance terrorism seem able to adjust their behaviour to avoid dealing with entities that are obliged to report. Ideally, FINTRAC should be able to obtain financial transaction reports from all sectors that can be used for TF.

---

68 *Hunter v. Southam* [1984] 2 S.C.R. 145; *Re Section 83.28 of the Criminal Code* [2004] 2 S.C.R.

69 Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6962; Exhibit P-440: FINTRAC Response to Supplementary Questions of the Commission, February 5, 2008, Question 2(m)(i) [Second FINTRAC Response to Supplementary Questions of the Commission].

70 2008 FATF Mutual Evaluation of Canada, paras. 630-640.

7.4.6. The Need for FINTRAC to Provide Better Information and Training to Private Sector Reporting Entities

Private sector reporting entities are essential partners in FINTRAC's work to detect and deter TF. The reporting entities provide, at their own expense, most of the information and data which FINTRAC receives.[71] Suspicious Transaction Reports (STRs) from reporting entities play an important role in alerting FINTRAC to possible TF. These STRs, like the VIRs supplied by government agencies, show the value of shared intelligence in identifying targets for further examination by FINTRAC, as opposed to reliance on the automatic reporting of certain prescribed transactions, such as those of $10,000 or more, or those involving listed terrorist individuals or organizations.

The preparation of STRs that are useful depends on the ability of private sector reporting entities to identify what is suspicious. However, FINTRAC perhaps has not done a good job of communicating to reporting entities the distinction between TF and money laundering, and some reporting entities do not see TF as a priority.[72] FINTRAC should make every effort to help reporting entities identify transactions that may involve TF.[73] Better education on TF issues should lead to better and more frequent STRs about TF from private sector entities.

FINTRAC and other authorities should also supply reporting entities with current and user-friendly lists of terrorist entities and other relevant information, even if terrorists will not likely often conduct financial transactions using listed names.

CSIS and the RCMP could also assist in the training of reporting entities on TF issues. They could provide feedback to the entities about the importance of the information they supply to FINTRAC, something that FINTRAC does not at present do.

7.5 The Legal Profession

Members of the legal profession have been identified by the FATF as possible conduits for TF or money laundering. The "40 Recommendations" of the FATF on money laundering explain that jurisdictions are responsible for ensuring that the legal profession is covered by anti-TF measures.[74] The "Interpretative Notes to the 40 Recommendations of the FATF" also state that each jurisdiction must determine the extent of legal professional privilege, and that lawyers might be

---

71 *PCMLTFA*, s. 54.

72 Exhibit P-241, Tab 2: Deloitte, Report of Findings as a Result of the Interviews of Regulated Entities on the Topic of Terrorist Financing In, Through and Out of Canada, September 28, 2007, paras. 5.1.4, 5.1.12.

73 This could be done using a three-pronged approach: adding more information on the listings page about each organization's suspected means of TF; creating an open-source database, possibly to be maintained by an academic institution with funding by government; and providing more extensive information about specific groups, if that information is available.

74 Recommendations 12 and 16, online: Financial Action Task Force <http://www.fatf-gafi.org/document/28/0,3343,en_32250379_3226930_33658140_1_1_1_1,00.html> (accessed January 24, 2009).

allowed to send STRs to their regulatory bodies instead of to their country's FIU if there is appropriate cooperation between the two bodies.[75]

In November 2001, regulations made under the predecessor to the *PCMLTFA* came into force. The regulations would have required lawyers to report suspicious transactions. The Law Society of British Columbia and the Federation of Law Societies of Canada successfully challenged this obligation.[76] In granting a temporary exemption, Justice Allan of the Supreme Court of British Columbia spoke of the regulation's damage to the solicitor-client relationship:

> The proclamation of s. 5 of the Regulations authorizes an unprecedented intrusion into the traditional solicitor-client relationship. The constitutional issues raised deserve careful consideration by the Court. The petitioners seek a temporary exemption from the legislation until the merits of their constitutional challenge can be determined. I conclude that the petitioners … are entitled to an order that legal counsel are exempt from the application of s. 5 of the Regulations pending a full hearing of the Petitions on their merits.[77]

Following this interlocutory decision, the federal government and the Federation of Law Societies of Canada agreed that the matter would be adjourned indefinitely if the government agreed, which it did, not to require lawyers to report to FINTRAC without the Federation's consent. If, however, a future government required lawyers to report, the case could go to a full hearing.

In 2005, then FINTRAC Director Horst Intscher stated that, "I would be happier if there were some reporting requirement for lawyers because, at present, the reporting we get is not by them but about them by other financial institutions."[78]

Solicitor-client privilege was addressed during both Senate and House of Commons committee reviews of the *Anti-terrorism Act*. However, both reviews primarily discussed the *Criminal Code* offence of not reporting terrorist property, rather than the proposed reporting obligations of lawyers under the *PCMLTFA*. The Commons and Senate committees reached opposite conclusions. The

---

75 Interpretative Note to Recommendation 16, online: Financial Action Task Force <http://www.fatf-gafi.org/document/28/0,3343,en_32250379_32236920_33988956_1_1_1_1,00.html#Interpretative_Note_to_r_16> (accessed January 24, 2009).

76 2004 Auditor General Report on Money Laundering, para. 2.30; *The Law Society of B.C. v. A.G. Canada*, 2001 BCSC 1593. Mark Potter testified that at the time the *Anti-terrorism Act* was drafted in 2001, Canada recognized the possibility that lawyers could become involved in money laundering and TF, and included the legal profession in the category of entities which were required to file reports with FINTRAC: Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6976.

77 2001 BCSC 1593 at para. 108.

78 The Senate of Canada, *Fundamental Justice in Extraordinary Times: Main Report of the Special Senate Committee on the Anti-terrorism Act*, February 2007, p. 57, online: Parliament of Canada <http://www.parl.gc.ca/39/1/parlbus/commbus/senate/Com-e/anti-e/rep-e/rep02feb07-e.pdf> (accessed February 17, 2009) [Senate Report on the *ATA*].

