A New Review Mechanism for the RCMP's National Security Activities

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

Cat. No: CP32-88/2-2006E
ISBN 0-660-19666-2

Available through your local bookseller or through
Publishing and Depository Services
Public Works and Government Services Canada
Ottawa, Ontario
KIA OS5

Telephone: (613) 941-5995
Orders only: 1 800 635-7943
Fax: (613) 954-5779 or 1 800 565-7757
Internet: http://publications.gc.ca

Printed by: Gilmore Print Group

Ce document est également publié en français sous le titre
Un nouveau mécanisme d'examen des activités de la GRC en matière de sécurité nationale

www.ararcommission.ca

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

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

The Honourable Dennis O'Connor
Commissioner

L'honorable Dennis O'Connor
Commissaire

December 2006

To Her Excellency
The Governor General in Council

May it please Your Excellency:

Pursuant to an Order in Council dated February 5, 2004, I respectfully submit my report on a review mechanism for the RCMP's national security activities.

Dennis R. O'Connor

PO Box / CP 507, Station B / Succursale B
Ottawa, Canada K1P 5P6

613 996-4741 Fax / télécopieur *613* 992-2366

www.ararcommission.ca / www.commissionarar.ca

Contents

I
Introduction and Overview

1.
INTRODUCTION

The Order in Council establishing this Inquiry provided a two-part mandate. The first part, called the Factual Inquiry, directed that I investigate and report on the actions of Canadian officials in relation to what happened to Maher Arar. I have already delivered my report on the Factual Inquiry to the government.

The second part, the Policy Review, requires that I make recommendations for an independent, arm's-length review mechanism with respect to the RCMP's national security activities. This is my report on the Policy Review.

2.
ORGANIZATION OF THE REPORT

The following six chapters of this Report are descriptive in nature, setting out the results of the Inquiry's extensive research and information-gathering process. After an historical survey of the evolution of Canada's national security activities (Chapter II), I examine the major legislative changes enacted following the terrorist attacks of September 11, 2001 (Chapter III). I then review the RCMP's current national security activities (Chapter IV) as well as those of the other Canadian national security actors (Chapter V). Finally, I examine the Canadian (Chapter VI) and international (Chapter VII) experience in review of national security activities.

The information in these chapters provides the context for my subsequent analysis of the unique features of national security activities that call for enhanced review (Chapter VIII); the objectives of the review process (Chapter IX); and my conclusion that existing review mechanisms for the RCMP's national security activities are not adequate (Chapter X). In Chapter XI, I set out my detailed recommendations and rationales for a new single review body for the RCMP's

national security activities. I also recommend independent review of five other departments and agencies, and mechanisms to coordinate the work of all national security review bodies. Finally, in Chapter XII, I describe the process followed for the Policy Review.[1]

3. OVERVIEW OF MY CONCLUSIONS AND RECOMMENDATIONS

I conclude that existing accountability and review mechanisms for the RCMP's national security activities are not adequate in large part because of the evolution and increased importance of that national security role. Among the more significant changes have been enhanced information sharing, new legal powers and responsibilities, and increased integration in national security policing. I have also been influenced by the Canadian and international experience with both policing and security intelligence review, and the inability of a complaint-based approach to provide a firm foundation for ensuring that the often secret national security activities respect the law and rights and freedoms. Finally, I conclude that the difficulties that the CPC has encountered in obtaining access to information from the RCMP can undermine the effectiveness of its review function and public confidence in the effectiveness of the review.

In light of these conclusions, my main recommendations are as follows.

Enhanced Powers — In order to provide effective review, the powers of the new review mechanism for the national security activities of the RCMP should be enhanced in two significant respects. First, in addition to the power to investigate and report on complaints, the review mechanism must have the authority to conduct self-initiated reviews, similar to those currently conducted by the Security Intelligence Review Committee (SIRC) in respect of CSIS operations, in order to review the RCMP's national security activities for compliance with laws, policies, ministerial directives and international obligations, as well as for standards of propriety that are expected in Canadian society.

The need for self-initiated reviews stems from the fact that most of the RCMP's national security activities are conducted in secret and receive little, if any, judicial scrutiny, yet have the potential to significantly affect individual rights and freedoms. It is vital that those within the Force involved in national security activities be held accountable for such activities by a body that is independent of the RCMP and government. Providing the review mechanism with the authority to conduct self-initiated systemic reviews will be a major step towards ensuring appropriate and effective review of those activities and engendering public confidence and trust in the review process.

The second major enhancement involves giving the review mechanism extensive investigative powers, similar to those applicable to public inquiries under the *Inquiries Act*, to allow it to obtain all of the information and evidence necessary to conduct thorough and complete reviews and complaint investigations. These powers should allow the review mechanism to decide what information is necessary to fulfill its mandate and to subpoena documents and compel testimony from any federal, provincial, municipal or private sector person or entity.

The RCMP's national security investigations are increasingly integrated with the activities of other federal, provincial and municipal agencies. Integration is desirable and should be encouraged. However, it is critical that the review mechanism have access to all information that may be relevant to an investigation or a review, wherever that information may be found. When collecting information, the review mechanism must not be hampered by jurisdictional boundaries. It must be able to follow the trail wherever it leads, to ensure full and effective investigation or review of the RCMP's national security activities.

Independent Complaints and National Security Review Agency for the RCMP — The most effective review of the RCMP's national security activities will be achieved by a review mechanism that has jurisdiction to review all of the RCMP's activities, including those related to national security. That mechanism should be located within a restructured Commission for Public Complaints Against the RCMP (CPC) with the significantly enhanced powers that I recommend in this report and a new name, the Independent Complaints and National Security Review Agency for the RCMP (ICRA), to reflect its broader mandate.

In my view, there are significant advantages to having a single review agency for all of the RCMP's activities. The RCMP is a law enforcement agency. Reviewing law enforcement activities requires special expertise and experience that can best be developed and maintained by a review body that specializes in the review of law enforcement activities. Broad exposure to all of the RCMP's activities will enhance the review body's expertise.

The RCMP's national security activities make up a relatively small proportion of its overall workload. There could be serious risks in entrusting review of national security activities to one body and review of the balance of the RCMP's activities to another. To start, the different bodies might apply different and possibly inconsistent standards to the same or similar law enforcement activities. Moreover, separating what is properly considered a national security activity from other activities conducted by the RCMP could in many circumstances be difficult, and the existence of separate review bodies could lead to disagreements and jurisdictional disputes.

In making this recommendation, I recognize that, in the past, there have been tensions between the RCMP and CPC that may have impeded effective review. However, I am satisfied that, if properly structured in the manner I suggest below and given the enhanced powers I recommend, ICRA can provide the most effective review of the RCMP's national security activities.

Mandate and Powers — In Chapter XI, I make detailed recommendations regarding ICRA's mandate for the review of the RCMP's national security activities. Specifically, I recommend that ICRA conduct self-initiated reviews to ensure that the RCMP's national security activities fall within its law enforcement mandate; that its information sharing practices are appropriate and conform to policy; that its relationships with other domestic and foreign agencies are properly regulated; that its national security investigators are properly trained and show proper respect for human rights and individual liberties; that its communications with foreign countries, including communications when Canadians are being detained abroad, are appropriate; and also to ensure that there is effective review of any operational activities of the RCMP that are integrated with those of other agencies.

I also make detailed recommendations respecting the process for investigating complaints, the composition of ICRA and the manner in which ICRA should report to the government. The credibility of ICRA is crucial. I recommend that appointees be highly-regarded individuals whose judgements would be broadly respected—individuals with a stature similar to SIRC appointees.

Independent Review for Other Departments and Agencies — I recommend that the government extend independent review to the national security activities of the Canada Border Services Agency (CBSA), Citizenship and Immigration Canada (CIC), Transport Canada, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) and Foreign Affairs and International Trade Canada (DFAIT). My mandate directs that, in making recommendations in relation to the RCMP's national security activities, I consider how a review body for the RCMP's national security activities would interact with existing review mechanisms for other federal departments and agencies involved in the field. The five departments and agencies mentioned above have significant involvement in the national security field. Their activities are frequently integrated with those of the RCMP and other federal entities that carry out national security activities. However, at present, none is subject to independent review of the kind I propose for the RCMP or the kind provided by SIRC and the CSE Commissioner in respect of CSIS and the Communications Security Establishment (CSE).

The reasons for this recommendation are, in the main, the same as those for independent review of the RCMP's national security activities and the

activities of CSIS and the CSE. The national security activities of the five entities in question are integrated to a significant degree with those of the RCMP. Integration of national security activities is a critical component of Canadian policy, and co-operation among Canadian agencies involved with national security should be encouraged. However, effective review of RCMP national security activities that are integrated with those of the five entities requires that the latter's activities be subject to a similar type of review. Otherwise, there is a serious potential for gaps in accountability for integrated national security activities and inconsistent or incoherent results in the review of the same activities.

In my view, SIRC is the body best positioned to review the national security activities of four of the above-mentioned entities: CIC, Transport Canada, FINTRAC and DFAIT. Since the national security activities of the CBSA are largely related to law enforcement, I consider ICRA to be best suited to provide independent review of those activities.

These recommendations have the advantage of building upon existing institutions that have developed expertise and experience that can be applied to similar types of activities that will fall within their expanded jurisdictions.

Statutory Gateways — In order to provide integrated review of integrated national security activities, I recommend that the government enact statutory gateways linking the three independent review bodies — ICRA, SIRC, and the CSE Commissioner — to provide for the exchange of information, referral of investigations, conduct of joint investigations, and coordination and preparation of reports.

As I state above, the RCMP's national security activities are significantly integrated with those of other federal agencies. The Factual Inquiry showed how they were integrated with those of CSIS, Canada Customs (now part of the CBSA) and DFAIT. Since the events of September 11, 2001, the amount of integration of national security activities has increased substantially. The primary federal agencies involved in national security activities are or will be (if my recommendations are implemented) subject to independent review by one of three separate review bodies: ICRA, SIRC and the CSE Commissioner. It is essential that there be extensive co-operation among these review bodies when integrated operational activities involving those agencies are being reviewed. The statutory gateways I recommend are designed to achieve the necessary co-operation in review.

I note that several other countries have adopted statutory gateways for similar situations.

Integrated National Security Review Coordinating Committee — The government should establish a committee, to be known as the Integrated National

Security Review Coordinating Committee (INSRCC), comprising the chairs of ICRA and SIRC, the CSE Commissioner and an outside person to act as committee chair, to oversee the review of integrated national security activities. In particular, INSRCC would ensure that the statutory gateways are functioning as intended, provide a unified intake mechanism for complaints regarding national security activities of federal entities, and report to the federal government on accountability issues relating to Canada's national security practices and trends, including the effects of those practices and trends on human rights and freedoms.

INSRCC would not conduct any reviews itself. The independent review bodies would have sole responsibility in that regard. However, in my view, it is essential that there be a specifically mandated process for ensuring that the integrated review that I propose is working effectively. It is also important that there be a single point for filing complaints about national security activities. Given the amount of integration of operational activities and the secret nature of those activities, it is sometimes difficult, if not impossible for complainants to know where to file a complaint. The federal government should provide a mechanism to allow for a single body, INSRCC, to receive complaints and subsequently direct them to the appropriate review authority or authorities. Finally, it is important that a single body monitor trends and practices in national security activities, particularly as they affect human rights and freedoms. INSRCC would be ideally positioned to carry out this type of overview function and periodically report to the government.

Review in Five Years — I recommend that, in five years' time, the government appoint an independent person to examine how the review structure I propose is functioning. The national security landscape in Canada is constantly evolving to keep abreast of threats to our national security. It is vital that review and accountability mechanisms keep pace with operational changes. A review in five years' time should assist in this respect.

As a concluding observation, I believe that a credible review process that is able to fully address integrated national security activities should obviate the need for public inquiries or ad hoc reviews of individual cases.

My complete list of recommendations, with detailed rationales, can be found in Chapter XI.

Notes

[1] In the course of the Policy Review, Commission counsel and staff prepared a Consultation Paper and Background Papers for the roundtables of Canadian and international experts on review and oversight. These papers, as well as transcripts of hearings and roundtables and other information about the Policy Review, are included in the CD that accompanies this Report; they are also available on the Inquiry's website, at www.ararcommission.ca.

II

The History and Evolution of Canada's National Security Activities

1. INTRODUCTION

A fundamental obligation of any state is to protect public safety and national security. All states are concerned about protecting national security from both external threats to the state and threats to individuals that are of such a magnitude that they threaten the stable functioning of the state and its sense of well-being. Democracies like Canada face particular restraints and challenges in pursuing the vital goal of national security.

Well before 9/11, the 1985 terrorist bombings of two Air India flights that killed 331 people signalled the grave threats that terrorism presents to national security and the safety of Canadians. Canada has committed itself internationally to taking reasonable steps to combat terrorism by signing and ratifying 13 international conventions and instruments against terrorism. The first convention, the Tokyo Convention on Offences and Certain Other Acts Committed on Board Aircraft, was signed by Canada in 1963 and ratified in 1969. The most recent, the International Convention for the Suppression of Acts of Nuclear Terrorism, was signed by Canada in September 2005.

Since 9/11, there has been greater emphasis on matters of national security and public safety within government, and increased intensity and integration of the Government's counter-terrorism activities. In addition to police and security intelligence agencies, many other government departments and agencies are being mandated to pursue national security responsibilities. Canada has enacted new laws — the *Anti-terrorism Act* and the *Public Safety Act* — to try to prevent future acts of terrorism. The federal government has a new Department of Public Safety and Emergency Preparedness and has issued its first national security policy. This policy stresses the need for the Government of Canada to

take an integrated approach to threat assessment, threat prevention, consequence management and review with respect to threats to national security ranging from terrorism to natural disasters.

Canada has faced threats to its national security and the safety of Canadians from Confederation on. The focus of the threats has evolved over time from Fenians, to "enemy aliens" during the World Wars, to Communists in the Cold War, to terrorists in a modern era that includes the October Crisis, the Air India bombings and the events of 9/11. Failure to prevent terrorism and other threats to national security can have devastating consequences, as witnessed by the deaths of 331 people in the Air India bombings and almost 3,000 people, including Canadians, in the 9/11 attacks. At the same time, the past contains reminders of the harms of overreacting in trying to achieve national security — the internment of Japanese Canadians during World War II, and excesses with respect to investigating Communists and those affiliated with the Quebec sovereignty movement are examples. As the McDonald Commission eloquently stated, the purpose of national security in a democracy is to preserve democracy, including respect for the rule of law and the right of dissent.[1] The Supreme Court of Canada has recently issued similar warnings, reminding us that a response to terrorism "within the rule of law preserves and enhances the cherished liberties that are essential to democracy"[2] and that "it would be a Pyrrhic victory if terrorism were defeated at the cost of sacrificing our commitment to those values"[3] such as liberty, the rule of law and the principles of fundamental justice. The RCMP has a significant role in Canada's response to threats to national security. In the post-9/11 world, however, the RCMP's national security activities are only one element of Canada's national security landscape. To understand the RCMP's role, and to address the issue of the type of review required for this role, it is necessary to put it in the context of Canada's national security activities as a whole. This chapter begins with that context by describing the history of national security activities in Canada from Confederation through the events of September 11, 2001. The next three chapters complete the context by setting out the changes since September 11, 2001; the RCMP's current national security activities; and Canada's current national security landscape.

Throughout this report, I use the term "national security" as equivalent to the term "threats to the security of Canada" as defined in section 2 of the *Canadian Security Intelligence Service Act* (*CSIS Act*):[4] espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage; foreign-influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person;

activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state; and activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada.[5]

2.
CONFEDERATION TO WORLD WAR II[6]

At the time of Confederation, matters of national security were primarily within the authority of the Dominion Police Force, which was created by Parliament to protect federal buildings in Ottawa and eventually expanded to provide all national security requirements of the federal government. Important elements of national security work from the outset were the collection of information and the development of intelligence about potential threats to Canada.[7] The Dominion Police supervised a network of undercover agents operating in Canada and the United States, mainly to obtain information about Fenian activities.[8]

The need for national security intelligence intensified during World War I. The Dominion Police Force grew from 12 individuals in 1868 to 140 in 1919. At this time, the RCMP[9] also became increasingly involved in gathering national security intelligence: for example, RCMP personnel investigated allegations of pro-German sympathies among European immigrants. In 1920, the RCMP absorbed the Dominion Police Force and became the primary federal agency responsible for both collecting national security intelligence and enforcing laws concerning national security. The McDonald Commission report noted that "one of the principal purposes of this change was to unify and strengthen the federal security intelligence capability."[10] The primacy of the RCMP in both national security intelligence gathering and law enforcement was to continue until the 1980s.

Between 1920 and 1946, national security activities were the responsibility of the RCMP's Criminal Investigation Branch (CIB). Until the mid-1930s there was little to differentiate national security intelligence gathering from national security criminal investigations, or national security work in general from the CIB's other work — the same personnel did all types of work and reported to the same superiors. It was not until 1936 that an Intelligence Section, tasked with collecting and analyzing national security information, was established within the CIB. The Section remained small up until World War II.

World War II brought considerable, although temporary, growth in the RCMP's national security intelligence collection work. At its peak, in 1943, the Intelligence Section at Headquarters had three officers and 95 other personnel. In addition, specialized intelligence units were developed within certain divisional headquarters, including Toronto (20 personnel), Montreal (19 personnel) and Vancouver (9 personnel).

From the 1930s onward, the communist movement was a major focus of national security intelligence collection work. With the rise to power of Hitler and Mussolini, increased emphasis was placed on fascist and Nazi organizations in Canada. It is important to note that from the 1920s on, the RCMP had a policy of restricting covert intelligence-gathering operations to Canadian territory, and relied on liaisons with British and American agencies to obtain information from outside Canada. Aside from intelligence gathering, the RCMP's major national security activity during World War II concerned the registration and internment of what were referred to as "enemy aliens."

3.
NATIONAL SECURITY AFTER WORLD WAR II

After the Second World War, the Gouzenko spy affair[11] became a catalyst for changes to the RCMP's national security responsibilities. The Government implemented a security screening system in response to the affair to help ensure that individuals with access to sensitive information were trustworthy. The RCMP was made responsible for carrying out the screening process, which was eventually expanded to include screening for citizenship, identity certification (travel documents for non-citizens) and immigration.

Another program with which the RCMP became involved after the war was the compilation of lists of persons to be interned in the event of an emergency. Its role was to provide information about individuals or groups to an Advisory Committee on Internment appointed by the Department of Justice, which decided which names would be included on internment lists. The program focused on the Communist Party and other communist organizations.

A significant component of the RCMP's national security mandate at that time concerned foreign intelligence agencies operating in Canada and various forms of domestic subversion. The RCMP conducted surveillance of foreign intelligence agency groups and individuals and took preventative measures against them, sometimes referred to as "countering" or "counter-subversion." The work included both keeping check on foreign diplomats suspected of carrying out secret intelligence functions in Canada and investigating persons suspected of being long-term, deep-cover foreign agents. The Force assisted in several

prosecutions under the former *Official Secrets Act*[12] and decisions by the government to declare diplomats *personae non gratae*.[13] From World War II until 1980, there were about 20 charges under the *Official Secrets Act*, and 42 diplomats were declared *personae non gratae*.

The main focus in the area of domestic subversion in the immediate post-war period was on organizations suspected of being related to communism. By the 1960s, there was also increasing focus on several new perceived threats to national security. One such threat was terrorism which, while it had always been part of the Canadian national security landscape (for example, Fenian activities), began to increase in scale and in the level of concern to Canadians. International terrorism came into particular focus after the events of the 1972 Munich Olympics,[14] especially since Montreal was to host the Olympics in 1976. Other perceived threats included the Quebec separatist movement; and what was called the "New Left," which included anti-war, radical student and certain labour organizations.

The RCMP became increasingly involved in counter-subversion. Their activities were designed to disrupt groups considered to be subversive. In support of its countering activities, the RCMP relied primarily on information collected through covert sources, including electronic surveillance, mail opening, searches without warrant and the use of confidential personal information. It also used human sources such as informants and undercover agents.

RCMP national security activities during this period continued to involve the collection of significant amounts of information and intelligence. The McDonald Commission observed that very little of this information was actually used for prosecutions. Instead, most of it was stored and eventually used to provide reports to others, including other police forces and various government departments and agencies.[15]

The structure of the RCMP continued to evolve after the war. In 1946, the Intelligence Section became a Special Branch, but still reported to the Director of the CIB. In 1950, the officer in charge of Special Branch began to report directly to the Commissioner of the RCMP. In 1956, the officer in charge was elevated to the directorate level and the branch became known as the Directorate of Security and Intelligence, or "I" Directorate. This structure remained essentially unchanged until 1970, when the head of the "I" Directorate was appointed a director general — the same rank as a deputy commissioner — and the name of the Directorate was changed to the Security Service. The evolution of the RCMP's organizational structure reflected an increasing separation of the intelligence-gathering and analysis function from the criminal investigation function in relation to national security.

The number of RCMP personnel working on national security matters began to grow again during this period, and by the end of the 1960s had increased fifty-fold. Not all those involved in such work were regular members of the RCMP. Since 1951, individuals involved in national security work had been divided into four categories. The largest component was regular members of the RCMP. In addition, there were special constables, who were recruited for specialized investigative work but were not on the regular RCMP career path; public servants, who carried out support staff functions; and several civilian members, whose role was mainly to analyze information and write security reports.

Until the mid-1960s, Canadians seemed content by and large to let national security agencies do their work in secret, unchecked by any external scrutiny of the efficacy or propriety of their operations. Part of the explanation for this may lie in the relatively consensual and bipartisan nature of debates over national security during the war and the early Cold War years. In 1965, however, two security-related scandals erupted, quickly becoming partisan political issues. The firing of a Vancouver postal worker as a suspected Soviet spy caused a public outcry. Then the Gerda Munsinger affair implicated two former Cabinet ministers in a relationship with a woman believed to have connections to Soviet espionage. Under considerable pressure from Parliament and the press, Prime Minister Lester Pearson called two separate commissions of inquiry into these affairs, and then followed these up with a wider royal commission on security, known as the Mackenzie Commission. The Mackenzie Commission's terms of reference were to examine:

> the operation of [Canada's] security procedures . . . with a view to ascertaining firstly whether they [were] adequate . . . for the protection of the state against subversive action [and,] secondly, whether they sufficiently protect[ed] the rights of private individuals in any investigations which [were] made under existing procedures."[16]

The Mackenzie Commission reported in 1969. One of its principal recommendations was for the Security Service to be detached from the RCMP and reformed as a "new civilian non-police agency . . . quite separate from the RCMP . . . without law enforcement powers."[17] The Commission concluded that it was inappropriate for a law enforcement body to be involved in national security intelligence work and that such work was incompatible with the role of ordinary police. Specifically, it expressed concern about combining a mandate to collect security intelligence with the coercive powers of a police force. The Mackenzie Commission also concluded that the Security Service within the RCMP lacked the necessary sophistication and powers of analysis to perform the security

intelligence function competently. It was felt that security intelligence work should be undertaken by a civilian agency with more expertise and sophistication, and with greater direct accountability to the Government. The Commission also made recommendations for legislation to regulate intrusive investigative techniques and security screenings.

The MacKenzie Commission recommended creating a Security Review Board nominated by the Governor in Council, but "independent of any government department or agency."[18] The Board's main job would be to hear appeals from public servants, immigrants and citizenship applicants denied security clearance. The Board would also receive periodic reports from the head of the Security Service and would have "authority to draw to the attention of the Prime Minister any matter it considers appropriate."[19] This recommendation was linked to the recommendation to create a civilian security service separate from the RCMP in that the status of the Security Service as a branch of a police force was seen as an obstacle to developing accountability, in part due to concerns about "police independence."[20]

Most of the Mackenzie Commission's major recommendations were not implemented by the Government. In particular, the Government rejected the complete "civilianization" of the Special Branch and the Branch's removal from the RCMP. Instead, it adopted a compromise: the Security Service was to remain within the RCMP, but would become "increasingly separate in structure and civilian in nature."[21]

Some civilianization did take place in the late 1960s and early 1970s. Specifically, a number of civilians were appointed successively to the position of Director General of the Security Service. Between 1969 and 1979, the civilian membership of the Security Service increased from 9.9 percent to 17.2 percent. The McDonald Commission noted, however, that most civilians worked at jobs considered to be in the lower ranks, and that at the time of the Commission report no civilian held a position equivalent to an officer rank. During the 1970s many RCMP officers did take advantage of programs to upgrade their educational qualifications. While the composition of the Security Service remained essentially the same during this period, it became increasingly independent from the rest of the RCMP in matters of policy, budget and operations.

4.
THE 1970 OCTOBER CRISIS AND ITS AFTERMATH

Throughout the 1960s, the Security Service had been directing attention to the Quebec sovereignty movement, especially the violent terrorist wing that was engaging in criminal activity. In October 1970, cells of the Front de libération du

Québec (FLQ) kidnapped the British trade commissioner, James Cross, and kidnapped and later murdered the Quebec minister of labour, Pierre Laporte. The Canadian government, acting upon the request of the Quebec government, invoked the War Measures Act on the basis of an "apprehended insurrection," suspending normal civil liberties, detaining a number of individuals without charge and without legal counsel, applying censorship of the press, and declaring certain organizations retroactively illegal.

The October Crisis caused the federal government to conclude that it needed more information about the nature and scope of the separatist movement. The Government asked the RCMP to undertake a "proactive" strategy to gather more advance information about the intentions and activities of the organizations involved in the movement, and to "prevent" or "counter" disruptive acts. In response, the RCMP embarked on what the McDonald Commission later characterized as a campaign of intelligence gathering, infiltration, harassment and disruption directed at many forms of nationalist sentiment in Quebec. This campaign included activities that were clearly not authorized by law, including (among the more notorious) burning down a barn to prevent a meeting of what were perceived to be militant nationalists and American radicals; breaking into a Montreal news agency seen as "left-wing" and stealing and destroying files; and breaking into a Parti Québécois office and stealing membership lists.

Such extensively criticized activities on the part of the RCMP were not restricted to Quebec or the FLQ. Examples of what became known as "dirty tricks," aimed in particular at "left wing" or radical groups, took place throughout Canada.[22] When some of these methods and events came to light in the media during the 1970s, questions arose around national security and the specific role of the RCMP Security Service in illegal acts. Intrusive methods were now seen to be used not just against small groups such as the Communist Party allied with a hostile foreign power like the USSR, but also against domestic political forces, an inherently more controversial matter.[23]

In 1974, the Government enacted section 16 of the *Official Secrets Act*. That section required the RCMP to seek authorization from the Solicitor General[24] for the interception or seizure of communications if the Minister was satisfied that the interception was "necessary for the prevention or detection of subversive activity directed against Canada or detrimental to the security of Canada or is necessary for the purpose of gathering foreign intelligence information essential to the security of Canada." Subversive activity was defined broadly to include espionage and sabotage; foreign intelligence activities gathering information relating to Canada; activities directed towards accomplishing governmental change within Canada or elsewhere by force, violence or criminal means; activities by

a foreign power directed towards hostile acts to Canada; and activities of a foreign terrorist group directed towards the commission of terrorist acts in or against Canada.

In 1975, Cabinet approved guidelines for Security Service activities in an attempt to address the concern about the lack of a clear mandate. These guidelines provided that:

(a) The RCMP Security Service be authorized to maintain internal security by discerning, monitoring, investigating, deterring, preventing and countering individuals and groups in Canada when there are reasonable and probable grounds to believe that they may be engaged in or may be planning to engage in:
    (i) espionage or sabotage;
    (ii) foreign intelligence activities directed toward gathering intelligence information relating to Canada;
    (iii) activities directed toward accomplishing governmental change within Canada or elsewhere by force or violence or any criminal means;
    (iv) activities by a foreign power directed toward actual or potential attack or other hostile acts against Canada;
    (v) activities of a foreign or domestic group directed toward the commission of terrorist acts in or against Canada; or
    (vi) the use or the encouragement of the use of force, violence or any criminal means, or the creation or exploitation of civil disorder, for the purpose of accomplishing any of the activities referred to above;
(b) The RCMP Security Service be required to report on its activities on an annual basis to the Cabinet Committee on Security and Intelligence;
(c) The Solicitor General prepare for consideration by the Prime Minister a public statement concerning the role of the RCMP Security Service.[25]

The guidelines were criticized as being both too broad and too vague. They were also silent on methods of investigation or of countering that the Security Service could use.

By 1976, the Parti Québécois (PQ) was in power in Quebec and launched its own inquiry into police activities.[26] It was unclear to what extent the federal government, through its Security Service, distinguished between threats to national security clearly posed by the terrorist wing of the sovereignty movement and threats to national unity posed by the democratic and strictly law-abiding PQ. If the PQ proved to be a target of extra-legal surveillance methods, the matter would raise serious issues about liberal democracy of much wider concern to Canadians than to Quebec sovereignists alone. These developments gave rise

to increasingly vocal demands for greater accountability and transparency in the operations of the federal Security Service.

5. THE McDONALD COMMISSION

In July 1977, the McDonald Commission was appointed to inquire into "certain activities of the RCMP."[27] The immediate cause of its appointment was guilty pleas by a member of the RCMP, and by members of the Quebec and Montreal police forces, arising out of a break-in at the Agence de Presse Libre du Québec. The McDonald Commission's mandate was both to report on RCMP activities that were not authorized by law and to make recommendations on the adequacy of laws and procedures relating to RCMP national security activities.

By the time the McDonald Commission was established, there was considerable public concern about the operation of the Security Service in Canada. The Commission validated this concern, cataloguing a long list of substandard, inappropriate and illegal activity, as well as numerous infractions of civil liberties resulting from the Service's surreptitious investigative methods. It found that almost all of these illegalities and improprieties were undertaken without the knowledge of the political officials charged with overseeing the RCMP.

The McDonald Commission concluded that the Security Service lacked a precise mandate, effective political control or adequate review of its activities. It was critical of the combination of law enforcement and security intelligence collection in one agency. It was also critical of the Security Service itself, which it saw as lacking sophistication and analytical ability. For example, it observed that there was an inability to distinguish subversion from dissent, and a related anti-"left wing" bias.[28]

The Commission made several significant recommendations for a reformulated security intelligence agency. These recommendations focused on setting out a clear mandate for the Security Service; establishing clear guidelines for the Service's operational activities; implementing management, recruiting and other personnel policies appropriate to a security intelligence agency; and developing suitable structures and procedures to ensure that the entity responsible for security intelligence was under the direction and control of government, including both parliamentary and non-parliamentary review and oversight mechanisms.[29]

The overarching, and most significant, recommendation was the removal of the Security Service from the RCMP. The commissioners strongly felt that the power to collect security intelligence should not be contained in the same organization as the coercive power of a police force — the same concern that

the Mackenzie Commission had raised. As the McDonald Commission stated in support of its recommendation that the security intelligence agency not be authorized to enforce security measures:

> First, as we argued in Part III, we think it is unacceptable in Canada that the state should use a secret intelligence agency to inflict harm on Canadian citizens directly. This position, it must be noted, does not prevent a police force or a government department from using intelligence supplied by the security intelligence agency to enforce a law or security measure against an individual. Second, we think the liberty of Canadians would be best protected if measures to ensure security were not enforced by the organization with the prime responsibility for collecting information about threats to that security. The assignment of executive enforcement responsibilities to agencies other than the security intelligence organization assures desirable countervailing powers and avoids the danger that the security intelligence organization might be both judge and executor, in security matters.[30]

Further reasons the Commission gave for this recommendation included the following:

i) *Appropriate management and personnel policies*: The Commission saw the RCMP management structure as inimical to the structure proposed for an improved security intelligence agency. It recommended recruitment of more mature, more experienced, better-educated personnel; a new approach to career paths; a more participatory, less authoritarian style of management; and substantially different training and development approaches. This was contrary to the authoritarian, military-style approach and structure that were seen to be entrenched in the RCMP. While it was possible to have two very different management structures in the same organization, the Commission concluded that such an arrangement would too likely create conflict that was detrimental to the much smaller Security Service.[31]

ii) *Direction and control by government:* A central aim of the reforms the McDonald Commission recommended was to improve the direction and control exercised over the security intelligence function by other parts of government, including Parliament, the minister responsible, other Cabinet members, and other senior officials in various departments and agencies. It was felt that effective oversight could best be achieved by placing the security intelligence function in a separate agency for two reasons.

First, while the report identified several similarities for the two agencies, including the requirement for ministerial guidance on policy issues, allocation of resources and liaison arrangements, it noted one fundamental

difference. This difference related to the degree to which the Minister and other senior governmental officials should be involved in decisions about what groups and individuals to investigate and how such investigations should proceed. The Commission concluded that in the case of a security intelligence agency, the Minister should be actively involved, because such decisions can have ramifications for Canada's system of government and its relations with other countries. In the case of a police force, involvement by the Minister and senior officials "in decisions about whom to investigate and how these investigations should be conducted should be on an advisory basis only and limited to matters with significant policy implications."[32]

Second, the McDonald Commission noted that "the traditional, and we believe unhealthy, semi-independent relationship which the R.C.M.P. has enjoyed with government will not easily be changed."[33] In the Commission's opinion, the RCMP needed to be more accountable to government even in policing functions, especially on broader policy issues and general approaches. It was felt that there was great resistance to increased accountability within the Force at that time. This culture would hinder the development of greater accountability on the security intelligence side.

iii) *Trust in the RCMP*: In the McDonald Commission's view, the questionable activities that they had investigated, involving both the Security Service and the criminal investigations side of the Force, "have diminished significantly the trust that Canadians and their governments have in the R.C.M.P."[34] The report acknowledged that the RCMP Commissioner and many others in the Force were working very hard to restore trust, but felt that it would be some time before this goal was accomplished.

iv) *Checks and balances could develop between the RCMP and the Security Service*: Finally, by making one organization responsible for collecting security intelligence and the other responsible for enforcing it, it was hoped that a system of checks and balances would develop between the RCMP and the security intelligence agency. It is important to note that the McDonald Commission also recommended that the security intelligence agency not have powers of arrest, search and seizure, and that a police officer accompany security agents on surreptitious entries under judicial warrants. It was felt that this division of responsibilities would create an interdependency between the agencies that in turn would allow the two organizations to monitor each other. Moreover, having two agencies would give the Minister two separate systems to assess against each other.[35]

The McDonald Commission recommended three forms of "external controls" for the proposed security intelligence agency. The first was judicial oversight. The Commission recommended that the Federal Court have a role in releasing confidential information and in authorizing the use of intrusive surveillance methods such as electronic surveillance, mail interception and surreptitious entry.[36] It also recommended creating a Security Appeals Tribunal associated with the Federal Court and specifically tasked with hearing security screening appeals.[37]

The second form of external control recommended was an Advisory Council on Security and Intelligence, which was to be an independent, arm's-length review body. Such a body was seen as necessary because of the extreme secrecy of many national security intelligence operations and the potential impact on the civil liberties of individuals who are the subject of national security investigations. As the report noted,

> With normal operations of government the citizen knows what the government has done to him, and can decide whether he wishes to question the propriety or legality of government action. However, with regard to security intelligence investigations which a citizen may fear are encroaching on his privacy or his political liberty, he has no way of knowing whether he has been investigated as a threat to security and, if he has, whether the investigation has been carried out in a legal and proper manner.[38]

The Advisory Council's basic function was to carry out "a continuous review of security intelligence activities to ensure that they are lawful, morally acceptable and within the statutory mandate established by Parliament."[39] The Advisory Council was to report regularly to the Solicitor General and at least on an annual basis to a parliamentary committee. The subjects of the review were to include the interpretation of the security intelligence agency's statutory mandate; the implementation of administrative directives and guidelines; the operation of a system of controlling intrusive intelligence collection techniques; and relationships with other agencies.[40] The McDonald Commission also recommended that the Advisory Council review activities after they had occurred, partly to ensure independence. It noted that if the Advisory Council were to pre-approve actions, the Council members themselves would be implicated in the actions. The Advisory Council's jurisdiction was to extend to all organizations employed by the federal government to collect intelligence through clandestine means, other than the RCMP.[41]

Third, the McDonald Commission recommended establishing a parliamentary committee to oversee the security intelligence agency. The committee's main function would be "to scrutinize the activities of the security intelligence organization with a view to ensuring that it fulfills the intentions of Parliament as set out in the organization's legislative charter."[42] Unlike the Advisory Council, the parliamentary committee was to "be as much concerned with the effectiveness of the security intelligence organization as with the legality or propriety of its operations."[43] The Commission recommended that the parliamentary committee be relatively small (no more than 10 members) and include members from all major political parties, and that efforts be made to maintain continuity of membership for a reasonable period of time. It also recommended that all parliamentary committee sessions be held *in camera*.