Commons Committee recommended a limited exemption for the legal profession from reporting requirements under the *Criminal Code*. The Senate Committee concluded that lawyers should be subject to the reporting requirements under the *Criminal Code*, arguing that the reporting scheme sufficiently protected solicitor-client privilege.

The Senate Committee report called for the government to continue its current dialogue with the legal community on the subject of reporting requirements under the *PCMLTFA*.[79] The preceding year, another Senate committee, the Standing Senate Committee on Banking, Trade and Commerce, recommended that the federal government complete negotiations with the Federation of Law Societies regarding the client-identification, record-keeping and reporting requirements imposed on solicitors under the *PCMLTFA*. The Committee called for the requirements to respect solicitor-client privilege, the *Charter* and the *Quebec Charter of Human Rights and Freedoms*.[80]

In December 2008, provisions of a regulation made under the *PCMLTFA* came into force, subjecting the legal profession to client identification, verification, record-keeping and compliance obligations, although it did not impose any reporting obligations in the normal course of providing legal services.

In its 2008 Mutual Legal Evaluation of Canada, the FATF criticized Canada because its reporting requirements did not extend to the legal profession.[81] However, the regulation governing lawyers was not then in force. It is not clear whether FATF will see this new regulation as satisfying its concerns when it comes into force. The regulation deals primarily with identification, verification and record-keeping, not with reporting, but should help identify when particular targets of an investigation have dealings with lawyers.

The concern over imposing reporting obligations on the legal profession is driven by the legitimate need to respect solicitor-client privilege – an important, but not absolute principle.[82] However, excluding certain sectors from the obligation to report suspicious transactions has the potential to weaken the entire reporting component of the anti-TF program.

This is a live issue. Other organizations have looked at this question, and their analyses should be taken into account when assessing the appropriate

---

79 Senate Report on the *ATA*, p. 57.

80 Senate of Canada, Interim Report of the Standing Senate Committee on Banking, Trade and Commerce, *Stemming the Flow of Illicit Money: A Priority for Canada, Parliamentary Review of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, October 2006, p. 14, online: Parliament of Canada <http://www.parl.gc.ca/39/1/parlbus/commbus/senate/com-e/bank-e/rep-e/rep09oct06-e.pdf> (accessed January 16, 2009).

81 2008 FATF Mutual Evaluation of Canada, para. 1235. In fact, Canada received a Non-Compliant rating on Recommendation 12 because several sectors were not covered, including the legal profession. Several of these deficiencies were remedied by Bill C-25. On the subject of the legal profession, the FATF mentioned that: "The participation of lawyers in the AML/CFT effort is essential since their current exemption leaves a very significant gap in coverage."

82 *R. v. McClure*, 2001 SCC 14, [2001] 1 S.C.R. 445.

obligations of lawyers in combatting money laundering and TF. Lawyers, of course, should not be immune from legitimate TF investigations, especially if a reasonable suspicion exists of their involvement in TF. In addition, regulations relating to the obligations of lawyers to engage in client identification should be carefully monitored to address solicitor-client privilege issues and to ensure that there are no inappropriate gaps in their obligations under the *PCMLTFA* that could weaken the anti-TF program.

7.6 Review of FINTRAC and the Role of the Prime Minister's National Security Advisor

Greater attention should be paid to the process by which FINTRAC's work is reviewed. The Commission of Inquiry into the Activities of Canadian Officials in Relation to Maher Arar recommended that the jurisdiction of SIRC be expanded to include review of FINTRAC. As discussed in Chapter IV, the O'Connor Commission's recommendations were aimed mainly at reviewing FINTRAC's work to ensure that it was proper and lawful and that it respected privacy values. This type of review is valuable and can help promote public confidence, but it should be distinguished from a review of the efficacy or effectiveness of FINTRAC's work. Indeed, Justice O'Connor drew this important distinction and was clear that his focus was on propriety.[83] That focus was understandable given the events that led to his Inquiry. This Commission's focus on the effectiveness of Canada's anti-terrorism efforts is also understandable, given that the bombing of Air India Flight 182 led to the current Inquiry.

In her paper for the Commission, Professor Anand argued that "…no body undertakes an assessment of the efficacy of the existing [TF] regime. Indeed, in the absence of such an assessment mechanism, there appears to be an assumption that the regime is effective."[84] She continued that "…it appears that SIRC may not be the appropriate body to perform this oversight role."[85] She also stressed that proper evaluation cannot be done simply by examining FINTRAC on its own. Other agencies, such as the RCMP and CSIS, needed to be examined as well.[86]

Enhancing the role of the National Security Advisor (NSA), as recommended in Chapter II of Volume Three of the Commission's report, would help the NSA evaluate how well FINTRAC works with other agencies such as CSIS, the RCMP, CBSA, CRA and CSE.

Among the Commission's recommended new responsibilities for the NSA would be working on problems associated with the distribution of intelligence, helping resolve issues related to the exchange of information among agencies

---

83 Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (Ottawa: Public Works and Government Services Canada, 2006), pp. 523-524.

84 Anand Paper on Legal Regime Governing Terrorist Financing, p. 148.

85 Anand Paper on Legal Regime Governing Terrorist Financing, p. 149.

86 Anand Paper on Legal Regime Governing Terrorist Financing, p. 151.

and providing feedback about the utility of information shared. The NSA could play a role in ensuring that intelligence agencies provide FINTRAC and the CRA with relevant information. The NSA could work on coordination issues made more difficult by the fact that not all agencies involved in TF matters (such as FINTRAC on the one hand and CSIS, the RCMP and CBSA on the other) are within the same minister's portfolio.[87]

The success of initiatives against TF will depend on the appropriate sharing of intelligence and on cooperation among multiple agencies. An NSA with enhanced responsibilities would be well-positioned to ensure appropriate coordination and review of TF efforts. Just as the NSA would have to respect police and prosecutorial independence, the NSA would have to respect statutory restrictions imposed on FINTRAC and the CRA about the information that they are permitted to distribute.