Recommendations were also made on a review mechanism for the RCMP, once the security intelligence function had been removed. The Commission recommended establishing a complaints commissioner, which they called the Office of Inspector of Police Practices.[44] This Office was to have two functions: the power "in exceptional circumstances" to investigate complaints of RCMP wrongdoing and make recommendations to the Solicitor General; and the right to monitor the RCMP's own investigations of its alleged misconduct and to evaluate its complaint-handling procedure. The Office of Inspector was to report directly to the Solicitor General.[45]

The McDonald Commission did not recommend entirely removing the RCMP from national security work. Instead, it envisioned a system where the proposed security intelligence agency would have primary responsibility for intelligence gathering, but would be assisted by the RCMP in such matters as executing warrants. The RCMP would keep responsibility for preventing crime, and for investigating and arresting criminals in the national security field. There was no discussion in the McDonald Commission report about an intelligence-gathering role for the RCMP arising out of its crime prevention and criminal apprehension role.

6.
1984-2001

6.1
OVERVIEW

Following the McDonald Commission's recommendations, the Government of Canada accepted that combining security intelligence and policing responsibilities in a single policing agency was inappropriate. Consequently, in 1984

Parliament passed the *Canadian Security Intelligence Service Act* creating the Canadian Security Intelligence Service (CSIS) as a civilian security intelligence service with no powers of criminal investigation or prosecution. CSIS' mandate and activities are described in detail in Chapter V. In general terms, CSIS is required to collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyze and retain information and intelligence about activities that may on reasonable grounds be suspected of constituting threats to the security of Canada. CSIS may advise any minister of the Crown on matters relating to the security of Canada, or provide any minister of the Crown with information relating to security matters or criminal activities, that is relevant to the exercise of any power or the performance of any duty or function by that minister under the *Citizenship Act* or the *Immigration and Refugee Protection Act*. CSIS may also, in prescribed circumstances, within Canada, assist the Minister of National Defence or the Minister of Foreign Affairs in collecting information or intelligence relating to the capabilities, intentions or activities of any foreign state or group of states, or of any person who is not a Canadian citizen, a permanent resident of Canada or a corporation incorporated by or under an Act of Parliament or a provincial legislature.

National security was not placed exclusively in the domain of CSIS. At the same time it passed the *CSIS Act*, the Government also passed the *Security Offences Act*,[46] which gave the RCMP primary responsibility over national security law enforcement. As concern about terrorist threats increased, a number of other departments and agencies were given national security roles. Canada's national security landscape, as it exists today, is described in Chapter V.

In this section, I examine the RCMP's national security activities following the creation of CSIS and before the events of 9/11. It is useful to see this period as the foundation for the RCMP's current national security role, which is discussed in detail in Chapter IV. The section is divided into an introduction to the RCMP in the CSIS era; an examination of the RCMP's national security activities after the creation of CSIS; a discussion of the concept of intelligence-led policing; a description of the internal organization of the RCMP's national security activities before 9/11; a description of the interaction between the RCMP and CSIS; and a brief discussion of the most notable national security event during this period — the Air India bombings of 1985.

6.2 INTRODUCTION TO THE RCMP IN THE CSIS ERA

The *Royal Canadian Mounted Police Act (RCMP Act)*[47] establishes and authorizes the RCMP to be Canada's national police force. Section 4 of the Act provides that the RCMP may be deployed both within and outside Canada.

As a result of Canada's Constitution;[48] the historical development of the Force; various federal statutes;[49] and arrangements that certain provinces, territories, municipalities and First Nations communities have made to contract policing duties out to the RCMP, the Force's responsibilities today consist of a patchwork of law enforcement activities.

The RCMP has inherent responsibility for enforcing all federal laws, except significant parts of the *Criminal Code*, in all Canadian provinces and territories. It also has responsibility for enforcing all of the *Criminal Code*, as well as provincial and municipal laws, in jurisdictions that have contracted its policing services. All provinces except Ontario and Quebec have contracted the RCMP to provide policing services, as have the three territories, 197 municipalities and 192 First Nations communities.[50]

The RCMP's many statutory and contractual duties result in a long list of functions. These can be grouped under six broad headings:

(a) federal policing, including drug enforcement, economic crime and national security investigations;

(b) contract policing, including its provincial, territorial and municipal policing;

(c) national policing, including its forensic laboratory services, technical operations, the Criminal Intelligence Service Canada and the Canadian Police College;

(d) protective policing, including airport policing and protection of Canadian and foreign officials;

(e) international peacekeeping; and

(f) corporate services.[51]

Section 5 of the *RCMP Act* authorizes the Governor in Council to appoint a Commissioner who "under the direction of the Minister, has the control and management of the Force and all matters connected therewith."[52] This relationship has evolved into one where the Minister provides directions to the Commissioner setting out relatively broad policy guidelines and standards. As

described in a document entitled "The Directives System" prepared by the Solicitor General's department in 1984:

> Solicitor General Directives set standards for the RCMP in selected areas of policing activity. The Directive procedure is one of the most important means by which the Minister exercises his responsibility over the Royal Canadian Mounted Police.
>
> Effective policing requires the continued confidence and support of the public. In order to ensure that that confidence is maintained the Solicitor General must establish certain standards which balance individual rights with effective policing practices.[53]

In addition to the Commissioner, there are seven deputy commissioners, 24 assistant commissioners, and several chief superintendents, superintendents and inspectors, all appointed by the Governor in Council pursuant to the *RCMP Act*.[54]

The RCMP comprises more than 22,000 members, including over 15,500 regular members, over 2,500 civilian members and approximately 4,000 public servants.[55] The Force is divided into four regions, 14 divisions and over 750 detachments. Its headquarters are in Ottawa.[56]

Every officer and every other person designated as a peace officer under subsection 7(1) of the *RCMP Act* is a peace officer in every part of Canada, with the power, authority, protection and privileges that a peace officer has by law. Under section 18 of the RCMP Act, it is the duty of members who are peace officers, subject to the orders of the Commissioner:

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

This definition of the duties of peace officers includes not only the enforcement of federal and provincial laws and the execution of warrants, but also "the preservation of the peace" and the "prevention of crime."

6.3 RCMP NATIONAL SECURITY ACTIVITIES AFTER THE CREATION OF CSIS

As noted above, the McDonald Commission report did not call for eliminating RCMP involvement in all matters relating to national security. In carrying out many of the McDonald Commission's recommendations, the Government maintained a significant national security role for the RCMP. While CSIS was established to carry out the national security intelligence function that the Security Service had performed, the RCMP retained responsibility for national security law enforcement. The scope of that role was set out originally in the *Security Offences Act*.

The same year the *CSIS Act* was enacted to provide Canada with a civilian intelligence agency, the *Security Offences Act* was enacted. Section 6 of that Act provides that RCMP peace officers "have the primary responsibility to perform the duties that are assigned to peace officers" in relation to offences that arise "out of conduct constituting a threat to the security of Canada within the meaning of the [*CSIS Act*]"[57] or if "the victim of the alleged offence is an internationally protected person within the meaning of section 2 of the *Criminal Code*." Thus, the Act recognized that the RCMP, as the federal police force, as opposed to municipal or provincial forces, should have primary responsibility for investigating such criminal offences.

The definition of threats to the security of Canada set out in the *CSIS Act* includes references to sabotage, espionage, foreign-influenced activities, clandestine activities, threat or use of serious violence, and undermining by covert unlawful acts. On the basis of this definition there is a potentially long list of offences that could be national security crimes. The list includes sabotage (section 52 of the *Criminal Code*); and espionage; wrongful communication with a foreign power; and harbouring spies (sections 3, 4 and 8 respectively of the former *Official Secrets Act*).[58] In addition, offences such as treason and seditious speech or conspiracy (sections 46 and 61 of the *Criminal Code*), while rarely charged, could be national security offences. Offences that would otherwise not be national security offences could become so in certain circumstances. For example, the threat or use of serious violence against persons or property could include a wide range of *Criminal Code* offences relating to air or maritime safety, explosives, kidnapping, murder, mischief and arson. Foreign-influenced and

clandestine events that involved uttering threats contrary to section 264.1 of the *Criminal Code* could also be national security offences. The RCMP's primary responsibility for policing if the victim is an "internationally protected person"[59] also potentially involves many crimes.

Before the *Anti-terrorism Act* was enacted at the end of 2001, the RCMP's powers with respect to national security offences were largely the same as its powers with respect to its other responsibilities. As noted above, section 18 of the *RCMP Act* establishes that the duties of RCMP officers include the enforcement of laws and the execution of warrants, as well as the "preservation of the peace" and "the prevention of crime."

Even before the enactment of the *Anti-terrorism Act*, the RCMP and other police forces had a broad range of police powers that could be used in criminal investigations, including those involving threats to the security of Canada. One of the more important powers in the national security context is the ability to use electronic surveillance. Under Part VI of the *Criminal Code*, the police can in certain circumstances obtain a judicial warrant authorizing the interception of private communications. Normally, the warrant application must demonstrate that "other investigative procedures have been tried and have failed or why it appears they are unlikely to succeed or that the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures."[60] As will be seen, the *Anti-terrorism Act* changed this requirement.

In addition to the specific provisions for authorizing electronic surveillance under Part VI of the *Criminal Code*, there are also a wide variety of search powers under Part XV of the *Criminal Code*. These powers include search warrants, search warrants to make an arrest in a dwelling, warrants to obtain DNA samples, and a general warrant provision that allows judicial authorization of the use of any investigative technique or procedure that would otherwise constitute an unreasonable search or seizure. In general, warrants are granted on a demonstration under oath that there are reasonable grounds to believe an offence has been committed and that the search will reveal evidence of the offence. Limited powers of warrantless searches in exigent circumstances where it is not practicable to obtain a warrant are recognized in both the *Criminal Code* and under the jurisprudence of the *Charter of Rights and Freedoms*. Other police powers include arrest powers and warrants,[61] and the ability to apply for recognizances or peace bonds.[62] As will be discussed, the *Anti-terrorism Act* increased the ability to obtain recognizances.

In 2001, the *Criminal Code*[63] was amended to give public officers, including customs officers and police officers, the power to commit acts that would

otherwise constitute an offence. The police officer must be engaged in the investigation of criminal activity or enforcement of an act of Parliament, must be designated by a senior officer responsible for law enforcement and must believe on reasonable grounds that the commission of the act or omission as compared to the nature of the offence or criminal activity being investigated is reasonable and proportional in the circumstances.[64] If the activity is likely to result in loss of or serious damage to property, additional authorization from a senior officer is required. There are also provisions for public officers directing third parties to commit offences. The intentional or criminally negligent causing of death or bodily harm to another person, the willful attempt to obstruct justice and the violation of an individual's sexual integrity is never justified under this section.[65]

This provision provides several accountability measures short of the requirement for a judicial warrant that is generally required for searches and seizures, including the use of electronic surveillance. The peace officer who commits the act must as soon as is feasible file a written report to a senior officer under section 25.2. Public annual reports must be filed under section 25.3. As soon as feasible, and no later than a year later, a person whose property was lost or seriously damaged must be notified under section 25.4, unless the minister responsible for the RCMP is of the opinion that notification would compromise an ongoing investigation, an undercover officer or a confidential informant; endanger the life or safety of any person; prejudice a legal proceeding; or be otherwise contrary to the public interest.

6.4 INTELLIGENCE-LED POLICING

As noted above, the McDonald Commission Report envisioned a clear division between the security intelligence function (CSIS) and the law enforcement function (the RCMP and other police agencies). However, experience has shown there remains a significant overlap between these functions. An important element of this overlap was the development by the RCMP of an approach to policing that became known as intelligence-led policing.

Intelligence-led policing arose primarily from a new approach to policing developed in the 1980s and 1990s referred to as "Community Policing." Community Policing focused on developing better relations with the communities the Force served and engaging such communities in problem solving. It brought a general change in approach and a change in the training of front-line police officers, including an increased focus on working in the community and acquiring information about the community's needs; and an emphasis on

preventing crime through problem solving rather than strictly reacting to it after it occurs.[66]

It soon became evident that for the Community Policing approach to work effectively, the RCMP needed an accessible bank of information on which to base its problem-solving and crime prevention activities. Events like the Oka Crisis in the summer of 1990 underscored the need for better information and intelligence, as there was a perception that this event had taken the Force by surprise.[67] As stated in the RCMP's 1991 *Criminal Intelligence Program Implementation Guide*:

> Up to this time, the failure to develop a sophisticated strategic as well as tactical intelligence capability within the RCMP has seriously hindered the Force's ability to accurately measure and prevent crime having an organized, serious or national security dimension in Canada, or internationally as it affects Canada. This, in turn, has prevented the development of a more effective crime control strategy that would have a measurable impact on reducing the serious effects of crime on Canadian society.[68]

By the late 1990s, the new approach to policing was referred to as intelligence-led policing.

The basic concept of intelligence-led policing is relatively straightforward. As set out on the RCMP website:

> Most would agree, however, that at its most fundamental, intelligence-led policing involves the collection and analysis of information to produce an intelligence end product designed to inform police decision-making at both the tactical and strategic levels. It is a model of policing in which intelligence serves as a guide to operations, rather than the reverse. It is innovative and, by some standards, even radical, but it is predicated on the notion that a principal task of the police is to prevent and detect crime rather than simply to react to it.[69]

Intelligence-led policing has developed into an RCMP-wide approach and is not restricted to any particular type of criminal activity.[70] Indeed, the approach is employed by most major police forces in the Western world.[71] In my view, it is both logically and practically linked to policing, and as I noted in the Factual Inquiry report, has been an important and reasonable response to the increasingly complex and sophisticated criminal activities that the RCMP must investigate. However, in the national security context, intelligence-led policing has resulted in the RCMP engaging in activities very similar to those CSIS engages in, albeit for different ultimate purposes. As the government report *On Course: National Security for the 1990s* noted in 1991,

> Both employ similar investigative methods and techniques to acquire information on the activities of individuals and groups, the RCMP to enable the force to prevent crime or to lay charges, CSIS in order to report to and advise the Government with respect to threats.[72]

The different ultimate purpose for which intelligence is collected has resulted in the use of the term "criminal intelligence" as distinct from the "security intelligence" that CSIS collects.[73] Criminal intelligence is characterized as intelligence with a link to criminal activity, gathered in support of investigations, with the goal of preventing or deterring a criminal act or of arresting a criminal. Security intelligence, on the other hand, refers to information relating to threats to the security of Canada that is collected for the purpose of advising the Government.[74]

It seems clear, however, that in the national security context, the very same information can be both criminal intelligence and security intelligence. It is also clear that both forms of intelligence can be gathered and analyzed in the same way.[75] In addition, while "criminal intelligence" is collected to further the RCMP's criminal mandate, the link between the collection of intelligence and a criminal prosecution can be somewhat distant. For example, the RCMP recognizes a difference between intelligence gathering and traditional investigative work. In its *Criminal Intelligence Program Guide*, the RCMP states

> The development of intelligence should not be confused with traditional investigative work. Although the two are related, they are only cousins in the police and law enforcement system. Investigative reporting is evidentiary in nature. Intelligence reporting is like an early warning system — what are the capabilities, vulnerabilities, limitations and intentions of criminal organizations or individual criminals?[76]

Thus, while the purposes for collecting security intelligence may be different than those for collecting criminal intelligence, the distinction between the two may blur in practical application. I note in the Factual Inquiry report that while it is appropriate for the RCMP to continue with its intelligence-led policing approach, it is critical that in doing so, the Force remains within its law enforcement mandate. Given the potential for blurring, it is important that the policing purpose for which the RCMP gathers intelligence is respected.

6.5
THE INTERNAL ORGANIZATION OF THE RCMP'S NATIONAL SECURITY ACTIVITIES BEFORE 9/11

After CSIS had been created, the RCMP made several organizational changes concerning its national security mandate. In 1988, the Force established a National Security Investigation Directorate (NSID) and a National Security Operations Branch (NSOB) at Headquarters to provide expertise and dedicated resources for investigating offences with a national security dimension, and to supply investigative and related support for its protective policing program (including government officials and internationally protected persons). National Security Investigation Sections (NSIS) were created in 1988 and given responsibility for the operational aspects of national security investigations. From the outset, they had a centralized reporting function.[77]

To facilitate the new intelligence-led policing approach, a Criminal Intelligence Directorate (CID) was created in 1991. The CID mission statement provides the following:

> The mission of the Criminal Intelligence Directorate is to provide a national program for the management of criminal information and intelligence which will permit the RCMP to detect and prevent crime having an organized, serious or national security dimension in Canada, or internationally as it affects Canada.[78]

The establishment of CID also involved reorganizing the national security function. All Headquarters departments involved directly in the RCMP's national security mandate were located within CID. CID included a Security Offences Branch to coordinate investigations of national security offences. In addition to CID at Headquarters, there were also criminal intelligence sections in the divisions. Their role was to bring together various pieces of information in the provinces and to provide those to Headquarters.

An important component of CID's creation in 1991 was the establishment of the Secure Criminal Information System (SCIS). SCIS, which is described in greater detail in Chapter IV, is a centralized database used exclusively for national security information and intelligence. Because of its connection to national security, all such information is classified by the RCMP. Access to SCIS is restricted to personnel with the appropriate security clearance who "need to know" the information to perform their functions.

6.6 INTERACTION WITH CSIS

The RCMP developed its relationship with CSIS in the 1980s and 1990s. In July 1984, a ministerial directive was issued describing the expected relationship between the RCMP and CSIS. A further directive in August 1986 established the RCMP/CSIS liaison officer program to facilitate communication and coordination between the two organizations. This program involved appointing personnel within each organization as point persons for information and consultation. In 1986, the Minister also approved a memorandum of understanding (MOU) between the RCMP and CSIS dealing with co-operation between the two organizations, including the exchange of information as it relates to law enforcement.[79] The MOU was amended in 1991. Together with relevant legislative provisions, it continues to govern the relationship between the RCMP and CSIS.[80]

The MOU sets out the following guiding principles:

- The RCMP will rely on CSIS for intelligence relevant to national security offences.
- CSIS will provide to the RCMP intelligence relevant to the RCMP's security enforcement and protective security responsibilities.[81]
- The RCMP will provide to CSIS information relevant to the CSIS mandate.
- The RCMP will be the primary recipient of security intelligence on national security offences.
- The RCMP and CSIS will consult each other with respect to the conduct of [national] security investigations.
- The RCMP and CSIS will conduct security investigations in accordance with guidelines, standards and directions provided by the Solicitor General.