The NSA would be able to evaluate the work of the agencies in a confidential setting that would not risk security breaches. The fact that the NSA reports to the Prime Minister should make certain that the NSA has the necessary power to ensure that agencies operate effectively as part of the overall system to counter TF and terrorism.

7.7 Resources for TF Investigations

Previous chapters of this volume describing the roles of various agencies also discussed resources. The 2008 FATF Mutual Evaluation of Canada concluded that "…[o]verall, authorities seem to be well-equipped, staffed, resourced and trained,"[88] but representatives of some agencies testified about inadequate funding. The federal government appears to have resolved some of these concerns, but should continue to monitor the adequacy of resources closely.

As noted during the hearings, the term "resources" means more than money. Just as important, the term refers to the capacity to recruit and retain qualified individuals. One submission to the Commission suggested that the federal government should "…[r]eview for adequacy, the levels of financial and human resources across all government agencies responsible for combating terrorism financing, and where appropriate, increase financial and human resources."[89]

One way to enhance the quality of work of those involved in the anti-TF program would be to share training across agencies and to take steps to cut duplication of services within the agencies dealing with TF. For example, one agency could take the lead in training and make it available to other agencies. This would make efficient use of limited training funds. Training across several agencies might also help break down organizational barriers and build inter-agency linkages

87 Testimony of Tyson George, vol. 56, October 2, 2007, p. 7072.

88 2008 FATF Mutual Evaluation of Canada, para. 53. The FATF did mention that FINTRAC lacks sufficient resources for analysis.

89 *Where is Justice?*, AIVFA Final Written Submission to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, February 29, 2008, p. 160 [AIVFA Final Written Submission].

that could pay important dividends later. Joint training would also complement the enhanced use of secondments among agencies.

In some cases, it may be possible to avoid duplication of services among agencies – for example, in collecting open source material about common TF issues. Avoiding duplication might not only save resources, but may promote increased daily cooperation and exchange of information among the agencies.

7.8 Charities and Not-for-profit Organizations

As explained in detail in Chapter VI, charities and not-for-profit organizations (NPOs) can be among the many vehicles used for raising and moving funds for terrorism. Although much concern has been expressed about the use of these organizations – particularly registered charities – it is important to remember that charitable status is not necessarily important to those committed to raising and moving funds. Many terrorist acts cost so little to carry out that setting up a charity to raise funds is not necessary. Those committed to financing terrorism are not likely to be deterred from providing funds simply because the recipient cannot issue tax receipts to them. Furthermore, the process of obtaining and maintaining charitable status involves being monitored by the Charities Directorate – additional attention that those interested in financing terrorism certainly do not want.

That said, there are other reasons for groups that want to finance terrorism to seek charitable or not-for-profit status. Many of these reasons were identified in Chapter VI. They include the frequently cash-intensive nature of transactions involving such organizations, making it more difficult for the authorities to identify TF, and the ability of such organizations to transfer funds to other countries with relative ease.

Federal and provincial governments must recognize their shared responsibility for the regulation of charities. Constitutional obstacles preclude a regulated system similar to that of the England and Wales Charity Commission. The ideal would be federal-provincial agreements on the monitoring and regulation of charities. If there is no agreement, federal and provincial governments must individually assume their responsibilities to deal with the possible use of charities for TF. For example, the federal government could examine which parts of the UK Charities Commission model could be implemented without provincial involvement.

The following several sections provide specific suggestions and recommendations to reduce the likelihood that charities and NPOs will be used to finance terrorism.

7.8.1 Sharing Intelligence

The denial of charitable status should be one stage in a whole-of-government effort that could, in appropriate cases, see further investigation of a charity by CSIS or the RCMP.

The CRA should continue to work closely with other agencies to identify charities that may be involved in TF. The CRA should be included in the overall network of agencies that are concerned with TF, and it should have access to appropriate information from domestic and foreign agencies. It would be almost impossible for any regulator to find the indicia of TF by sifting through information about all charities. Intelligence must be shared to help identify targets. This will require the RCMP, and especially CSIS, to work closely with the CRA and to provide it with the best possible intelligence. Greater effort should be made to share general information about TF that is of common interest to all these agencies. For example, CRA is not a member of ITAC, while FINTRAC is. CRA could benefit from such membership.

The CRA has limited resources to devote to audits of charities. It is essential that the CRA receive the best intelligence possible from all sources about charities that may be involved in financing terrorism to make optimal use of its audit resources.

Largely because of changes introduced by Bill C-25 to the *PCMLTFA* late in 2006, the CRA can now share more extensive information with other agencies. However, it took considerable time for the changes allowing this increased sharing to come into effect. The impetus for change occurred on September 11, 2001. Bill C-25 was enacted only in 2006 and came into effect in stages. Its provisions were fully in force only in December 2008. Such delays are unacceptable.

As well, the CRA, RCMP, CSIS and FINTRAC would all benefit if reporting on the value of the exchanged information were made mandatory, or at least encouraged. Such follow-up would also help the National Security Advisor to review the effectiveness of Canada's efforts to combat TF, including how well the CRA, FINTRAC, CSIS and the RCMP are working together.

A charitable organization whose registration is revoked for terrorism or TF reasons should be reported to the appropriate agencies for further investigation. Revocation of charitable status should be only part of a response that includes continued intelligence operations and, possibly, law enforcement investigations.

7.8.2 Intermediate Sanctions

It is particularly helpful for the CRA to make full use of the "intermediate sanctions" now available to it (for example, monetary penalties or the suspension of a charity's power to issue tax receipts for donations) to encourage charities to "clean house" by removing directors and trustees who may be involved in terrorist activities. Creative and robust use of intermediate sanctions can indirectly achieve some of the goals that are obtained in the United Kingdom through a charity commission.

7.8.3 Statistics

It would be helpful to have statistics indicating the role that terrorism or TF issues play in decisions to revoke charitable registrations or to use intermediate sanctions. Such statistics would help determine the extent to which the Charities Directorate contributes to government-wide efforts to stop TF. Such information could also assist other agencies such as CSIS, RCMP, FINTRAC and the NSA. It would also be of value to have statistics, to the extent that these can be assembled, on the extent of TF through charities.

7.8.4 The *Charities Registration (Security Information) Act* Process

The question arises whether the *Charities Registration (Security Information) Act*[90] (*CRSIA*) process is necessary if it is not being used.

Canada has a legitimate interest in protecting information that could endanger national security or endanger persons if it were disclosed. The *CRSIA* allows secret intelligence to be presented to a judge while only a summary containing non-sensitive information is disclosed to the charity or person challenging the CRA. The *CRSIA* has a potential value in deterring TF and also underlines Canada's commitment to stopping the subversion of charitable status through TF. For these reasons, it should be retained.

Still, the CRA appears to have managed without invoking the *CRSIA* process. Although the *CRSIA* was created to allow the CRA to revoke or deny registration on the basis of classified information, organizations that support terrorism will likely also fail to meet other requirements for charitable registration and not obtain or lose charitable status for those reasons.

It is difficult to fault the government for not using the untested procedures of the *CRSIA* if it is possible to deny or remove charitable status on other grounds. Nevertheless, to demonstrate its ability to refuse to register charities without making use of the *CRSIA*, the CRA should be more transparent and keep better statistics about when concerns about TF have led to denial of charitable status.

Chapter VI described the debate about whether the *CRSIA* should contain a due diligence defence. The need for such a defence is difficult to assess at this time because no *CRSIA* certificate proceedings have yet occurred. However, the loss or denial of charitable status is not a consequence of the same magnitude as the prospect, for example, of detention or punishment for an individual. This may make the lack of a due diligence requirement in the *CRSIA* more defensible.

The lack of experience with the *CRSIA* also makes it difficult to assess other possible deficiencies, such as enabling the government to rely on secret evidence and the fact that the *CRSIA* does not on its face contemplate allowing security-cleared special advocates to see and challenge secret evidence. It

90 S.C. 2001, c. 41, s. 113.

would be helpful to have a track record of *CRSIA* certificate proceedings. Claims about deficiencies in the *CRSIA* could then be examined as real, rather than speculative, issues.

7.8.5 Not-for-profit Organizations

A serious obstacle hinders the fight against TF in Canada. Each province can control and regulate NPOs under section 92 of the *Constitution Act*, *1867*.[91] Rules vary among the provinces. In fact, there are few reporting rules in any of the provinces. As the organizations are non-profit, the CRA is normally not involved. The problem lies in the ability of NPOs to operate in a clandestine manner and to ignore what rules there are, making it almost impossible to identify TF within them.

There is obviously much to be gained by federal and provincial governments harmonizing their treatment of NPOs. The federal government should take the lead in bringing together provincial authorities to coordinate responses to the abuse of charitable or not-for-profit organizations. It is especially important that regulators be provided with the information and assistance they need to identify the abuse of charities and not-for-profit organizations for TF.

Organizations should also be prohibited from using the description "charity," "non-profit organization," "not-for-profit organization," or similar descriptions, unless registered as such with the CRA or the appropriate provincial agency.

7.8.6 Publicity

The CRA should, when practicable, publish reasons for denying or revoking the registration of charities or NPOs and for applying intermediate sanctions to charities. Indeed, publicity will be an important factor if these sanctions are to influence charities and NPOs to reform themselves and to alert potential donors that a given organization supports terrorism. The Commission acknowledges the tradition of keeping income tax information confidential. These concerns are laudable, but the traditional protection of tax information from disclosure needs to be reconsidered in light of concerns about terrorism.

7.8.7 Avoiding Harm to Legitimate Charities and NPOs

It is essential that measures to defeat the use of charities or NPOs for TF not unnecessarily impede the valuable activities of legitimate organizations. Any new guidelines or best practices that the CRA may contemplate to help it address TF in the charitable sector should be developed in close cooperation with the charitable sector. The work of honest charities should not be hindered because of unrealistic guidelines or best practices.

---

91 (U.K.), 30 & 31 Vict., c. 3, reprinted in R.S.C. 1985, App. II, No. 5.

7.9 International Aspects of Terrorist Financing

Funds can move across multiple jurisdictions and finance terrorists throughout the world. A 2007 Department of Finance Memorandum of Evidence on Terrorist Financing described the challenge that this presents:

> Because of the global reach of terrorist networks, the increasing integration of financial systems and the speed and facility with which money can be moved between jurisdictions, tracing and intercepting terrorist funding represents a major transnational challenge that is most effectively addressed through complementary international and domestic actions.[92]

FINTRAC reported that Electronic Fund Transfer Reports, provided by reporting entities, were contained in 93 per cent of its disclosures to law enforcement and security intelligence agencies in matters relating to TF or threats to the security of Canada.[93] The international nature of terrorism and TF makes the resulting investigations more complex and much lengthier than if the transactions involved were domestic only.[94] Superintendent Reynolds testified:

> [B]y the very nature of terrorism it's international. And the fact that it moves across borders and into areas where perhaps the infrastructure is broken down, it makes it extremely difficult to follow the paper trail as far as the cash – the movement of cash, the movement or procurement of materials.[95]

There is a need to integrate TF into the work of agencies including CSIS, DND and DFAIT. The Integrated Threat Assessment Centre (ITAC) situated in CSIS already provides some integration in terms of threat assessments.

Canada's cryptologic agency, the Communications Security Establishment (CSE), also needs to be integrated more effectively into anti-TF efforts. The NSA should, in his or her expanded role, ensure that CSE makes appropriate and necessary disclosures to FINTRAC. Such intelligence could help FINTRAC perform its analyses and make more useful disclosures of designated information to the RCMP, CSIS and other agencies.

---

92 Exhibit P-227, Tab 3: Department of Finance Memorandum of Evidence on Terrorist Financing, February 28, 2007, para. 2.6. The FINTRAC *Report on Plans and Priorities for the years 2007-2008 to 2009-2010* expresses a similar view at p. 7, online: Treasury Board of Canada Secretariat <http://www.tbs-sct.gc.ca/rpp/0708/fintrac-canafe/fintrac-canafe-eng.pdf> (accessed January 26, 2009).