Part I of the MOU deals with the exchange of information and intelligence, and in particular the types of information that will be exchanged. Part II deals with operational support and assistance, specifically with support that will be provided for special events, security assessments, air services, protective security, photographic services, foreign liaison and incident management. On some occasions, when CSIS is unable to do so, the RCMP provides investigative assistance such as surveillance.[82]

Part III of the MOU sets out principles and mechanisms to facilitate co-operation in the exchange of information. Specifically, four principles are set out:

(a) All information, documentation or material provided under the MOU shall be fully protected and any caveats imposed by either party shall be fully respected to the extent provided by law.

(b) National security investigative files shall be maintained separately from other investigative records and access to these files shall be strictly governed by the "need to know" principle.
(c) Subject only to the requirements of the courts, information provided by either party to the MOU shall not be used for the purposes of obtaining search warrants or authorizations to intercept private communications produced as evidence in court proceedings or disclosed to Crown prosecutors or any third party without the prior express approval of the party that provided the information.
(d) The MOU shall not be interpreted as compelling either party to disclose the identity of its sources or caveated information from a third party.

These principles reflect the secrecy appropriate to national security intelligence. They also reflect the fact that it is necessary to protect the identity of sources and to respect the conditions imposed on the sharing of information from foreign agencies to ensure the continued flow of such information. Further, they suggest that much security intelligence (at least what CSIS provides) will never be used as evidence in court.

The CSIS/RCMP MOU provides for a liaison officer program and a liaison committee. The liaison officer program has been replaced by an officer exchange program through which personnel from each entity are seconded. These liaison and exchange programs are intended to foster co-operation in the identification and exchange of information and intelligence; the provision of operational assistance; the investigation of targets of mutual interests; and the establishment of combined operations.

6.7
THE AIR INDIA BOMBINGS OF 1985

Before turning to the changes to the Government's approach to national security after the 9/11 terrorist attacks, it is important to mention the most notable national security event that occurred in the post-CSIS era up to 9/11 — the terrorist bombing of Air India Flight 182. That bombing killed 329 people in what remained, until 9/11, the world's most deadly act of aviation terrorism. Two other people were killed in Narita, Japan, when a bomb placed on an Air India flight out of Vancouver also exploded. As Bob Rae recently stated in his report: ". . . the bombing of the Air India flight was the result of a conspiracy conceived, planned, and executed in Canada. Most of its victims were Canadians. This is a Canadian catastrophe, whose dimension and meaning must be understood by all Canadians."[83]

The bombing of the Air India flights revealed many new and deadly threats to Canada's national security. It showed how events in foreign lands may affect the security of Canadians in Canada and abroad. The conspiracy to bomb Air India originated in the Babbar Khalsa movement, a Sikh group that wished to separate from India, especially in light of the Indian government's raid on the Golden Temple in 1984. In response to these events, which included attacks on the acting Indian high commissioner in Canada and a diplomatic note from the state of India, the Government of Canada established an interdepartmental committee on Sikh terrorism in May 1985 with representatives from the Department of Foreign Affairs, the RCMP, CSIS and the Solicitor General.[84] This demonstrates, even before 9/11, a recognition of the need for increased integration within the federal government with respect to threats to national security.

The Air India bombings show how modern-day threats to national security require co-operation and integration among agencies responsible for national security. Mr. Rae's report identified several issues relating to how these agencies should best function together. In March of 1985, CSIS obtained a warrant to intercept the communications of Talwinder Singh Parmar, one of the conspiracy leaders. CSIS agents also carried out physical surveillance of Parmar and his associates, including Inderjit Singh Reyat, who has been convicted of manslaughter in both the bombing of Air India Flight 182 and the related Narita bombing. At the same time, there were problems within CSIS around translating and keeping the electronic surveillance tapes, and around informing the RCMP of information relevant to its crime-based mandate. At the time, CSIS was devoting 80 percent of its resources to counter-intelligence and counter-espionage, and the experience of the Cold War "had created a culture of secrecy and only telling others on a 'need to know' basis."[85] Thus, the situation raises issues about the desirable degree of consultation and co-operation between the RCMP and CSIS, and how information and intelligence gathered from a security intelligence agency can and should be passed on to police forces. Air India stands as a chilling reminder of the importance of co-operation between CSIS and the RCMP, and the need for information sharing between two institutions that have distinct but complementary and vital roles in protecting the national security of Canada.

The Air India bombings also illustrate how government institutions beyond the police and security intelligence agencies have responsibilities for national security and the public safety of Canadians. Given intelligence and the political situation, Canadian authorities were aware that Air India flights originating in Canada could be terrorist targets. As a result, special precautions were being taken to screen luggage and to match it with passengers on Air India flights. Tragically, the luggage containing bombs was allowed to travel from Vancouver

both on the Narita-bound flight and with connections through Toronto to Air India Flight 182, even though the passenger who checked in the luggage did not travel on either flight. An X-ray machine used to screen the luggage before it was loaded onto Air India Flight 182 in Toronto broke down, and a hand-held explosive sniffer of doubtful reliability was used on the remainder of the luggage.

The Air India bombings, like the October Crisis, are painful reminders that Canada and Canadians are not immune from terrorism. Canada has agreed to 13 different international conventions and instruments relating to various forms of terrorism. Three of these instruments from the 1960s and 1970s relate to offences on aircraft and hijackings.[86] Another relates to violence at airports,[87] and two others to terrorism on the seas.[88] Two relate to crimes against internationally protected persons and the taking of hostages.[89] Two others, including the most recent, relate to nuclear material and terrorism.[90] One relates to plastic explosives and another to terrorist bombings.[91] One of the more recent conventions relates to the financing of terrorism.[92] Canada has committed itself to the prevention of terrorism as a key component of its national security and public safety strategy.

Notes

1 Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Freedom and Security under the Law*, Second Report, vol. 1 (Ottawa: Supply and Services Canada, 1981), p. 44, para. 19 (Chair; D.C. McDonald) [McDonald Commission report, vol. 1].

2 *Re s. 83.28 of the Criminal Code,* [2004] 2 S.C.R. 248 at para. 7.

3 *Suresh v. Canada (Minister of Citizenship and Immigration)*, [2002] 1 S.C.R. 3 at para. 4.

4 R.S.C. 1985, c. C-23 [*CSIS Act*].

5 The definition is broad and, as discussed below, encompasses grey areas. The specific activities included in the definition are discussed in more detail throughout this chapter.

6 The history and background set out in this chapter are based largely on the McDonald Commission report. The primary purpose of the background information is to provide context. As such, I did not consider it an efficient use of resources to undertake extensive research in this regard. More detail on the topics discussed in this section can be found in Part I, Chapter 2 (vol. 1), and Part VI, Chapter 1 (vol. 2), of the McDonald Commission report.

7 For the purposes of this report, I adopt the distinction between "information" and "intelligence" used by the RCMP. The RCMP *Operational Manual* provides that information is unprocessed data that may be used in the production of intelligence. Intelligence is the end product of information that has been subject to the intelligence process, which involves collection, evaluation, collation, analysis reporting and dissemination. (See Exhibit P-12, Tab 32A, Arar Commission Factual Inquiry.)

8 The Fenian Brotherhood was an American organization of mainly Irish and Irish Americans. The organization's primary goal was the separation of Ireland from Great Britain. In support of this goal, factions of the Fenian Brotherhood favoured an invasion of Canada (or British North America, as it then was). Indeed, such an invasion was attempted in 1866.

9 Until 1920 the RCMP was known as the Royal North-West Mounted Police, but will be referred to throughout this section as the RCMP.

10 McDonald Commission Report, vol. 1, p. 58, para. 36.

11 In 1945, Igor Gouzenko, a cypher clerk in the Soviet Union's Ottawa embassy, defected to Canada with documentary evidence of an extensive Soviet spy ring operating in Canada. The ring included Canadian civil servants and scientists who passed information important to the defence of Canada to the Soviet Union.

12 The *Official Secrets Act* was renamed the *Security of Information Act* (R.S.C. 1985, c. O-5) in 2001. (See the *Anti-terrorism Act*, S.C. 2001, c. 41.)

13 The *Official Secrets Act* was first enacted in 1890 and substantially revised in 1939. Until it was amended in 2001 to include prohibitions against communications to further terrorist activities, the *Official Secrets Act* focused on wrongful communications with and unauthorized use of Canadian government information by foreign powers.

14 During the Munich Olympics, terrorists claiming to be from Black September, a Palestinian guerrilla group, entered the Olympic Village, killed two Israelis and took nine hostages. By the time the incident ended, all the hostages, five of the captors and two West German police officers had been killed.

15 McDonald Commission report, vol. 1, p. 68.

16 *House of Commons Debates*, March 7, 1966, v. III, p. 2297.

17 Canada, MacKenzie Commission, *Report of the Royal Commission on Security* (Abridged) (Ottawa: The Queen's Printer, 1969), p. 105, para. 297 (Chair: M.W. MacKenzie [MacKenzie Commission report].

18 Ibid., p. 109, para. 299.

19 Ibid., p. 110, para. 299(d).

20 See further discussion on police independence in Chapter IX.

21 *House of Commons Debates*, June 26, 1969, p. 10637.

22 See the McDonald Commission Report, vol. 1, p. 7 on.

23 Journalistic accounts of the public scandals surrounding the RCMP include John Sawatsky, *Men in the Shadows: The RCMP Security Service* (Toronto: Doubleday, 1980) and Jeff Sallot, *Nobody Said No* (Toronto: Lorimer, 1979). See also Reg Whitaker, "Canada: the RCMP scandals," in Andrei S. Markovits and Mark Silverstein, eds., *The Politics of Scandal: Power and Process in Liberal Democracies* (New York: Holmes & Meier, 1988), pp. 38–61.

24 In 1965–1966, the Solicitor General replaced the Minister of Justice as the minister responsible for the RCMP.

25 McDonald Commission report, vol. 1, p. 75, para. 96.

26 Quebec, Department of Justice, *Report of the Commission of inquiry into police operations on Québec territory* (Quebec: Department of Justice, 1981) (Chair: Jean F. Keable).

27 Order in Council PC 1977-1911, Canada Gazette, 6 July 1977.

28 McDonald Commission report, vol. 1, pp. 445–513, 599–604.

29 Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Freedom and Security under the Law*, Second Report, vol. 2 (Ottawa: Supply and Services Canada, 1981), p. 754 (Chair: D.C. McDonald) [McDonald Commission report, vol. 2].

30 McDonald Commission report, vol. 1, p. 613, para. 2.

31 McDonald Commission report, vol. 2, pp. 755–756.

32 Ibid., p. 757, para. 11. See also the background paper "Police Independence."

33 McDonald Commission report, vol. 2, p. 756, para. 9.

34 Ibid., p. 758, para. 15.

35 Ibid., p. 759.

36 Ibid., p. 882.

37 Ibid., p. 883.

38 Ibid., p. 884, para. 10.

39 Ibid., p. 884, para 11.

40 Ibid., p. 888.

41 Ibid., p. 885.

42 Ibid., p. 898, para 40.

43 Ibid., p. 899, para. 43.

44 Ibid., p. 985, para. 49.

45 See also the background paper "Domestic Models of Review of Police Forces."

46 R.S.C. 1985, c. S-7.

47 Ibid., c. R-10 [*RCMP Act*].

48 Pursuant to subsection 91(27) of the *Constitution Act*, the federal government has the responsibility for formulating criminal law and procedure. The courts have interpreted this to include the power of enforcement (including the power to create police forces to do so.) Indeed, the federal enforcement power extends to the enforcement of all federal legislation. It is important to note that subsection 92(14) of the *Constitution Act, 1867* provides that the provinces have responsibility for the "administration of justice," which also includes the power to enforce the criminal law. In cases of conflicts between the exercise of these powers, the doctrine of paramountcy would apply and the federal exercise of power would prevail. See for example *O'Hara v. British Columbia*, [1987] 2 S.C.R. 591; *Reference re Adoption Act (Ontario)*, [1938] S.C.R. 398; *Di Iorio v. Montreal (City) Common Jail*, [1978] 1 S.C.R. 152. The enforcement of the *Criminal Code* has evolved so that the provinces enforce most aspects of the Code, but some such offences are reserved for the RCMP. The provinces do not enforce non-criminal federal offences, such as those found in the *Narcotic Control Act*, R.S.C. 1985, c. N-1; the *Income Tax Act*, R.S.C. 1985, c. 1 (5th Supp.); or *the Official Secrets Act*. For a discussion, see Peter W. Hogg, *Constitutional Law of Canada*, 2nd ed., (Toronto: Carswell, 1999) pp. 425–430.

49 For example, the *Security Offences Act*. (See discussion in next section.)

50 Loeppky testimony, Arar Commission Factual Inquiry Public Hearing (June 30, 2004), p. 701; "Organization of the RCMP," online, RCMP, http://www.rcmp.ca/html/organi_e.htm (accessed July 11, 2006) [RCMP, "Organization of the RCMP"].

51 "Corporate Facts," online, RCMP, http://www.rcmp-grc.ca/factsheets/pdfs/corporate_.pdf (accessed July 11, 2006) [RCMP, "Corporate Facts"]. See also the RCMP's *Report on Plans and Priorities 2003–2004*, p. 25, online, http://www.rcmp.ca/pdfs/rpp_2003_e.pdf (accessed July 11, 2006).

52 The "Minister" was the Solicitor General and is now the Minister of Public Safety.

53 Exhibit P-12, Tab 21, Arar Commission Factual Inquiry. See also the discussion of the Minister's role concerning the RCMP in light of the doctrine of police independence in Chapter IX.

54 *RCMP Act*, s. 6.

55 RCMP, "Organization of the RCMP" (see note 50). See also Loeppky testimony (June 30, 2004), pp. 722–723, June 30, 2004.

56 RCMP, "Corporate Facts" (see note 51).

57 Set out in s. 2 of the *CSIS Act*.

58 As discussed in Chapter III, the *Official Secrets Act* (now called the *Security of Information Act*) has been significantly expanded by the *Anti-terrorism Act* to cover various forms of prohibited assistance to terrorist groups.

59 Defined in s. 2 of the *Criminal Code* as a foreign head of state, minister of foreign affairs or other representative of states and international organizations, and the family members who accompany such persons on foreign trips.

60 *Criminal Code*, R.S.C. 1985, c. C-46, paras. 185(1)(*b*), 186(1)(*b*).

61 Ibid., c. C-46, ss. 494–495, 511, 529.1–5.

62 Ibid., ss. 810–810.2.

63 *An Act to amend the Criminal Code (organized crime and law enforcement) and to make consequential amendments to other acts*, S.C. 2001, c. 32.

64 *Criminal Code*, s. 25.1(8).

65 Ibid., subss. 25.1(9), (10), (11).

66 Loeppky Testimony (June 30, 2004), pp. 742–743, 747–749.

67 Ibid., p. 745.

68 Exhibit P-12, Factual Inquiry, Tab 42, p. 1.

69 "Intelligence-Led Policing: A Definition," online, RCMP, www.rcmp-grc.gc.ca/crimint/intelligence_e.htm; Exhibit P-12, Tab 16, Arar Commission Factual Inquiry.

70 Indeed, before the events of 9/11, the core of the RCMP's intelligence activities seem to have been more clearly linked to its mandate on organized crime.

71 See Peter Gill, "Rounding Up the Usual Suspects: Developments in Contemporary Law Enforcement Intelligence" (Alderstet: Ashgate, 2000).

72 Exhibit P-12, Tab 20, p. 48, Arar Commission Factual Inquiry.

73 The two types of intelligence have also been referred to by the courts (see for example the decision of the Supreme Court of Canada in *Canada (Minister of Employment and Immigration) v. Chiarelli*, [1992] 1 S.C.R. 711 at 744) and in legislation (see for example the *Charities Registration (Security Information) Act,* S.C. 2001, c. 41, and the *Immigration and Refugee Protection Act,* S.C. 2001, c. 27.

74 I note that the Department of National Defence refers to the intelligence it collects as "military intelligence." This term similarly relates to that department's mandate.

75 See Loeppky testimony (June 30, 2004), pp. 784–785; (July 6, 2004), pp. 1289–1290.

76 Exhibit P-12, Tab 44, p. 19, Arar Commission Factual Inquiry.

77 Four of the 14 NSISs were converted to INSETs after 9/11.

78 Exhibit P-12, Tab 42, p. 13, Arar Commission Factual Inquiry.

79 Exhibit P-12, Tab 49, Arar Commission Factual Inquiry.

80 After the research in the Policy Review was completed, but before this Report was published, the RCMP and CSIS signed a new Memorandum of Understanding. The 2006 MOU is, like its predecessor, focussed on cooperation between the two organizations and in particular on the exchange of information. One of the most significant differences is that the 2006 MOU provides for the creation of a committee at the senior level of both organizations, the primary role of which is to "coordinate the investigations of both agencies through meaningful, timely and ongoing exchange of information, and by: (a) developing a common counter-terrorism overview and priorities; and (b) developing joint training to ensure that personnel in both counter-terrorism programs are trained to common standards with common understandings of roles and policies". Significantly, the MOU continues to recognize the important differences in the roles of the RCMP and CSIS in regard to national security. In general terms each agency agrees to provide the other with information and intelligence in its possession relating to the "assigned security related responsibilities" of the other agency. As in the previous MOU, it is specifically provided that nothing in it shall be interpreted as compelling either party to disclose the identity of its sources or caveated information from a third party.

81 As noted above, these responsibilities were defined as the prevention, detection, investigation and laying of charges in relation to any offence referred to in s. 2 of the *Security Offences Act*, or the apprehension of the commission of such an offence included in the *Criminal Code*, *Official Secrets Act* or any other federal statute having a national security dimension; the protective security measures to safeguard VIPs, federal properties, airports and vital points from security offences or threats; the provision of advice to departments and agencies of

government respecting protective security measures; and the consolidation of threat assessments from CSIS and other sources to provide appropriate protection to VIPs and for special events.

82 Loeppky testimony (July 6, 2004), p. 1141. Deputy Commissioner Loeppky testified that such assistance would be provided if CSIS was "absolutely strapped."

83 The Hon. Bob Rae, *Lessons to be Learned* (Ottawa: Air India Review Secretariat, 2005), p. 2.

84 Ibid., p. 6.

85 Ibid., p. 23.

86. *Convention on Offences and Certain Other Acts Committed on Board Aircraft*, 14 September 1963, 704 U.N.T.S. 219, online, http://untreaty.un.org/English/Terrorism/Conv1.pdf (accessed July 11, 2006); *Convention for the Suppression of Unlawful Seizure of Aircraft*, 16 December 1970, 860 U.N.T.S. 105, online, http://untreaty.un.org/English/Terrorism/Conv2.pdf (accessed July 11, 2006); *Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation*, 23 September 1971, 974 U.N.T.S. 177, online, http://untreaty.un.org/English/Terrorism/Conv3.pdf (accessed July 11, 2006).