93 Exhibit P-438: FINTRAC Response to Supplementary Questions of the Commission, January 9, 2008, Question 3(b).

94 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6820.

95 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6820.

7.9.1 Difficulties in Securing International Cooperation

The definition of terrorism varies from jurisdiction to jurisdiction. This in turn leads to inconsistencies in deciding what constitutes TF. In addition, anti-TF rules and programs are not identical, or interpreted identically, in all countries. This poses major challenges for attempts to secure cooperation from other countries. Keith Morrill of DFAIT highlighted the difficulties through a fictitious example:

> If Canada has an offence of terrorist financing, and we have listed the Faroffistan Widows and Orphans Fund because we know that that is being used to fund terrorists in the mythical country of Faroffistan, and the money moves from a bank account in Canada to a bank account in France, and France does not regard the Faroffistan Widows and Orphans Fund as being linked to a terrorist group, that greatly limits our capacity to have criminal law enforcement cooperation because what is to us an activity which seems to be linked to an offence is to France … simply a legitimate transfer of funds.[96]

A foreign country is not necessarily a "weak link" country. In fact, it could be a well-regulated country with an otherwise adequate anti-TF program, but the country may differ with Canada about whether a person or entity should be considered a terrorist or whether a given act constitutes terrorism.

In addition, as Superintendent Reynolds testified, it is "…[n]ot that it is difficult to get cooperation, but you're now into different judicial systems, different understanding, the priority of the organizations that you're dealing with changes, yours may not be the priority, so it slows down the process."[97]

Cooperation among agencies in Canada is often heavily regulated (such as through FINTRAC's and CRA's disclosure rules). When FINTRAC makes arrangements for international cooperation in TF, it faces even more hurdles than it encounters when cooperating with agencies in Canada. For example, FINTRAC can share information with financial intelligence units abroad, but only under the same conditions that it may share information with law enforcement agencies in Canada, and only if FINTRAC has a memorandum of understanding with the foreign FIU.[98] Furthermore, the FIU receiving information from FINTRAC must have specific provisions for the protection of privacy interests.[99] This process for sharing information is both formal and lengthy.

---

96 Testimony of Keith Morrill, vol. 54, September 28, 2007, p. 6703.
97 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6843.
98 *PCMLTFA*, s. 56.1.
99 Second FINTRAC Response to Supplementary Questions of the Commission, Question 6(b).

Professor Rudner commented on this in his paper for the Commission:

> Whereas the Egmont Group and other international organizations generally encourage and promote the sharing of financial intelligence, actual flows and exchanges of information between and among FIUs seem to be constrained by national privacy concerns, perhaps even more so than in other areas of security intelligence or law enforcement. In practice, national FIUs have tended to restrict the sharing of financial intelligence to foreign units and countries with whom bilateral agreements have been reached specifying the terms of such exchanges.[100]

As the 2008 FATF Mutual Evaluation of Canada noted, the mutual legal assistance (MLA) process is laborious.[101] The Commission did not receive evidence on this point, but it is clear that some countries, even Western countries, do not cooperate as fully with each other on TF matters as is warranted. While the FIU process described by Professor Rudner appears to function relatively well, information does not flow as freely as it should. As the passage of time dims the memory of 9/11, London and Madrid, Western countries will likely see even less urgency in cooperating on TF matters – unless there is a new major act of terrorism.[102]

7.9.2 The Problem of "Weak Links"

Adding to the difficulties in securing international cooperation is the reality that some countries are notoriously weak links in the global anti-TF system. For example, the FATF has warned about financial dealings in Iran and Uzbekistan because of heightened money laundering and TF risks.[103]

Countries that are considered state sponsors of terrorism are obviously the most problematic. Other countries, without being "official" state sponsors, are sometimes seen as sources, even if unwitting, for TF.

When funds leave Canada, they become more difficult to track. That difficulty increases if the funds enter a country deficient in financial controls and law enforcement – for example, Afghanistan or Sudan. "Weak links" in the global

---

100 Rudner Article on Using Financial Intelligence, p. 49.

101 See 2008 FATF Mutual Evaluation of Canada, paras. 1477-1502. The report mentions that, on TF matters, Canada received 14 requests for assistance (during 2001-2006), with 8 being executed, 2 withdrawn and 4 being active. By way of comparison, 143 requests for assistance had been made on ML matters: see para. 1522.

102 A recent U.S. National Intelligence Estimate noted the likelihood that international cooperation will wane as 9/11 grows more distant: see Michael Jacobson, "Extremism's Deep Pockets: The growing challenge of fighting terrorist financing," p. 22, online: The Politic <http://thepolitic.org/content/view/91> (accessed June 3, 2009).

103 See FATF Chairman's Summary, London Plenary, June 18-20, June 20, 2008, online: Financial Action Task Force <http://www.fatf-gafi.org/dataoecd/50/1/40879782.pdf> (accessed January 29, 2009).

anti-TF system are valuable for terrorists. As American academic Philip Bobbitt wrote, "…[t]he system of global terrorist financing depends upon the inability of states to compel other states to disclose financial holdings and transfers."[104] Some jurisdictions, including the UK, have attempted to help strengthen the anti-TF system in "weak link" countries.[105]

7.9.3 Trade

Professor Passas identified poor surveillance of trade transactions as an important deficiency in countering TF in most countries, including Canada:

> Currently, there are serious gaps in the way government authorities deal with trade transactions. Incomplete, erroneous or illegal documentation can be found through routine review of forms filed with Customs agencies. There is plenty of room for improving enforcement action and attempts at rendering the transactions accurate and transparent. Mistakes and mis-statements concerning country of origin, ultimate consignee, counter-parties or value abound and reveal significant opportunities for misconduct, including terrorist finance. In other instances, trade diversion practices and mis-invoicing cannot be easily detected as the paperwork in such cases is not forged or fake but the content of the documents is wrong. Very high values can be moved literally under the nose of even quite careful inspectors. Such infractions may only be detected through inside information or in-depth checks and inquiries, which cannot be routinely instituted.
>
> Such vulnerabilities were found in the trade of precious stones and metals, electronics, medicine, cosmetics, textiles, foodstuff, tobacco, car or bicycle parts, etc.. In short, trade is currently not transparent and represents a serious threat to all efforts countering money laundering, terrorist finance or other financial crime.
>
> Given that financial and trade transactions are not jointly monitored and matched, irregularities, suspicious transactions and blatant abuses may be going undetected. Research has shown that irregularities amounting to billions of US dollars go undetected and uninvestigated. In the light of the large volumes of trade conducted daily, the risk of financing serious crime includes activities not only related to more expensive forms of terrorism as well as proliferation and weapons of mass destruction.[106]

---

104 Philip Bobbitt, *Terror and Consent: The Wars for the Twenty-First Century* (New York: Knopf, 2008), p. 455.
105 Testimony of Paul Newham, vol. 58, October 4, 2007, p. 7244.
106 Passas Report on Terrorism Financing, pp. 83-84 [references omitted].

The FATF has discussed trade-based money laundering in two papers.[107] Although the FATF has made no recommendations about trade to date, some are said to be forthcoming. The FATF describes the problem with trade as follows:

> The Financial Action Task Force (FATF) has recognised misuse of the trade system as one of the main methods by which criminal organisations and terrorist financiers move money for the purpose of disguising its origins and integrating it into the formal economy. As the anti-money laundering (AML) and counter-terrorist financing (CFT) standards that have been applied to other money laundering techniques have become increasingly effective, such abuse of the trade system is expected to become increasingly attractive. However, currently, many customs agencies, law enforcement agencies, financial intelligence units (FIU), tax authorities and banking supervisors (i.e. competent authorities) appear less capable of identifying and combating trade-based money laundering than they are in dealing with other forms of money laundering and terrorist financing.[108]

7.9.4 Civil Redress for Terrorist Acts Committed Outside Canada

Several parties and intervenors forcefully suggested that the Commission support passage of a Private Senator Public Bill that was introduced to facilitate civil lawsuits against terrorists and their sponsors. Professor Ed Morgan of the Faculty of Law at the University of Toronto described civil remedies as "…one of the most effective and targeted means of curtailing the financing of terrorism that the legal system can endorse."[109] The Bill was S-225, *An Act to amend the State Immunity Act and the Criminal Code (deterring terrorism by providing a civil right of action against perpetrators and sponsors of terrorism*).[110] Proponents of civil redress argued that such lawsuits are a good vehicle for drying up terrorist funds. Lawsuits would thus become a component of the fight against TF.

At present, Canadian law allows civil suits against foreign states for a breach of contract or a personal injury that happened in Canada, but this does not include remedies for sponsoring acts of terrorism which occur abroad and injure or kill Canadians. The summary that accompanied the first reading version of Bill S-225, which died on the Order Paper when Parliament was prorogued for the

107 "Trade Based Money Laundering," June 23, 2006, online: Financial Action Task Force <http://www.fatf-gafi.org/dataoecd/60/25/37038272.pdf> (accessed January 24, 2009); "Best Practices Paper on Trade Based Money Laundering," June 20, 2008, online: Financial Action Task Force <http://www.fatf-gafi.org/dataoecd/9/28/40936081.pdf> (accessed January 24, 2009) [FATF Best Practices Paper on Trade Based Money Laundering].

108 FATF Best Practices Paper on Trade Based Money Laundering, para. 1. See also *FATF Annual Report 2007-2008*, June 30, 2008, online: Financial Action Task Force <http://www.fatf-gafi.org/dataoecd/58/0/41141361.pdf> (accessed January 27, 2009).

109 Testimony of Ed Morgan, vol. 55, October 1, 2007, p. 6897.

110 2nd Sess., 39th Parl., 2007. Several similar bills have been introduced over the years.

October 2008 election, described the purpose of the Bill as follows:

> This enactment amends the *State Immunity Act* to prevent a foreign state from claiming immunity from the jurisdiction of Canadian courts in respect of proceedings that relate to terrorist conduct engaged in by the foreign state.
>
> It also amends the *Criminal Code* to provide victims who suffer loss or damage as a result of conduct that is contrary to Part II.1 of the *Criminal Code* (Terrorism) with a civil remedy against the person who engaged in the terrorist-related conduct.[111]

The main provisions of Bill S-225 can be summarized as follows:

- A foreign state is not immune from the jurisdiction of a court in any proceedings that relate to terrorist conduct engaged in by the foreign state on or after January 1, 1985;
- The Minister of Finance and the Minister of Foreign Affairs must assist any judgment creditor to identify, locate and execute against the property of the foreign state or certain other entities; and
- Any person who has suffered loss or damage on or after January 1, 1985, as a result of conduct by any person, including a foreign state, that constitutes an offence set out in Part II.1 of the *Criminal Code* (dealing with terrorism) can, in any court of competent jurisdiction, sue the person or foreign state.[112]

The first provision mentioned above would have allowed victims of the Air India tragedy to sue in Canadian courts any foreign actor that may have contributed to the tragedy. Professor Morgan testified that the clause was meant to apply to state sponsors of terrorism. If the Bill had been enacted, it would have allowed some degree of enforcement by private individuals of laws against terrorism and TF.[113]

Bill S-225 would have allowed a victim of terrorism to sue a bank that may have provided financial services to terrorists. What is not clear is how, if the bank was not convicted criminally, the victim would be able to demonstrate on a balance of probabilities that the bank had contravened the *Criminal Code*. The courts would also have to determine the validity of the Bill's attempt to give *Criminal Code* provisions a retroactive effect, if only for the limited purposes of civil, not criminal liability.

---

111 Summary notes of Bill S-225, online: Parliament of Canada <http://www2.parl.gc.ca/content/Senate/Bills/392/public/S-225/S-225_1/S225-e.htm> (accessed January 24, 2009).