87 *Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation* (supplementary to the *Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation*), 24 February 1988, online, http://untreaty.un.org/English/Terrorism/Conv7.pdf (accessed July 11, 2006).

88 *Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation*, 10 March 1988, 1678 U.N.T.S. 201, online, http://untreaty.un.org/English/Terrorism/Conv8.pdf (accessed July 11, 2006); *Protocol to the Convention for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf*, 10 March 1988, 1678 U.N.T.S. 201, online, http://untreaty.un.org/English/Terrorism/Conv8.pdf (accessed July 11, 2006).

89 *Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, Including Diplomatic Agents*, 14 December 1973, 1035 U.N.T.S. 167, online, http://untreaty.un.org/English/Terrorism/Conv4.pdf (accessed July 11, 2006); *International Convention Against the Taking of Hostages*, 17 December 1979, 1316 U.N.T.S. 205, online, http://untreaty.un.org/English/Terrorism/Conv5.pdf (accessed July 11, 2006).

90. *Convention on the Physical Protection of Nuclear Material* (with annexes), 3 March 1980, 1456 U.N.T.S. 101, online, http://untreaty.un.org/English/Terrorism/Conv6.pdf (accessed July 11, 2006); *International Convention for the Suppression of Acts of Nuclear Terrorism*, 14 September 2005, A/RES/59/290, online, http://untreaty.un.org/English/Terrorism/English_18_15.pdf (accessed July 11, 2006).

91 *Convention on the Marking of Plastic Explosives for the Purpose of Detection,* 1 March 1991, U.S. Treaty Doc. 103-8, online, http://www.unodc.org/unodc/en/terrorism_convention_plastic_explosives.html (accessed July 11, 2006); *International Convention for the Suppression of Terrorist Bombings*, 15 December 1997, A/RES/52/164, online, http://untreaty.un.org/English/Terrorism/Conv11.pdf (accessed July 11, 2006).

92 *International Convention for the Suppression of the Financing of Terrorism*, 9 December 1999, online, http://untreaty.un.org/English/Terrorism/Conv12.pdf (accessed July 11, 2006).

III

Legislative Changes Following the Terrorist Attacks of September 11, 2001

1. INTRODUCTION

The terrorist attacks of September 11, 2001 gave rise to significant changes in the way the federal government responds to threats to the security of Canada.

In this chapter, I focus on the post-9/11 legislative changes of particular relevance to the RCMP's national security activities: the creation of a number of new national security offences; new police powers designed to assist the RCMP in carrying out its national security activities; enhanced provisions for safeguarding information the disclosure of which would harm national security; and an increased emphasis on co-operation and integration among agencies, both foreign and domestic, particularly in regard to the sharing of information relating to terrorism.

2. NEW OFFENCES

The federal response to the events of 9/11 included the creation of a number of new national security offences. The changes were, for the most part, contained in the *Anti-terrorism Act*, which I discuss below.

2.1 *ANTI-TERRORISM ACT*

The *Anti-terrorism Act*[1] created measures to deter, disable, identify, prosecute, convict and punish terrorist groups and to prevent and punish the financing, preparation, facilitation and commission of acts of terrorism. It also provided law enforcement agencies with new preventive and investigative tools and established stronger laws against hate crimes and propaganda. Government of

Canada training material on the Act described its purpose and operational impact as follows:

> A key element of Canada's *Anti-terrorism Act* is prevention. The focus on prevention is something of a cultural shift for our law enforcement community. It places the emphasis on the collection of intelligence, rather than the investigation of crimes that have already occurred.[2]

The Act amended the *Criminal Code*, *Official Secrets Act* (renamed the *Security of Information Act*), *Canada Evidence Act*, and *Proceeds of Crime (Money Laundering) Act* (renamed the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*), as well as the *National Defence Act* as it related to the activities and review of the Communications Security Establishment. It also enacted the *Charities Registration (Security Information) Act*. In this chapter, I focus on the new offences created by the *Anti-terrorism Act*, as they most directly affect the RCMP's responsibilities to prevent and investigate crime and its national security activities.

2.2
NEW DEFINITIONS: TERRORIST ACTIVITY AND TERRORIST GROUP

The *Anti-terrorism Act* added Part II.1, "Terrorism," to the *Criminal Code*. Significant changes included an expansive definition of "terrorist activity," a new definition of "terrorist group" and new terrorism offences.

The definition of "terrorist activity" in the *Criminal Code* does not in itself create a crime, but it is incorporated into new offences and new police powers. A terrorist activity is defined in part as an act or omission committed in or outside Canada that, if committed in Canada, would constitute one of various offences under subsections 7(2) through 7(3.37) of the *Criminal Code*.[3] This definition is designed to implement various international law instruments in relation to hijacking and damage to aircraft and ships, the taking of hostages, use of nuclear material, crimes against internationally protected persons, terrorist bombings and terrorist financing.

In addition, a "terrorist activity" is an act or omission that is committed within or outside Canada

- in whole or in part for a political, religious or ideological purpose, objective and cause
- with the intent of intimidating the public or a segment of the public with regard to its security, including its economic security, or compelling a

person, government, or domestic or international organization to do or to refrain from doing any act

and

- intentionally causes death or serious bodily harm by the use of violence, intentionally endangers a person's life, intentionally causes a serious risk to the health or safety of the public or any segment of the public or intentionally causes substantial property damage that is likely to seriously harm or endanger a person or cause a serious risk to public health or safety, or
- intentionally causes serious interference with or disruption of an essential public or private service, facility or system other than as a result of advocacy, protest, dissent or stoppage of work not intended to harm or endanger a person or pose a serious risk to public health and safety.[4]

The fact of expressing political, religious or ideological thought, belief or opinion alone is not a "terrorist activity" unless it constitutes an act or omission that satisfies the above criteria.[5] A "terrorist activity" includes a conspiracy, attempt or threat to commit any of the above acts or omissions, counselling or procuring a person to commit any such acts, and being an accessory after the fact in relation to any such acts or omissions.

Another important definition that is incorporated into many of the new offences is the following definition of a "terrorist group":

- an entity that has as one of its purposes or activities facilitating or carrying out any terrorist activity (and includes an association of such entities), or
- an entity that has been listed by the Governor in Council on the basis that there are reasonable grounds to believe that it has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity or that it is knowingly acting on behalf of, at the direction of or in association with such an entity (listed entity).

A listed entity may include a person, group, trust, partnership, fund or unincorporated association or organization. The Governor in Council has so far listed 39 groups, pursuant to section 83.05 of the *Criminal Code*.[6]

2.3
NEW TERRORISM OFFENCES

The *Anti-terrorism Act* also created the following new terrorism offences under the *Criminal Code*:

- knowingly participating in or contributing to, directly or indirectly, any activity of a terrorist group for the purpose of enhancing the ability of a terrorist group to facilitate or carry out terrorist activities — this may include recruiting, providing or receiving training, or entering or remaining in any country for the benefit or at the direction of or in association with any terrorist group; the offence may be committed regardless of whether any terrorist activity was facilitated, whether the participation actually enhanced the ability to carry out a terrorist activity, or whether the accused knew the specific nature of any terrorist activity;
- knowingly facilitating a terrorist activity, regardless of whether the person knows that a particular terrorist activity was planned, whether any particular terrorist activity was foreseen or planned when facilitated, or whether it was actually carried out;
- committing any indictable offence for the benefit or at the direction of, or in association with a terrorist group;
- knowingly instructing another person to carry out any activity for the purpose of enhancing the ability of any terrorist group to carry out a terrorist activity, regardless of whether the activity instructed is carried out, a particular person is instructed to carry it out, the person knows that the activity being instructed will benefit a terrorist group, or the activity actually enhances the ability of a terrorist group to facilitate or carry out a terrorist activity;
- knowingly instructing another person to carry out a terrorist activity, regardless of whether the terrorist activity is carried out, a particular person is instructed to carry it out, or the person knows that the activity being instructed is a terrorist activity; and
- knowingly harbouring or concealing someone he or she knows has carried out or is likely to carry out a terrorist activity, for the purpose of enabling the person to facilitate or carry out any terrorist activity.[7]

2.4
NEW TERRORIST FINANCING OFFENCES

The *Anti-terrorism Act* also created a number of new offences respecting the financing of terrorism, as follows:

- wilfully and without lawful justification or excuse providing or collecting property, either directly or indirectly, intending that it be used or knowing that it will be used to carry out certain terrorist activities or acts intended to cause death or serious bodily harm to a civilian for the purpose of intimidating the public or compelling a government or international organization to do or refrain from doing any act;
- collecting, providing, inviting to provide, or making available property or financial services knowing that they will be used by or will benefit a terrorist group or intending or knowing that they will be used for the purpose of facilitating a terrorist activity or for benefiting any person who is facilitating or carrying out a terrorist activity;
- using or possessing property for the purpose of facilitating or carrying out a terrorist activity or possessing property intending or knowing that it will be used, directly or indirectly, in whole or in part, for the purpose of facilitating or carrying out a terrorist activity;
- for a person in Canada or a Canadian outside Canada, knowingly dealing with property owned or controlled by a terrorist group or providing financial or other related services in relation to such property for the benefit or at the direction of a terrorist group;
- for a person in Canada or a Canadian outside Canada, failing to disclose forthwith to the RCMP Commissioner and the Director of CSIS property in his or her possession or control that he or she knows is owned or controlled by a terrorist group or information about a transaction or proposed transaction in respect of such property; and
- for various financial institutions, failing to report monthly on whether or not they are in possession or control of property owned or controlled by a listed entity.[8]

2.5
DEFINITION OF TERRORISM OFFENCES

The definition of terrorism offences in section 2 of the *Criminal Code* includes not only the new terrorism and financing of terrorism offences set out above, but also any indictable offence committed for the benefit of, at the direction of or

in association with a terrorist group. Although a robbery or a fraud would not normally be a terrorist offence, it could be, if one of the above circumstances applied. Terrorism offences as defined in the *Criminal Code* moreover include indictable offences that also constitute terrorist activity as defined in the Code. An example would be a murder or other act of violence that satisfies the definition of a terrorist activity discussed above.

The Supreme Court has affirmed that terrorism offences as defined in the *Criminal Code* include offences, such as murder, that existed before the enactment of the *Anti-terrorism Act* in 2001. Justices Iacobucci and Arbour have expressed agreement with the "characterization of a 'terrorism offence' as 'a descriptive compendium of offences created elsewhere in the *Criminal Code*.'"[9] A terrorism offence is not limited to an offence that incorporates or satisfies the definition of terrorist activity added to the Code in 2001, but could be almost any indictable offence in the *Criminal Code*, including an attempt, conspiracy, counselling or being accessory after the fact, if the indictable offence is committed for the benefit of, at the direction of or in association with a terrorist group or if it would constitute terrorist activity as broadly defined in section 83.01 of the Code.

2.6
FORFEITURE ORDERS AND TERRORIST FINANCING OFFENCES

The Attorney General of Canada now has the power under sections 83.13 and 83.14 of the *Criminal Code* to seize and forfeit property that is owned or controlled by a terrorist group or that has been or would have been used to facilitate or carry out a terrorist activity. Search warrants and restraint orders are obtained from a Federal Court judge, who examines applications in private and issues warrants or restraint orders if there are reasonable grounds to believe that forfeiture orders may be made.[10]

2.7
CONSENT OF PROVINCIAL OR FEDERAL ATTORNEY GENERAL

The consent of either the provincial or the federal Attorney General is required to commence proceedings in respect of a terrorism offence.[11] Although most crimes are prosecuted provincially, the *Anti-terrorism Act* amended the *Criminal Code* to give the Attorney General of Canada concurrent jurisdiction for prosecuting offences relating to terrorism and certain offences pertaining to internationally protected persons.[12] Similarly, under the *Security Offences Act*, the Attorney General of Canada may choose to prosecute an offence that would

otherwise be prosecuted by a provincial attorney general where it involves a threat to the security of Canada or an internationally protected person.[13]

2.8
OTHER NEW OFFENCES

In addition to broadening the definition of first-degree murder to include causing death during terrorist activities[14] and also amplifying the definition of a threat against an internationally protected person,[15] the *Anti-terrorism Act* added the following offences to the *Criminal Code*: threats against United Nations personnel or attacks on them, hate-motivated mischief relating to religious property, and the placement of explosives or other lethal devices in public places.[16]

The *Public Safety Act* also added a new terrorism offence to the *Criminal Code*, that of perpetrating a hoax regarding terrorist activity, which covers a person causing a reasonable apprehension that terrorist activity is occurring or will occur, without believing in its truth and with the intent of causing a person to fear death, bodily harm, or substantial damage to or interference with property.[17] As with other terrorism offences, the consent of the federal or provincial Attorney General is required to commence proceedings in relation to such hoaxes.

2.9
SECURITY OF INFORMATION ACT

The *Anti-terrorism Act* substantially amended the *Official Secrets Act* and renamed it the *Security of Information Act*. Before the 2001 amendments, neither terrorist groups nor terrorist activities were subject to the Act, which focused on foreign states. Now, the *Security of Information Act* is an important piece of the legislative framework for national security, covering terrorist groups and non-state entities, as well as foreign entities. Moreover, the definition of a foreign entity now includes governments in waiting, governments in exile, and associations of foreign governments, governments in waiting, or governments in exile with one or more terrorist groups. The Act uses the definitions of "terrorist group" and "terrorist activity" found in the *Criminal Code*.

The Act moreover provides a new and comprehensive definition of "a purpose prejudicial to the safety or interests of the State,"[18] which includes the following:

- offences against the laws of Canada for a political, religious or ideological purpose or to benefit a foreign entity or terrorist group;
- a terrorist activity inside or outside Canada;

- endangerment of life, health or safety;
- interference with public or private services or computer programs in a manner that has a significant adverse impact on health, safety, security or economic or financial well-being of the people or the functioning of any government;
- damage to certain persons or property outside Canada;
- impairment of or interference with the Canadian Forces;
- impairment of Canadian security and intelligence capabilities;
- impairment of Canadian responses to economic threats or instability;
- impairment of Canadian diplomatic or consular relations or international negotiations;
- use of toxic, radioactive or explosive devices, contrary to international treaty; and
- an act or omission in preparation of the undertaking of any of the above activities.

The phrase "purpose prejudicial to the safety or interests of the State" is incorporated into many offences under the Act, including the offence of wrongfully communicating, using, receiving or retaining confidential or other information.[19]

The following are offences under the Act: unauthorized use of uniforms, falsification of reports, forgery, impersonation and use of false documents for the purpose of gaining admission to a prohibited place or for any other purpose prejudicial to the safety or interests of the State.[20] It is also an offence under the Act to approach or pass over a prohibited place for any purpose prejudicial to the safety or interests of the State at the direction or for the benefit of, or in association with a foreign entity or terrorist group.[21] The Act moreover has complex provisions relating to individuals bound to secrecy that create offences for leaks and establish a limited public interest defence.[22]

Other offences target the communication, without lawful authority, of various forms of safeguarded information to a foreign entity or a terrorist group, and the actual or attempted inducement of any person, by threat, accusation or menace, to do anything that will harm Canadian interests or increase the capacity of a foreign entity or terrorist group to harm Canadian interests.[23] The threat, accusation, menace or violence in question need not occur in Canada.

It is also an offence for a person to knowingly harbour or conceal someone he or she knows has committed an offence under the Act, or is likely to do so, for the purpose of enabling or facilitating an offence under the Act.[24]

The Act further provides that it is an offence to do anything specifically directed towards or done in preparation of the commission of certain offences,[25] including the following:

- entering Canada at the direction of or for the benefit of a foreign entity or terrorist group;
- obtaining, retaining or gaining access to any information;
- knowingly communicating to a foreign entity or terrorist group a willingness to commit the offence;
- asking a person to commit the offence, at the direction of a foreign entity or terrorist group; and
- possessing any device or software useful for concealing the content of information or for covertly communicating information.

Liability for all offences under the Act is extended to persons who conspire or attempt to commit such offences, counsel in relation to such offences or are accessories after the fact.[26] Moreover, when committed by certain persons, including Canadian citizens, acts or omissions outside Canada that would be offences under the Act if committed in Canada are deemed to have been committed in Canada.[27]

As with terrorism offences, the consent of the Attorney General of Canada is required for any prosecution.[28] This limits normal police powers to lay charges.

2.10
PROCEEDS OF CRIME (MONEY LAUNDERING) AND TERRORIST FINANCING ACT

The *Anti-terrorism Act* substantially amended the *Proceeds of Crime (Money Laundering) Act* and renamed it the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. The amended Act provides for both new terrorist financing offences relevant to national security investigations and new powers for information sharing between the private sector and government, within government, with the RCMP, and with foreign agencies.

The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* defines "terrorist activity financing offence" as an offence under section 83.02, 83.03 or 83.04 of the *Criminal Code* or under section 83.12 of the Code arising out of a contravention of section 83.08 of the Code. "Terrorist activity" has the same meaning as in the *Criminal Code* and "threat to the security of Canada," the same meaning as in section 2 of the *Canadian Security Intelligence Service Act*.

The stated objects of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* are as follows:

a) to implement specific measures to detect and deter money laundering and the financing of terrorist activities and to facilitate the investigation and prosecution of money laundering offences and terrorist activity financing offences, including
   i. establishing record keeping and client identification requirements for financial services providers and other persons or entities that engage in businesses, professions or activities that are susceptible to being used for money laundering or the financing of terrorist activities;
   ii. requiring the reporting of suspicious financial transactions and of cross-border movements of currency and monetary instruments; and
   iii. establishing an agency that is responsible for dealing with reported and other information.

b) to respond to the threat posed by organized crime by providing law enforcement officials with the information they need to deprive criminals of the proceeds of their criminal activities, while ensuring that appropriate safeguards are put in place to protect the privacy of persons with respect to personal information about themselves; and

c) to assist in fulfilling Canada's international commitments to participate in the fight against trans-national crime, particularly money laundering, and the fight against terrorist activity.[29]

Part 1 of the Act focuses on record keeping and reporting of suspicious and prescribed financial transactions. It stipulates that entities such as banks, credit unions and certain other companies or persons must report every financial transaction in respect of which there are reasonable grounds to suspect that the transaction is related to a money laundering or terrorist activity financing offence to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). I discuss this further below. They must also report certain other transactions to FINTRAC, including international electronic fund transfers over $10,000 and large cash transactions over $10,000.

Part 2 focuses on the cross-border movement of currency and monetary instruments. It imposes reporting duties and provides for searches of persons, conveyances, baggage and mail on the basis of reasonable suspicion of unreported currency. It also contains forfeiture provisions.