112 This includes the *Criminal Code* anti-TF provisions. Morgan stated that: "That proposal is, more or less, modeled on section 36 of the *Competition Act* which, as you know, gives a civil cause of action to anyone who has suffered damages as a result of a defendant engaging in any of the quasi-criminal provisions of the *Competition Act*": Testimony of Ed Morgan, vol. 55, October 1, 2007, p. 6902.

113 Testimony of Ed Morgan, vol. 55, October 1, 2007, p. 6903.

As mentioned earlier, several parties and intervenors made submissions about civil liability, most notably the Canadian Jewish Congress and the Canadian Coalition Against Terror (C-CAT).[114] C-CAT maintained that the Canadian legal framework does not provide adequate constraints to combat TF and that the campaign against TF requires innovative strategies such as those proposed in Bill S-225.[115] According to C-CAT, Bill S-225 would "…(i) deter future acts of violence (by bankrupting or financially impairing the terrorist infrastructure); (ii) hold the wrongdoers responsible (even where the criminal system has failed); (iii) compensate victims; and (iv) enable terrorist assets to be located and seized."[116] C-CAT cited American examples to support its position.

As noted above, Bill S-225 died with the calling of the 2008 federal election. Despite the failure of this Bill to proceed, Canadian citizens filed a civil lawsuit in Quebec Superior Court in July 2008 against the Lebanese Canadian Bank, whose sole foreign representative office was in Montreal.[117] The claim alleged that the plaintiffs were injured while in Israel in 2006 by rockets launched by Hezbollah. The plaintiffs also alleged that the bank provided extensive financial and banking services to Hezbollah. The total compensation sought was $6.15 million. In August 2008, the matter was adjourned indefinitely. While this lawsuit did not involve a foreign state, it did represent a new way of fighting TF, as recommended by C-CAT, and the progress of this and future cases merits watching.

7.10 The Reality Facing Efforts to Suppress Terrorist Financing

Donna Walsh, Director of the Review and Analysis Division in the Charities Directorate of the CRA, testified that "…countering terrorist financing is a complex issue. No one strategy or measure will stop it."[118] In his paper, Professor Passas called measures to counter TF "necessary and vital," but also called for "realistic expectations and targets."[119]

An approach involving shared intelligence provides the best prospect for success against TF, especially in an environment of limited resources. Agencies such as the RCMP and CSIS will play a critical role in providing information to FINTRAC and the CRA. In TF matters, the RCMP and, in particular, CSIS are best suited to adapt quickly, observe the evolution of events, identify the important players and understand the variables involved. For example, an individual's deposit of a small amount of money might not raise a bank's suspicion. As a result, information about the transaction would not be reported to FINTRAC. However, a front-line intelligence agent who knew about the individual's links to terrorism might have suspicions about the transaction. Furthermore, the agent

---

114 Both also made submissions to the Standing Senate Committee.
115 Final Submissions by the Canadian Coalition Against Terror (C-CAT) to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, January 31, 2008 [C-CAT Final Submissions].
116 C-CAT Final Submissions, p. 7.
117 *Yefet, Sappir, Shalmoni v. Lebanese Canadian Bank* (Qc. Sup. Ct.), Docket No. 500-17-043962-086.
118 Testimony of Donna Walsh, vol. 57, October 3, 2007, p. 7109.
119 Passas Report on Terrorism Financing, p. 106.

might understand how a group raises and moves money, and the transaction might follow that pattern. In short, the agent might understand the subtleties of TF that would escape detection by a formal and mechanical reporting system.

The entire AML/ATF Initiative must shift from relying primarily on formal reporting systems and instead ensure adequate resources for law enforcement and security intelligence agencies to work together effectively.[120] As mentioned above, there is also a need to invest more in educating private sector entities to help them identify suspicious transactions and report them to FINTRAC.

7.11 Ways to Develop "Human Capital" for Anti-Terrorist Financing Efforts

An effective approach to TF will require both an increase in the sharing of information and increased investment in human capital. One way to achieve the latter goal is to facilitate increased secondments among agencies working on TF issues. This is now done for the Integrated Threat Assessment Centre and is suggested in Volume Three for the office of the National Security Advisor. FINTRAC already has a secondee from the RCMP Proceeds of Crime Unit,[121] and this program should be expanded to include secondees from agencies involved in counterterrorism. Secondment opportunities allow limited resources to be shared. Moreover, they allow junior and senior officials to develop a whole-of-government perspective on TF issues and improve cooperation among agencies.

Employees seconded to one agency would face the same statutory restrictions on access to their home agency database as any other employee of the agency to which they are seconded. In other words, the agency to which a FINTRAC employee is seconded (for example, the RCMP) would not receive greater access to FINTRAC information simply because a FINTRAC employee is seconded to that agency.

The response of one senior official in charge of the CSIS anti-TF program to a question about the magnitude of the problem illustrates the gaps in understanding: "I haven't been able to sit back and do a proper analysis like that. So I really can't comment on that. I know we're very busy in my office and there is no lack of files."[122] The official cannot be faulted if the resources were not available for such an analysis.

Professor Passas expressed concern about the lack of reliable information about TF:

> The lack of confirmed and validated information about terrorism finance limits the effectiveness of [anti-TF] efforts.

120 This view is supported by Passas: see Passas Report on Terrorism Financing, pp. 95-98.
121 Exhibit P-442: Summary of Meeting between Commission Counsel and FINTRAC, April 10, 2008, p. 3.
122 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6913.

> Canadian authorities have stressed the integration of the various agencies involved in counter-terrorism. This may be the case in Canada, but not everywhere else. Limited intelligence distribution to different domestic agencies and overseas counterparts is a long standing problem that could be resolved through the use of a terrorism finance database supported by open source information.[123]

FINTRAC officials were asked whether a database existed on matters such as TF cases, prosecutions and media reports worldwide, and whether, if one did not exist, such a database would be helpful. They responded as follows:

> There are numerous databases that contain valuable information on terrorist groups and incidents that FINTRAC consults as part of its analytical work. To FINTRAC's knowledge there is no comprehensive database which includes all relevant TF information that would be of value to FINTRAC exercising its mandate. Any database that contained reliable information on all aspects of every terrorist activity financing case would be very useful.[124]

The type of database on TF cases proposed by Professor Passas would provide a relatively inexpensive tool to help government agencies and private sector entities improve their understanding of TF and related issues.