Part 3 deals with FINTRAC, an independent agency established in 2000 that is at arm's length from law enforcement agencies and other entities to which it is authorized to disclose information. I examine the role of FINTRAC in the

national security landscape in greater detail in Chapter V. After analyzing and assessing reports and information, FINTRAC is required to disclose "designated information" to the appropriate police force if it has reasonable grounds to suspect that the information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence.[30] Where FINTRAC has reasonable grounds to suspect that designated information would be relevant to threats to the security of Canada, it is required to disclose that information to CSIS.[31] "Designated information" as defined in the Act is limited information relating to a financial transaction or an importation or exportation of currency or monetary instruments, such as names, addresses, amounts and account numbers.[32] FINTRAC must record its reasons in writing for disclosing information to a police force.[33] As I discuss in Chapter V, FINTRAC may also disclose certain information to institutions or agencies of foreign governments or international organizations that have powers or duties similar to its own.

The Act sets out the procedure under which the Attorney General may apply for a production order for the purposes of a money laundering or terrorist financing investigation.[34] CSIS may also apply to a judge for the disclosure of information to enable it to investigate a threat to the security of Canada after obtaining the approval of the Minister of Public Safety. These applications are heard in private.[35]

Part 4 of the Act focuses on regulations and Part 5 deals with offences and punishment. There are exemption provisions in respect of peace officers or persons acting under the direction of peace officers who commit certain offences under the act if they are committed for the purpose of investigating a money laundering offence or a terrorist activity financing offence.[36]

2.11
UNITED NATIONS SUPPRESSION OF TERRORISM REGULATIONS

Canada's *United Nations Suppression of Terrorism Regulations* were enacted on October 2, 2001 pursuant to the *United Nations Act*. They establish a list of persons who there are reasonable grounds to believe have carried out, attempted to carry out or participated in or facilitated the carrying out of a terrorist activity. Important aspects include:

- prohibitions on the provision and collection of funds for the use of a listed person by any person in Canada or any Canadian outside Canada, or the assistance or promotion of such activities;[37]
- prohibitions on knowingly dealing directly or indirectly in any asset owned or controlled by a listed person, or assisting or promoting such activity;[38]

- a duty for financial institutions to determine whether they are in possession or control of assets owned by a listed person and to disclose any such assets; and
- a requirement for persons in Canada and Canadians outside Canada in possession or control of assets they believe are owned or controlled by a listed person to disclose this information to the RCMP or CSIS.

Like the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, the Regulations provide for means by which the RCMP may receive information relevant to national security investigations and offences that could be charged in national security investigations.

3. NEW POLICE POWERS

The *Anti-terrorism Act* provides the police, including the RCMP, with new powers in relation to terrorism investigations. I note that, in a recent decision, the Supreme Court indicated that the purpose of one of these new powers, the investigative hearing, should be the prevention and prosecution of terrorism offences and not the broader protection of national security.[39]

3.1 INVESTIGATIVE HEARINGS

The *Criminal Code* provides for a procedural mechanism to gather information for investigating or preventing terrorism offences from persons believed on reasonable grounds to have relevant information.[40] On the consent of the Attorney General, a peace officer may apply to a judge in private for an order directing individuals with information relevant to an ongoing investigation of a terrorism offence to appear before a judge and provide information.

Investigative hearings may be ordered where the judge is satisfied of the following:

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

The person named in the order has the right to legal counsel, but must answer questions and produce things as required by the order, subject only to claims of privilege or non-disclosure, which are to be decided by the judge presiding at the investigative hearing. The person has no right to refuse to comply on the ground that it might incriminate him or her, but such information and any evidence derived from it may not be used in current or future criminal proceedings against the person except in prosecutions for perjury or giving contradictory evidence.

The Supreme Court of Canada reviewed this new procedure in proceedings relating to trials arising from the terrorist bombing of Air India Flight 182. In *Application under s. 83.28 of the Criminal Code (Re),* it upheld the constitutionality of the procedure. Speaking for the majority, Justices Iacobucci and Arbour held that the procedure did not violate section 7 of the *Canadian Charter of Rights and Freedoms*. In doing so, the justices relied on the protections in subsection 83.28(10), which provides that compelled evidence or evidence derived from such evidence may not be used against the person in subsequent criminal proceedings. They also indicated that evidence compelled at the investigative hearing should not be used in subsequent extradition and deportation proceedings.[41] The Court noted the important role that the presiding judge and counsel representing the subject of the investigative hearing would play in the procedure. It indicated that section 7 of the Charter would prevent the use of an investigative hearing if the predominant purpose was to determine penal liability. The majority of the Court rejected arguments that the procedure violated judicial independence and impartiality and stressed the important role of the judge in investigative hearings in ensuring the protection of common law, evidentiary and constitutional rights, and the presumption that such hearings should be open.[42]

In the companion case of *Vancouver Sun (Re),*[43] the Court held that there is a rebuttable presumption that investigative hearings should be held in open court, with the burden of demonstrating the need for secrecy resting on the government.[44] However, the Court agreed that the application for a judge to authorize an investigative hearing must be heard in private.[45]

Under the *Criminal Code*, federal and provincial attorneys general are required to prepare annual reports on the use of investigative hearings,[46] although such reports must not reveal any confidential national security information. The RCMP and the federal Department of Justice reported no investigative hearings from December 24, 2001 to December 23, 2005. Only one application to conduct such a hearing was made, retrospectively, with respect to the Air India matter. However, the investigative hearing was not actually held.[47]

3.2
RECOGNIZANCE WITH CONDITIONS (PREVENTIVE ARREST)

The *Anti-terrorism Act* also created a new power of "preventive arrest." Different provisions govern arrest with warrant and arrest without warrant. A recognizance (peace bond) with conditions may then be imposed by a judge to prevent terrorist activity.

With regard to preventive arrest with warrant, the *Criminal Code* states that, with the consent of the Attorney General, a police officer, who

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

may lay an information under oath before a provincial court judge. The judge may then compel the person named to appear before the judge.[48]

In order to make a preventive arrest without warrant, a peace officer must have a reasonably grounded suspicion that detention of the person is necessary to prevent a terrorist activity, and one of the following requirements must be met:

- the conditions for the laying of an information exist but exigent circumstances make it impracticable to do so; or
- an information has already been laid and a summons issued.[49]

If an information has not been laid and the person is subject to arrest without warrant, the police officer is to lay an information and obtain the consent of the Attorney General without unreasonable delay, within a period of 24 hours or as soon as possible, unless the person has been released.

The person detained in custody must be taken before a provincial court judge within 24 hours or as soon as possible.[50] A show cause hearing must be held to determine if further detention is necessary to ensure the person's appearance before a judge, prevent a terrorist activity or interference with the administration of justice, or for any other just cause, including maintaining confidence in the administration of justice.[51] The matter may be adjourned by a judge, but only for a maximum of a further 48 hours if the person is not released.

If satisfied that there are reasonable grounds for suspecting that the imposition of a recognizance is necessary to prevent a terrorist activity, the judge

may order that the person enter into a recognizance to keep the peace for a period not exceeding 12 months and to comply with other reasonable conditions. Further, if the person refuses to enter into the recognizance, the judge may commit the person to prison for a term not exceeding 12 months.[52]

Federal and provincial attorneys general are required to prepare annual reports on the use of the recognizance with conditions provisions and the ministers responsible for policing at the federal and provincial levels are required to report on the use of the arrest without warrant provisions set out in section 83.3.[53] I note that the RCMP and the federal Department of Justice reported no use of preventive arrests from December 24, 2001 to December 23, 2005.[54]

The *Anti-terrorism Act* also amended section 810.01 of the *Criminal Code* to enable any person who fears on reasonable grounds that another person will commit a terrorism offence to apply, with the consent of the Attorney General, for a recognizance similar in terms to those available under section 83.3. The Attorney General's reporting requirements under section 83.31 do not apply to such peace bonds.

3.3
ENHANCED ELECTRONIC SURVEILLANCE PROVISIONS

The *Anti-terrorism Act* amended the *Criminal Code* to make wiretapping provisions apply to all terrorism offences and to new offences relating to internationally protected persons and explosives. Amendments were also made to except terrorism offences from the requirement pertaining to the actual or likely failure of other less intrusive investigative techniques.[55] Moreover, the authorization period for the interception of communications was increased to one year,[56] and a judge may grant an extension of no more than three years for notifying a person of the electronic surveillance.[57]

3.4
AN ACT TO AMEND THE FOREIGN MISSIONS AND INTERNATIONAL ORGANIZATIONS ACT

This Act provides that the RCMP has primary responsibility for ensuring the security of intergovernmental conferences in which two or more states participate. The RCMP "may take appropriate measures, including controlling, limiting or prohibiting access to any area to the extent and in a manner that is reasonable in the circumstances."[58]

4.
ENHANCED PROTECTIONS FOR NATIONAL SECURITY CONFIDENTIALITY

Part of the federal government's response to the events of 9/11 has been increased legislative protection of information that, if publicly disclosed, would injure national security. This enhanced protection is relevant to my mandate because it may increase the secrecy of the RCMP's national security activities and affect the work of the body that reviews such activities. Amendments to the *Security of Information Act* are discussed above. In this section, I examine the amendments to the *Canada Evidence Act* and to federal privacy and access to information legislation.

4.1
CANADA EVIDENCE ACT

Part 3 of the *Anti-terrorism Act* amended sections of the *Canada Evidence Act*. This Act provides that a government official may object to the disclosure of information before a court, person or body on the grounds of a specified public interest. The appropriate court may authorize or prohibit disclosure after weighing the public interest in disclosure against the importance of the specified public interest.[59] The provisions as originally enacted stated that a hearing or an appeal of an order was to be heard in private. However, in 2004, they were repealed so that, rather than being required to conduct the hearing in private, a court may now exercise its inherent jurisdiction to provide for such a hearing when the need arises.[60]

The Act also deals with the disclosure of sensitive or potentially injurious information in the course of legal proceedings, providing that

> [e]very participant who, in connection with a proceeding, is required to disclose, or expects to disclose or cause the disclosure of, information that the participant believes is sensitive information or potentially injurious information shall, as soon as possible, notify the Attorney General of Canada in writing of the possibility of the disclosure, and of the nature, date and place of the proceeding[61]

and that

> [a]n official, other than a participant, who believes that sensitive information or potentially injurious information may be disclosed in connection with a proceeding may notify the Attorney General of Canada in writing of the possibility of the disclosure, and of the nature, date and place of the proceeding.[62]

"Sensitive information" means:

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

and "potentially injurious information" means:

> information of a type that, if it were disclosed to the public, could injure international relations or national defence or national security.[63]

The Attorney General may apply to the Federal Court for an order with respect to the disclosure of information about which notice was given.[64] Moreover, a person, other than a witness, who is required to disclose information must, in certain circumstances, apply to the Federal Court for an order with respect to disclosure, and a person who is not required to, but wishes to disclose or cause the disclosure of information in connection with a proceeding may apply to the Federal Court for such an order.[65] Applications are confidential and measures may be taken by the court to protect their confidentiality.

Under the Act,

> [u]nless the judge concludes that the disclosure of the information would be injurious to international relations or national defence or national security, the judge may, by order, authorize the disclosure of the information.[66]

Moreover,

> [i]f the judge concludes that the disclosure of the information would be injurious to international relations or national defence or national security but that the public interest in disclosure outweighs in importance the public interest in non-disclosure, the judge may by order, after considering both the public interest in disclosure and the form of and conditions to disclosure that are most likely to limit any injury to international relations or national defence or national security resulting from disclosure, authorize the disclosure, subject to any conditions the judge considers appropriate, of all of the information, a part or summary of the information, or a written admission of facts relating to the information.[67]

Further, "[i]f the judge does not authorize disclosure under subsection (1) or (2), the judge shall, by order, confirm the prohibition of disclosure."[68]

A hearing or an appeal or review of an order made pursuant to any of the above provisions must be heard in private, and the judge or court may give any person who makes representations, and must give the Attorney General (and in

some cases the Minister of National Defence) the opportunity to make representations without the other side being present.[69] The judge or court may make any order deemed appropriate in the circumstances to protect the confidentiality of the information to which the hearing, appeal or review relates.[70] The court records are confidential, and a judge may order that the records be sealed and not be made accessible to the public.

The Attorney General may personally issue a certificate that prohibits the disclosure of information in connection with a proceeding for the purpose of protecting information obtained in confidence from, or in relation to, a foreign entity (as defined in the *Security of Information Act*) or for the purpose of protecting national defence or national security.[71] The certificate may only be issued after an order or decision that would result in the disclosure of the information has been made under an act of Parliament, and expires 15 years after the day on which it was issued.

A party to a proceeding for the purpose of protecting information obtained in confidence from, or in relation to, a foreign entity or for the purpose of protecting national defence or national security may apply to the Federal Court of Appeal for an order varying or cancelling the certificate.[72] The judge who hears the application must make an order to this effect if part or all of the information is found not to relate to information obtained in confidence from or in relation to a foreign entity or to national defence or national security. However, if all of the information subject to the certificate does so relate, the judge must make an order to confirm the certificate. The judge's determination of the matter is final and is not subject to appeal.

The Act recognizes that a criminal trial judge may make any order that is appropriate to protect the right of the accused to a fair trial, such as an order to stay proceedings, provided it complies with a valid certificate prohibiting disclosure of information issued under 38.13, any order authorizing or prohibiting disclosure made under section 38.06, or any judgment made on appeal from or review of such an order.[73]

4.2
ACCESS TO INFORMATION AND PRIVACY LEGISLATION

The *Anti-terrorism Act* amended the *Access to Information Act,*[74] *Personal Information Protection and Electronic Documents Act*[75] and *Privacy Act*,[76] providing that, where a certificate under section 38.13 of the *Canada Evidence Act* prohibiting disclosure of information in a record or of the personal information of a specific individual is issued before a complaint is filed under any of the above acts in respect of a request for access to that information, those acts do

not apply to that information. Moreover, where a section 38.13 certificate is issued after the filing of a complaint under any of those acts, then all proceedings under the acts are discontinued and the Access to Information Commissioner or Privacy Commissioner, as the case may be, must take precautions to ensure that the information is not disclosed and must return the information to the head of the government institution that controls or provided the information.

5.
INCREASED INFORMATION SHARING AND INTEGRATION OF NATIONAL SECURITY ACTIVITIES

Although the RCMP frequently interacted and shared information with other domestic and foreign agencies in the past, the events of 9/11 have led to a sharper focus on information sharing and integrated activities.

A significant number of domestic agencies, both federal and provincial, have a role to play in Canada's response to threats to its national security. As I discuss in chapters IV and V, co-operation between those agencies ranges from information sharing, to joint operations, to full integration, where members from various home agencies work together in an integrated unit. In this section, I describe the domestic and international responses to 9/11 that establish the legal basis for such increased co-operation.

5.1
UNITED NATIONS SECURITY COUNCIL RESOLUTION 1373

The international nature of recent terrorist threats has given rise to greater co-operation among governments in combating terrorism. Shortly after the terrorist attacks of 9/11, the UN Security Council adopted Resolution 1373 calling for suppression of the financing of terrorism and for international co-operation between states. The Resolution, which was adopted under Chapter VII of the Charter of the United Nations, making it binding on all member states, provided important background for changes to Canadian law and policies after 9/11. For example, the preamble to Canada's *Anti-terrorism Act* provides that "Canada must act in concert with other nations in combating terrorism, including fully implementing United Nations and other international instruments relating to terrorism."

Resolution 1373 sets out the following obligations for all states:

- to prevent and suppress the financing of terrorism, and criminalize the willful provision or collection of funds for such acts;

- to freeze the funds, financial assets and economic resources of those who commit or attempt to commit terrorist acts or participate in or facilitate the commission of terrorist acts and of their entities, as well as of persons and entities acting on behalf of or at the direction of terrorists; and
- to prohibit their nationals or any persons and entities within their territories from making funds, financial assets, economic resources, and financial or other related services available to persons who commit or attempt to commit, facilitate or participate in the commission of terrorist acts.[77]

The focus on terrorism financing in Resolution 1373 has resulted in the creation of many new terrorist financing offences in Canada, as well as requirements for financial reporting and information sharing.

The Resolution also addresses support of terrorist acts, imposing the following obligations on all states:

- to refrain from providing any form of support to entities or persons involved in terrorist acts;
- to take the necessary steps to prevent the commission of terrorist acts, including by provision of early warning to other States by exchange of information;
- to deny safe haven to those who finance, plan, support, or commit terrorist acts, or provide safe havens;
- to prevent those who finance, plan, facilitate or commit terrorist acts from using their respective territories for those purposes;
- to ensure that any person who participates in the financing, planning, preparation or perpetration of terrorist acts or in supporting terrorist acts is brought to justice and ensure that such terrorist acts are established as serious criminal offences in domestic laws and regulations;
- to afford one another the greatest measure of assistance in connection with criminal investigations or criminal proceedings relating to the financing or support of terrorist acts; and
- to prevent the movement of terrorists or terrorist groups by effective border controls and controls on issuance of identity and travel documents and through measures for preventing counterfeiting, forgery or fraudulent use of such documents.[78]

Resolution 1373 specifically addresses the need for information sharing, calling upon all states to take the following action:

- find ways to intensify and accelerate the exchange of operational information, especially regarding terrorist movements or actions, false travel

documents, arms and explosives trafficking, trafficking in sensitive materials, and terrorist use of communications technologies and possession of weapons of mass destruction;
- exchange information and co-operate on administrative and judicial matters to prevent terrorist acts;
- co-operate, particularly through arrangements and agreements, to prevent and suppress terrorist attacks and take action against perpetrators of such acts;
- become parties to the relevant international conventions and protocols relating to terrorism;
- increase co-operation and fully implement international conventions and protocols relating to terrorism and Security Council resolutions 1269 and 1368;
- take appropriate steps before granting refugee status to ensure that asylum seekers have not planned, facilitated or participated in the commission of terrorist acts; and
- ensure that refugee status is not abused by the perpetrators, organizers or facilitators of terrorist acts and that political motivation is not recognized as a ground for refusing extradition requests in regard to alleged terrorists.[79]

The link drawn in the Resolution between terrorism and refugee applications suggests that terrorism investigations may involve co-operative efforts by the police and other parts of government, including immigration officials.

A Committee of the Security Council has been set up to monitor implementation of Resolution 1373.[80] Canada has thus far filed five reports with the Committee, outlining its various anti-terrorism efforts and steps taken to implement the Resolution.[81]

5.2
CANADA-U.S. SMART BORDER AGREEMENT

Canada's physical proximity to the United States, the length of the shared border and the two countries' significant economic interdependence have resulted in particular pressures for greater co-operation and interaction between Canadian and American agencies with regard to matters related to terrorism.

In December 2001, Canada and the United States signed the Smart Border Declaration[82] and companion 32-point Action Plan,[83] which includes a number of measures to enhance border security. The Action Plan has four pillars: the secure flow of people, the secure flow of goods, secure infrastructure, and information sharing and coordination in the enforcement of those objectives.

Two of the thirteen action points related to the "secure flow of people" involve sharing advance passenger information and passenger name records (API/PNRs) for flights between Canada and the United States, including in-transit flights, and exploring means of identifying risks posed by passengers on international flights arriving in each other's territory. The two governments plan to establish joint passenger analysis units at key international airports in both countries.

Four of the eight action points under "coordination and information sharing in the enforcement of these objectives" concern joint enforcement coordination, whereby the two governments will work towards ensuring comprehensive and permanent coordination of law enforcement, anti-terrorism efforts and information sharing; integrated intelligence, involving the establishment of joint teams to analyze and disseminate information and intelligence, and the production of threat and intelligence assessments; removal of deportees, whereby the governments will address legal and operational challenges to joint removals and coordinate initiatives to encourage unco-operative countries to accept their nationals; and freezing of terrorist assets, involving the exchange of advance information on designated individuals and organizations in a timely manner.

5.3
NEW DEPARTMENT: PUBLIC SAFETY AND EMERGENCY PREPAREDNESS CANADA

On December 12, 2003, then Prime Minister Paul Martin announced restructuring changes to government on "Securing Canada's Public Health and Safety." The resulting Public Safety and Emergency Preparedness portfolio, headed by the Minister of Public Safety, integrates the activities of the former Department of the Solicitor General, the Office of Critical Infrastructure Protection and Emergency Preparedness (formerly part of the Department of National Defence), the National Crime Prevention Centre (formerly part of the Department of Justice), and the new Canada Border Services Agency, which includes the domestic enforcement units formerly under the Department of Citizenship and Immigration and Canada Customs. The RCMP and CSIS, which were part of the Solicitor General portfolio, come within this new portfolio. In 2005, the *Department of Public Safety and Emergency Preparedness Act* was enacted to codify this reorganization.

The Minister of Public Safety has power over all public safety and emergency preparedness matters within federal jurisdiction that have not been assigned in law to another federal government entity and is required to exercise

leadership relating to public safety and emergency preparedness at the national level.[84] To this end, he or she may coordinate policies with regard to public safety and emergency preparedness, co-operate with any province, foreign state, international organization or other entity, and facilitate the sharing of information, where authorized, to promote public safety objectives.[85]

5.4
NEW NATIONAL SECURITY POLICY

On April 28, 2004, the Government of Canada released a new national security policy entitled *Securing an Open Society: Canada's National Security Policy*.[86] The Policy emphasizes the importance of co-operation among agencies in protecting national security. It identifies three core national security interests: protecting Canada and Canadians at home and abroad, ensuring that Canada is not a base for threats to our allies, and contributing to international security. It focuses on six key security activities: intelligence, emergency planning and management, public health emergency response, transportation security, border security and international security. It contains a commitment to an arm's-length review mechanism for RCMP national security activities and a National Security Committee of Parliamentarians, and articulates the general principle that review should keep pace with the evolving nature of national security activities.

5.5
PUBLIC SAFETY ACT

In 2004, Parliament enacted the *Public Safety Act, 2002*.[87] The main provisions of this lengthy act can usefully be divided into those aimed at enhancing security for sites such as airports and airplanes that are vulnerable to terrorism, and substances such as explosives and toxins that can be used for terrorism; those directed at enhancing information sharing within and between governments; and those dealing with various emergencies.

Several parts of the Act relate to substances that can be used to commit acts of terrorism. Part 7 amends the *Explosives Act* to implement the Organization of American States' *Inter-American Convention against the Illicit Manufacturing of and Trafficking in Firearms, Ammunition, Explosives, and Other Related Materials* as it relates to explosives and ammunition. It prohibits the illicit manufacturing of and illicit trafficking in explosives. It allows for increased control over explosives and provides increased penalties for certain offences.

Part 8 amends the *Export and Import Permits Act* by providing for control over the export and transfer of technology, and authorizes the Minister of

Foreign Affairs to address security concerns when considering applications for permits to export or transfer goods or technology.

Part 23 enacts the *Biological and Toxin Weapons Convention Implementation Act*, which prohibits the possession, use or transfer of certain biological agents or toxins, as well as weapons to deliver such materials, and provides for regulation and inspections for authorized use of such materials.

Several parts of the Act address the security of sites that may be vulnerable to terrorist attacks. Parts 1 and 2 relate to aviation security and the screening of passengers. They create a new offence concerning passengers who are unruly or who jeopardize the safety or security of an aircraft in flight. They also require the provision of information for transportation security purposes and national security purposes and provide a legislative basis for security clearances.

Part 13 amends the *National Defence Act* to allow for the identification and prevention of the harmful unauthorized use of or interference with computer systems and networks of the Department of National Defence or the Canadian Forces, and to ensure protection of those systems and networks.

Part 14 amends the *National Energy Board Act* by extending the powers and duties of the National Energy Board to include matters relating to the security of pipelines and international power lines.

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

Part 11 amends the *Immigration and Refugee Protection Act* to allow for the making of regulations relating to the collection, retention, disposal and disclosure of information for the purposes of that Act. The amendments also allow for the making of regulations providing for the disclosure of information for national security, the defence of Canada or the conduct of international affairs.

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

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

Part 19 amends the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* by extending the types of government databases from which

FINTRAC may collect information considered relevant to money laundering or terrorist financing to include national security databases. The increased flow of information within government authorized under these amendments may affect the national security activities of the RCMP and its interaction with other parts of government and the private sector.

Finally, various parts of the Act allow the ministers of Transport, Environment, Health, and Foreign Affairs to make temporary directions in emergencies.

Notes

1 S.C. 2001, c. 41. The Act was introduced in Parliament on October 15, 2001. It was considered by committees of both the House of Commons and Senate, and amendments were introduced to place restrictions on the definition of terrorist activities and provide for increased judicial review. Technical amendments generally relating to translation issues were subsequently made in *An Act to Amend the Criminal Code and other Acts*, S.C. 2004, c. 12.

2 Department of Justice Canada, *The* Anti-terrorism Act*: An Act of Prevention*, CD-ROM (2002).

3 R.S.C. 1985, c. C-46, s. 83.01(1)(a) (as am. by the *Anti-terrorism Act*, S.C. 2001, c. 41).

4 Ibid., s. 83.01(1)(b).

5 Ibid.*,* s. 83.01(1.1).

6 See Canada, Public Safety and Emergency Preparedness, *Currently listed entities* (2006), online, http://www.psepc-sppcc.gc.ca/prg/ns/le/cle-en.asp (accessed May 24, 2006).

7 *Criminal Code*, ss. 83.18–83.23.

8 Ibid., ss. 83.02–83.04, 83.08, 83.1–83.12.

9 *Application under s. 83.28 of the Criminal Code (Re)*, [2004] 2 S.C.R. 248 at para. 59.

10 This is subject to notice provisions for those with an interest in the property. Property will not be subject to forfeiture if the judge is satisfied that a person with interest in the property has exercised reasonable care to ensure that the property not be used to facilitate or carry out a terrorist activity and is not a member of a terrorist group. In the case of a dwelling that is a principal residence, the judge must also consider the impact of forfeiture on the immediate family and whether such family members appear innocent of any collusion or complicity in terrorist activity.

11 *Criminal Code*, s. 83.24.

12 Ibid., s. 2.

13 R.S.C. 1985, c. S-7, s. 4.

14 *Criminal Code*, s. 231(6.01).

15 Ibid., s. 424.

16 Ibid., ss. 424.1, 430(4.1), 431.1, 431.2(2).

17 Ibid., s. 83.231 (as am. by the *Public Safety Act*, S.C. 2004, c. 15, Part 4).

18 R.S.C. 1985, c. O-5, s. 3 (as am. by the *Anti-terrorism Act*, S.C. 2001, c. 41).

19 Ibid., s. 4. This section has been referred to Parliament for review, to determine whether it should be amended in response to concerns about its breadth.

20 Ibid., s. 5.

21 Ibid., s. 6.

22 Ibid., ss. 8–15

23 Ibid., ss. 16–18, 20.

24 Ibid., s. 21.

25 Ibid., s. 22. The offence of economic espionage is also included, but I do not discuss it here, as my focus is on national security.

26 Ibid., s. 23.

27 Ibid., s. 26.

28 Ibid., s. 24.

29 S.C. 2000, c. 17.

30 Ibid., s. 55(3)(a). FINTRAC is also required to disclose designated information relevant to the offence of evading or attempting to evade taxes or duties to the Canada Revenue Agency and/or the Canada Border Services Agency (CBSA) and disclose designated information for defined immigration and refugee determination and offence purposes to the CBSA (ibid., s. 55(3)(d)).

31 Ibid., s. 55.1.

32 Ibid., s. 55(7).

33 Ibid., s. 55(5.1).

34 Ibid., s. 60.

35 Ibid., ss. 60.1, 60.2.

36 Ibid., s. 80.

37 *United Nations Suppression of Terrorism Regulations*, S.O.R./2001-360, ss. 3 and 6.

38 Ibid., ss. 4, 6.

39 *Application under s. 83.28 of the Criminal Code (Re)*, [2004] 2 S.C.R. 248 at paras. 39–40 [*Application under s. 83.28*].

40 Ss. 83.28, 83.29.

41 *Application under s. 83.28* at paras. 78–79.

42 Two of the dissenting judges concluded that the procedure violated the institutional independence of the judiciary by requiring it to preside over police investigations. All three dissenting judges concluded that the particular use of the investigative hearing in relation to the Air India trial constituted an abuse of process because it was an attempt by the Crown to gain information about a witness in an ongoing criminal trial: ibid. at para. 180.

43 [2004] 2 S.C.R. 332.

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

45 Two judges dissented on the basis that the open court presumption "would normally defeat the purpose of the proceedings by rendering them ineffective as an investigative tool" and would harm the rights of third parties and the administration of justice: ibid. at para. 60.

46 S. 83.31.

47 Canada, Department of Justice, *The Anti-terrorism Act – Reports* (2005), online, http://canada.justice.gc.ca/en/anti_terr/reports.html [*Anti-terrorism Act* reports].

48 *Criminal Code*, s. 83.3.

[49] Ibid., ss. 83.3(4), 83.3(5).
[50] Ibid., s.83.3(6).
[51] Ibid., s. 83.3(7).
[52] Ibid., ss. 83.3(8), 83.3(9).
[53] Ibid., s. 83.31. Section 83.3 is subject to a renewable five-year sunset provision pursuant to s. 83.32.
[54] *Anti-terrorism Act* reports (see note 47).
[55] *Criminal Code*, ss. 185 (1.1), 186 (1.1).
[56] Ibid., s. 186.1.
[57] Ibid., s. 196(5).
[58] *An Act to amend the Foreign Missions and International Organizations Act*, S.C. 2002, c. 12, s. 10.1(2).
[59] *Canada Evidence Act*, R.S.C. 1985, c. C-5, s. 37.
[60] See *An Act to amend the Criminal Code and other Acts*, S.C. 2004, c. 12.
[61] *Canada Evidence Act*, s. 38.01(1).
[62] Ibid., s. 38.01(3).
[63] Ibid, s. 38.
[64] Ibid., s. 38.04.
[65] Ibid., ss. 38.04(2)(b), 38.04(2)(c).
[66] Ibid., s. 38.06(1).
[67] Ibid., s. 38.06(2).
[68] Ibid., s. 38.06(3).
[69] Ibid., ss. 38.11(1), 38.11(2).
[70] Ibid., s. 38.12.
[71] Ibid., s. 38.13.
[72] Ibid., s. 38.131.
[73] Ibid., s. 38.14.
[74] R.S.C. 1985, c. A-1.
[75] S.C. 2000, c. 5.
[76] R.S.C. 1985, c. P-21.
[77] *United Nations Security Council Resolution 1373*, UN SCOR, 56th Sess., 4385th mtg., UN Doc. S/RES/1373 (2001), online, UN Security Council, http://daccessdds.un.org/doc/UNDOC/GEN/N01/557/43/PDF/N0155743.pdf?OpenElement (accessed June 5, 2006).
[78] Ibid., para. 2.
[79] Ibid., para. 3.
[80] Ibid., para. 6.
[81] The last report from Canada is dated May 4, 2006: United Nations Counter-Terrorism Committee, *Reports from Member States* (UNSC CTC, 2004), online, http://www.un.org/Docs/sc/committees/1373/c.htm (accessed Aug. 9, 2006).
[82] *Smart Border Declaration: Building a Smart Border for the 21st Century on the Foundation of a North American Zone of Confidence*, Ottawa, Canada, December 12, 2001, online, Foreign Affairs and International Trade Canada, www.dfait.gc.ca/can-am/main/border/smart_border_declaration-en.asp (accessed July 20, 2006).
[83] *32-point Action Plan*, Ottawa, Canada, December 12, 2001, online, Foreign Affairs and International Trade Canada, www.dfait-maeci.gc.ca/can-am/main/border/32_point_action-en.asp (accessed July 20, 2006).
[84] *Department of Public Safety and Emergency Preparedness Act*, S.C. 2005, c. 10, s. 4.
[85] Ibid., s. 6(1).

[86] Canada, Privy Council Office (Ottawa: PCO, 2004), online, http://www.pco_bcp.gc.ca/docs/Publications/NatSecurnat/natsecurnat_e.pdf (accessed July 20, 2006). See also Canada, Privy Council Office, *Securing an Open Society: One Year Later – Progress Report on the Implementation of Canada's National Security Policy* (Ottawa: PCO, 2005), online, http://www.pco-bcp.gc.ca/docs/ministers/deputypm/secure_e.pdf (accessed Aug. 25, 2006).

[87] S.C. 2004, c. 15.

IV
Current National Security Activities of the RCMP

1.
INTRODUCTION

In the preceding chapters, I set out the history of national security activities in Canada up to the events of September 11, 2001, with particular focus on the RCMP's national security role and the Canadian government's response to 9/11. In this chapter, I detail the RCMP's national security activities since those terrorist attacks. Together with the next chapter, in which I describe the other government actors involved in protecting Canada's national security, these four chapters provide a foundation for meaningfully addressing the issue at the centre of my mandate in the Policy Review: the need for and necessary features of a review mechanism for the RCMP's national security activities. My recommendations for a review mechanism set out in Chapter XI are directly linked to the characteristics of Canada's national security landscape as a whole, as well as the features of the RCMP's current national security activities and the context in which they are carried out.

The RCMP is currently involved in a broad range of activities in support of its national security mandate. In general terms, these include collecting, maintaining and analyzing information and intelligence related to national security; sharing such information and intelligence with other agencies, both domestic and foreign; preparing analyses and threat assessments and developing other methods of support for internal and external purposes; investigating crimes related to national security; investigating and countering activities to prevent the commission of crimes related to national security; and protecting specific national security targets.[1]

My discussion of these national security activities is divided into five parts: an organizational overview; a description of activities carried out by RCMP

branches and units involved in national security; a discussion of the overlap between the national security activities and other law enforcement activities carried out by the Force; a description of the information and intelligence management mechanisms employed by the RCMP; and an introduction to the RCMP's interaction with other national security actors.

Before I begin, however, I wish to draw attention to one pervasive feature of the RCMP's national security role: the Force's response to criminal threats to national security, like the government's response to national security threats in general, is continuously evolving. Many of the threats currently faced by Canada are different from in the past. It is therefore not surprising that the response to them is modified and adapted regularly. Significant changes have been made to the RCMP's national security activities even during the conduct of this Inquiry and, as I drafted this Report, I became aware of further proposals for changes. Two points thus arise: first, some of the details discussed herein may be out of date soon after this report is published; second, it is important that the evolving nature of RCMP national security activities — indeed, of the government's approach in general — be borne in mind in addressing the issue of a review mechanism. An effective mechanism must have the capability to adapt to change.

2.
ORGANIZATIONAL OVERVIEW

A discussion of the RCMP's national security activities requires a look at the context in which the Force carries out those activities, including how the activities fit into the organization as a whole and into the RCMP chain of command. I therefore begin with a description of the administrative organization in relation to the RCMP's national security activities. Following that, I set out a number of factors relevant to context, including ministerial directives and internal policies governing national security activities, the RCMP's internal accountability mechanisms, the number of RCMP personnel engaged in national security, and recruitment and training requirements in respect of those activities.

2.1
ORGANIZATION OF RCMP NATIONAL SECURITY ACTIVITIES

The Commissioner of the RCMP is assisted in the management and control of the Force by a number of deputy commissioners: one for each RCMP region or division (Atlantic, Central, North West and Pacific) and one each for Strategic Direction, Corporate Management and Operations (see Chart 1, p. 86). The Deputy Commissioner, Operations, is responsible for the RCMP's national security mandate, as well as for federal and international operations, protective

policing, community, contract and Aboriginal police services (CCAPS), criminal intelligence, and technical operations.

National security matters have come within the ambit of the Criminal Intelligence Directorate (CID) since this important component of intelligence-led policing was created in 1991. CID is headed by the Assistant Commissioner, CID, who reports to the Deputy Commissioner, Operations. In addition to its national security function, discussed below, CID includes the Criminal Intelligence Support Branch, Organized Crime Intelligence Branch, National Operations Centre and Director General, Intelligence Analysis and Communications.

In 2003, a new reporting function was created directly under the Assistant Commissioner, CID: the Director General, National Security. The Director General heads the National Security Directorate, which has three branches: the National Security Intelligence Branch (NSIB), National Security Operations Branch (NSOB) and Threat Assessment Branch (see Chart 2, p. 87).

Pursuant to ministerial directive (discussed below), RCMP National Headquarters is responsible for coordinating virtually all activities relating to the RCMP's national security mandate. In addition, the various branches, sections and units within the National Security Directorate are responsible for the analysis and management of national security information and intelligence, as well as the preparation of threat assessments and other national security information products. Much of the investigative work on national security matters is done at the divisional level. Such work is undertaken either by Integrated National Security Enforcement Teams (INSETs) or National Security Investigation Sections (NSISs). As discussed below, INSETs are teams made up of RCMP members and personnel seconded from other police forces and government agencies. They are located in Vancouver, Toronto, Ottawa and Montreal. RCMP divisions without an INSET have an NSIS, which carries out the same function, but is not integrated with other agencies. The work of both INSETs and NSISs is coordinated by National Headquarters and they both report to the NSOB, through the Division Criminal Operations Branch (see Chart 3, p. 88). I describe the national security work carried out at the headquarters and divisional levels in Section 3, below.