7.12 The Kanishka Centre(s) for Better Understanding and Preventing Terrorism

There is a need to develop the next generation of security professionals in government and to provide a means for existing professionals to enrich their understanding of terrorism and TF. Many of the recommendations made by the Commission flow from the realization that much work needs to be done if Canada is to match international best practices regarding the relationship between intelligence and evidence, terrorism prosecutions, witness protection, TF and aviation security. There is a need for continuing study of these issues in light of both rapidly changing circumstances in the world and Canada's own experience. Canada cannot afford to wait until the next terrorism tragedy occurs and another public inquiry is appointed to study the adequacy of its counterterrorism measures.

A number of researchers who prepared reports for this Commission commented on the lack of dedicated governmental support for research on terrorism issues. They spoke of the adverse effects that this lack of funding has had on public understanding of the challenges of terrorism and on the availability of trained

123 Passas Report on Terrorism Financing, p.92.
124 Second FINTRAC Response to Supplementary Questions of the Commission, Question 7.

people to do vital counterterrorism work. For example, Professor Rudner argued that, despite increased interest in terrorism among the public and students after 9/11, the capacity of Canadian institutions of higher education to exercise knowledge leadership remained "grossly inadequate":

> Very few university courses or programs dealing with intelligence and/or National Security studies are currently on offer in Canada….[R]esearch remains grievously constrained by a dire lack of financial support, even from official funding councils, coupled with acute staff shortages. It is indicative of the absence of priority that out of more than 1,800 Canada Research Chairs established in Canadian universities since 2000….not a single one was dedicated to Intelligence Studies. Not one. Just one Canada Research Chair relating to terrorism studies was recently established at Université Laval in Quebec City. Compared to the rather more dynamic situation in American, Australian and British universities and research institutions, Canada's educational and research capacity in these fields of vital national security concern remains woefully understrength.[125]

Professor Wesley Wark of the Munk Centre for International Studies at the University of Toronto stressed the need "…to open up both our historical and our present national security activities to greater and more informed public scrutiny"[126] in order to learn from past mistakes and develop a baseline for determining success.

Professor Kent Roach of the Faculty of Law at the University of Toronto noted that "…Canadian research into terrorism related issues has generally been relatively sparse. There is no dedicated governmental funding for research related to the study of terrorism and optimal counter-terrorism measures as there is in other fields such as military studies."[127]

In its final submissions, the Air India Victims Families Association suggested that "…[t]he federal government should provide funding for the establishment of an academic Centre of Excellence to be known as The Kanishka Centre as a living memorial to the victims and families of the bombing of Air India Flight 182."[128] The Association contemplated a "multi-disciplinary Centre within a University setting" that could "bring together expertise and discourse from policy, operational, and academic communities to address the study of terrorism

---

125 Martin Rudner, "Building Canada's Counter-Terrorism Capacity: A Proactive All-of-Government Approach to Intelligence-Led Counter-Terrorism" in Vol. 1 of Research Studies: Threat Assessment RCMP/CSIS Co-operation, pp. 141-142.

126 Wesley Wark, "The Intelligence-Law Enforcement Nexus" in Vol. 1 of Research Studies: Threat Assessment RCMP/CSIS Co-operation, p. 181.

127 Kent Roach, "Introduction" in Vol. 1 of Research Studies: Threat Assessment RCMP/CSIS Co-operation, p. 8.

128 AIVFA Final Written Submission, p. 98.

prevention and its related fields, with the intent of working with and assisting governments in this endeavour."[129]

Careful consideration could usefully be given to setting up such a research organization. A precedent for such a research program exists in the long-running Security and Defence Forum (SDF) sponsored by the Department of National Defence. The Department funds 12 "centres of expertise" in Canadian universities, with grants of between $100,000 and $165,000 per centre per year, as well as a Chair of Defence Management Studies.

Creating a research organization would respond to some of the problems that the Commission has identified, including inadequate public understanding of the dangers of terrorism. Exchanges between governments and such a research organization could enrich human capital on terrorism issues both within and outside of government.

7.13 Conclusion

Canada's anti-TF program is still relatively young.[130] The *Anti-terrorism Act* received Royal Assent in late 2001, and anti-TF operations began shortly after. The provisions governing the anti-TF program during its first few years limited its potential for success, but Bill C-25, which came into force in stages beginning in late 2006, enhanced that potential. However, it is still too early to tell if the Bill C-25 changes will increase the effectiveness of anti-TF measures.

The time may have come to use distinct legislative schemes to deal with money laundering and TF. By pursuing the fight against TF on the basis of the current money laundering model, there is a danger that TF transactions will be lost among the much larger sums involved in money laundering and organized crime. There is a danger as well that private sector reporting entities might view their anti-TF work almost as an afterthought, less important than their work on money laundering.

At several points, this chapter discussed the need for better sharing of information among agencies involved in countering TF. Such an approach is necessary because of the difficulties that FINTRAC would face if it were to rely solely on examining the millions of financial transaction reports that it receives yearly. The CRA processes thousands of applications for charitable status each year and faces a similar problem of pinpointing suspicious activity. FINTRAC and the CRA both require good intelligence to help them focus their limited resources. Hence, the RCMP, CSIS and other agencies should continue to work closely with FINTRAC and the CRA to provide them with the best possible intelligence about TF.

---

129 AIVFA Final Written Submission, p. 98.

130 Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6765; Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6967.

FINTRAC and the CRA also need to be better integrated into the broader intelligence community through measures such as secondments and joint training. They need to see themselves as a vital part of an intelligence cycle that may, in some cases, contribute to successful prosecutions and may, in other cases, facilitate preventive or disruptive measures.