2.2
MINISTERIAL DIRECTIVES

All of the RCMP's national security activities are ultimately under the control of the Commissioner of the RCMP who, pursuant to the *Royal Canadian Mounted Police Act* (*RCMP Act*),[2] "has the control and management of the Force and all matters connected therewith." As I discuss in Chapter II, this control and

CHART 1

RCMP National Organization

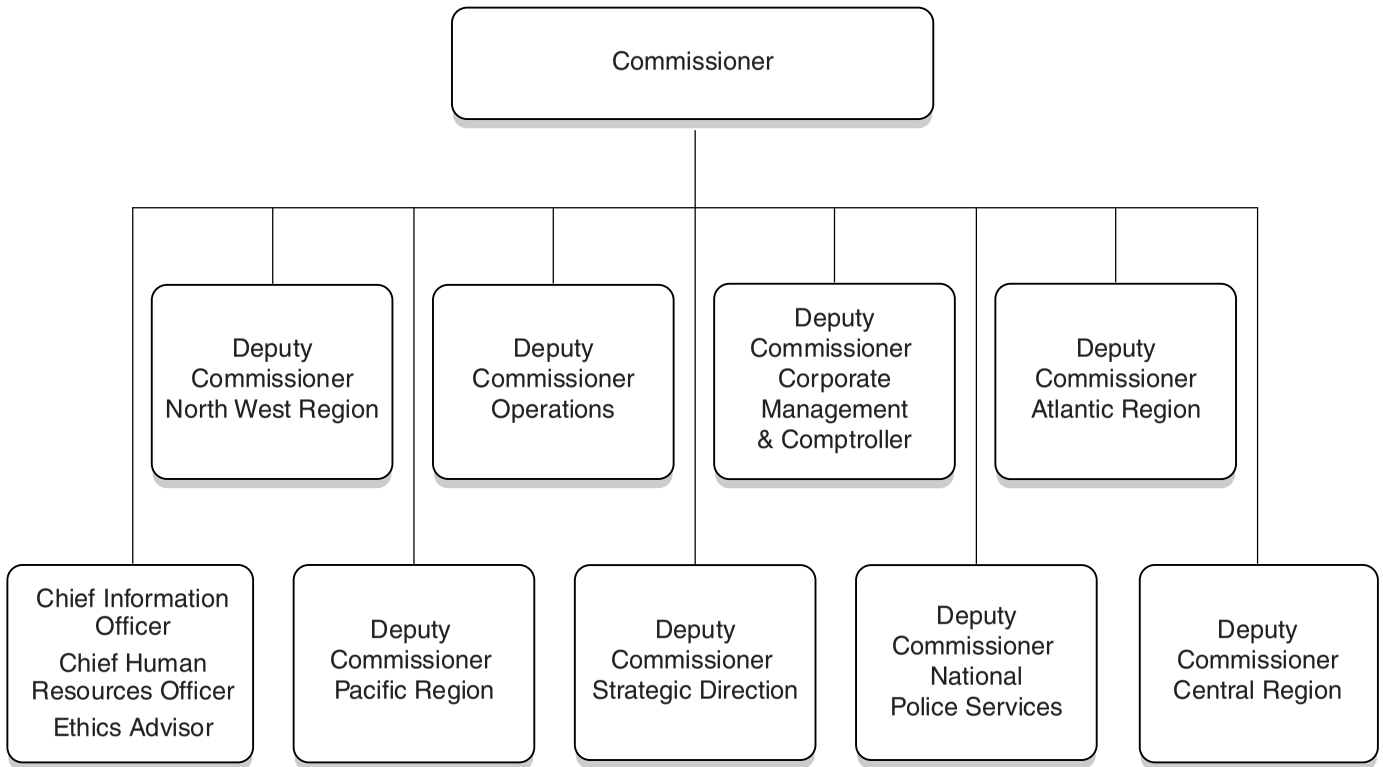


CHART 2

CID Organizational Structure

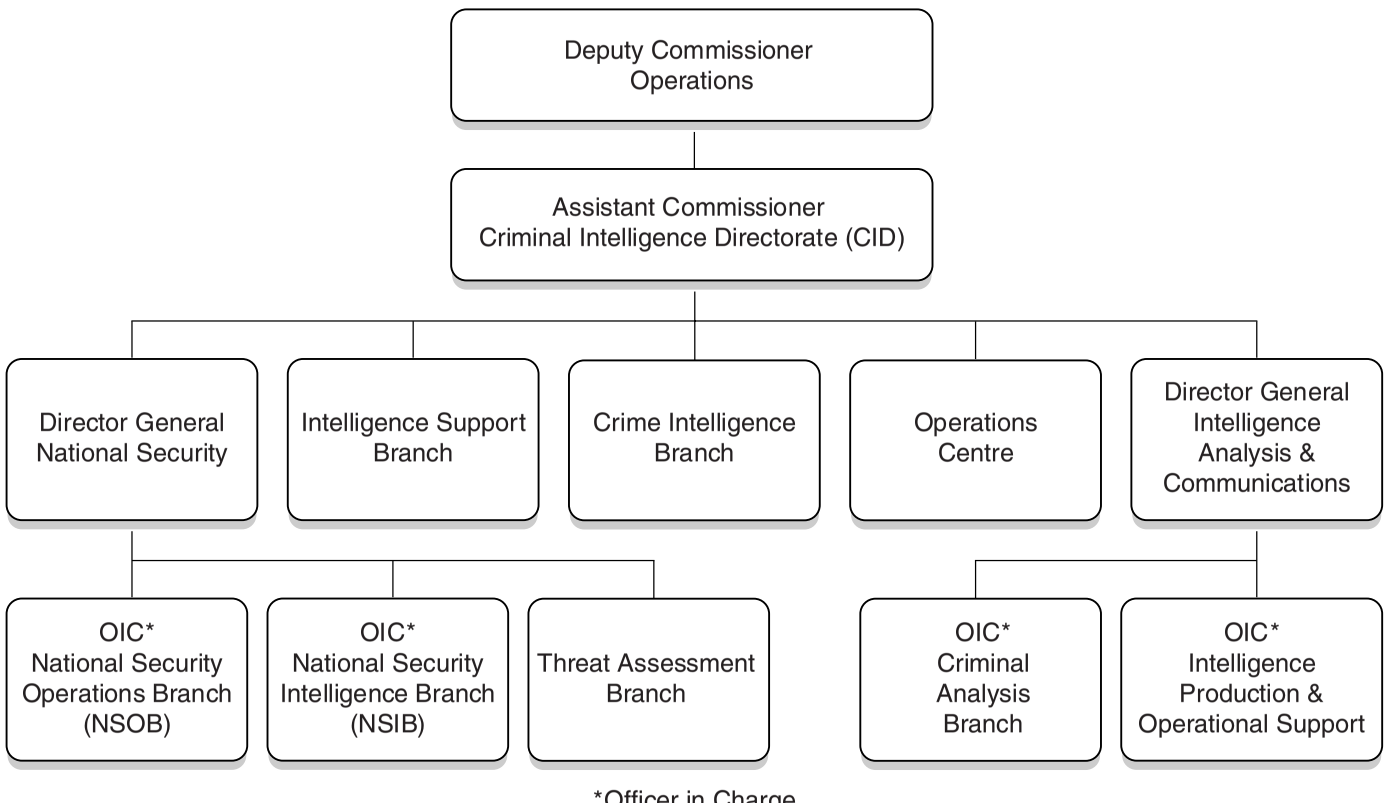
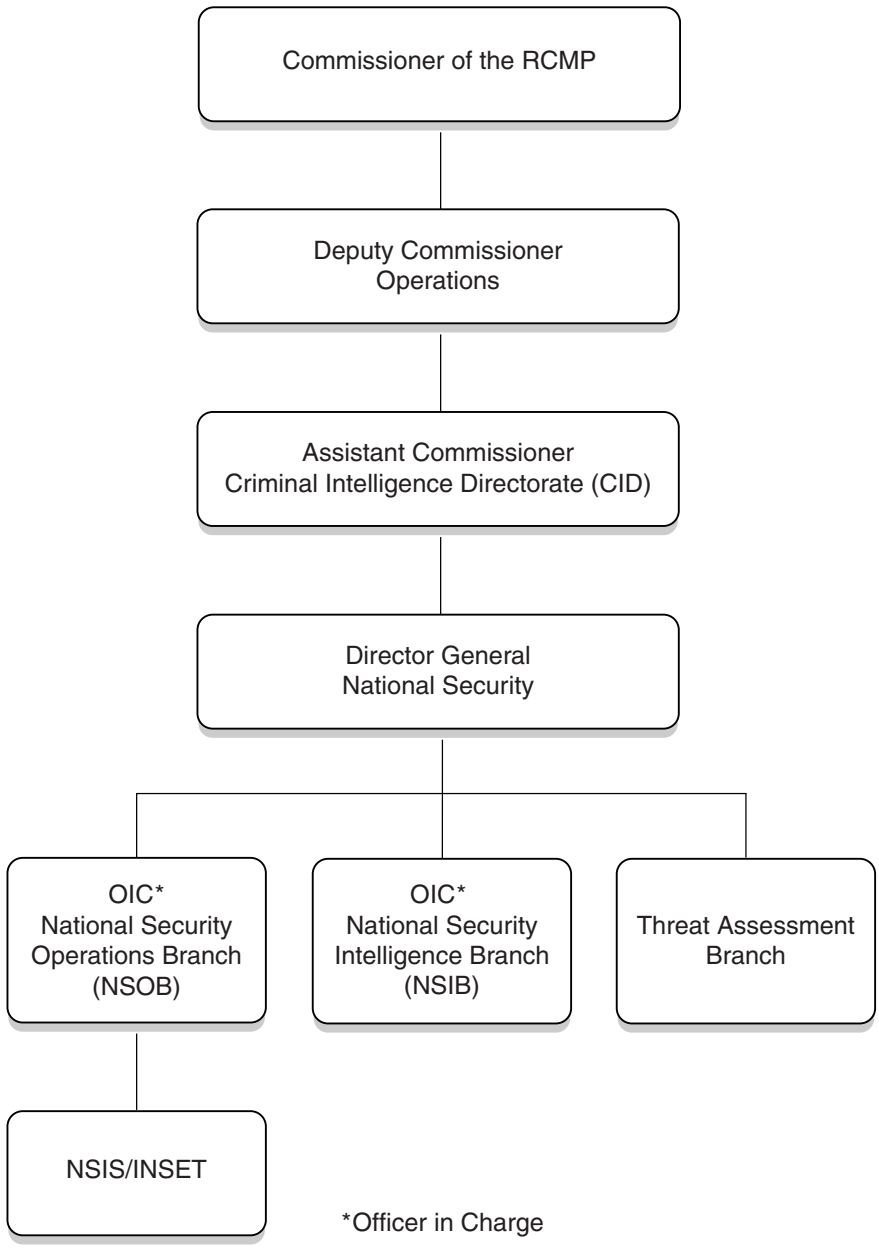


CHART 3

NSIS/INSET Reporting Structure



management is "under the direction of the Minister," who exercises his or her role with respect to the RCMP primarily by issuing directives to the RCMP. A number of ministerial directives (sometimes called ministerial directions) affect the RCMP's national security mandate:

(i) The Ministerial Directive on Police Assistance to Foreign Nations (1981)[3] sets out policies and guidelines in respect of the provision by the RCMP of police training, consultative assistance (providing advice in regard to training or an investigation) and investigative assistance to foreign countries (relocating RCMP staff and/or equipment to a foreign country to help with a criminal investigation in that country). The directive sets out procedures to be followed in reviewing such requests and the appropriate considerations.

(ii) The Ministerial Directive on RCMP Agreements (April 2002)[4] deals with "agreements entered into by the RCMP to provide services, information, assets, or assistance to, or receive same from, other departments, agencies and institutions of municipal, territorial, provincial, federal or foreign governments, or with international organizations." This directive provides guidance with respect to accountability and consultation requirements for RCMP agreements.

(iii) The Ministerial Direction – National Security Responsibility and Accountability (November 2003)[5] deals specifically with responsibilities and accountabilities of the RCMP in relation to investigations that fall under section 6(1) of the *Security Offences Act* and investigations related to a terrorist offence or terrorist activity as defined in section 2 of the *Criminal Code*. It affirms that the national security activities of the RCMP are under the control of the Commissioner, subject to direction by the Minister, that the Minister is accountable to Parliament for the RCMP, and that the Commissioner is in turn accountable to the Minister. The directive also provides that national security investigations should be coordinated at RCMP National Headquarters. It states that "[s]uch central coordination will enhance the Commissioner's operational accountability and in turn, will enhance ministerial accountability, by facilitating the Commissioner's reporting to the Minister." The Commissioner is required to keep the Minister apprised of all national security investigations that may give rise to controversy.

(iv) The Ministerial Direction – National Security Related Arrangements and Cooperation (November 2003)[6] "establishes the process for the Royal Canadian Mounted Police (RCMP) to follow when entering into an arrangement with foreign security or intelligence organizations for the purpose of

performing its duties and functions with respect to matters that fall under subsection 6(1) of the *Security Offences Act*, and those related to a terrorist offence or terrorist activity, as defined in . . . the *Criminal Code*." The directive states that "[t]he RCMP may, with the Minister's prior approval, enter into a written or oral agreement, or otherwise cooperate, with foreign security or intelligence organizations." It does not apply to arrangements or co-operation with foreign law enforcement agencies or organizations. The directive provides for consultation with Foreign Affairs and International Trade Canada (DFAIT) and CSIS regarding such arrangements. It also sets out a requirement that all such arrangements be recorded in writing and that the Commissioner report annually on their status to the Minister. I note that the RCMP has relatively few arrangements and/or agreements with foreign intelligence agencies, as such matters are generally left to CSIS.

(v) The Ministerial Direction – National Security Investigations in Sensitive Sectors (November 2003)[7] defines "sensitive sectors" as "fundamental institutions of Canadian society," including institutions "in the sectors of academia, politics, religion, the media and trade unions." All investigations involving sensitive sectors must be pre-approved by the Assistant Commissioner, CID, or his or her designate. The directive also states, in regard to university or post-secondary campuses, that "it is paramount that the investigations undertaken by the RCMP do not impact upon the free flow and exchange of ideas normally associated with an academic milieu."

2.3 INTERNAL POLICIES

The activities of RCMP personnel, including personnel engaged in national security activities, are also regulated by a number of internal policies, including a code of conduct.

In specific relation to national security, there are policy provisions dealing with national security investigations (including the requirement that the RCMP not gather information on or investigate organizations engaged in lawful activities unless such action is justified by allegations or intelligence); the requirement that anti-terrorism investigations be conducted by NSISs or NSETs; the obligation of members to respect the rights of those who are the subject of an investigation; a definition of national security and a threshold for identification of a matter as a national security matter; reporting requirements; the RCMP/CSIS exchange program; RCMP agreements; and information and human sources. I discuss those policies below.

Section 37 of the *RCMP Act* provides standards for all RCMP officers. These include respecting the rights of all persons, maintaining the integrity of the law and the administration of justice, performing duties without abusing their authority as RCMP officers, and ensuring that improper or unlawful conduct of any member of the Force is not concealed or permitted to continue.

The RCMP's Code of Conduct[8] is prescribed by regulation. Among other things, it requires RCMP officers to obey lawful orders and assist those in danger and prohibits them from making false, misleading or inaccurate statements or neglecting their duties. It also requires respect for rights and freedoms and prohibits discrimination.

2.4
INTERNAL ACCOUNTABILITY MECHANISMS

The RCMP has established various internal controls and accountability structures with respect to its mandate, including its national security activities. These mechanisms provide an opportunity for internal assessment of the conduct of the RCMP and its officers. In addition to the accountability and control framework inherent in its command structure, the RCMP has three internal accountability mechanisms: the disciplinary process, the Audit and Evaluation Branch and the board of inquiry. It also has an external accountability mechanism, the Commission for Public Complaints Against the RCMP (CPC), the role of which I describe in Chapter VI.

Where formal disciplinary action is required, the RCMP Code of Conduct is enforced through the establishment of an adjudication board under Part IV of the *RCMP Act*. The adjudication board is a formal disciplinary tribunal comprising three officers, one being legally trained. Officers of the Force may also be recommended for discharge or demotion by discharge and demotion boards, which are also made up of three officers, one being legally trained, appointed under the authority of Part V of the Act.[9]

The Adjudications Branch manages, administers and provides adjudicative services under the authority of the *RCMP Act*. The Branch consists of three legally trained members who act as chairs on both types of boards. Adjudication hearings are held in public and are formal, court-like processes. The rights of members are outlined in Part IV of the Act and in the Regulations, and rules of practice and procedure are set out in a Commissioner's standing order. Boards have legal authority to hear evidence, such as sworn testimony, to make determinations as required and, if a contravention is established, to administer different sanctions such as forfeiture of pay, demotion and dismissal. Discharge and demotion boards may demote or discharge a member. Members appearing

before an adjudication or discharge and demotion board may be represented by another member, a member representative or legal counsel. Proceedings are recorded by a court reporter. The written decision of the board is a public document and the original is kept in the registry of the Adjudications Branch. The decision of a board may be appealed to the RCMP Commissioner, as outlined in Parts IV and V of the Act.[10]

The RCMP External Review Committee provides recommendations on the disposition of an appeal to the Commissioner. Established by Part II of the Act, the Committee is an independent, arms-length labour relations tribunal. Its mandate is to review grievance, disciplinary, discharge and demotion cases referred to it by the RCMP and provide recommendations in their regard to the Commissioner. Although the bulk of its workload involves reviewing grievance decisions, the Committee also receives referral of the other matters mentioned above. Essentially, the Committee's reviews are intended to ensure transparency, fairness, impartiality and independence in the RCMP's internal labour relations process.[11]

The Committee does not have authority to initiate reviews. Cases must be referred to it by the Commissioner of the RCMP. The Act sets out the types of cases that require Committee review. Moreover, the Committee does not have investigatory powers. In all grievance, discipline, discharge and demotion matters referred to it, it must base its review on the record before it. This includes all of the original documents, the decision made, and the submissions of the parties. Where a review involves the appeal of a disciplinary or discharge and demotion decision, the Committee is also provided with the transcript of the board hearing and any exhibits entered at the hearing. The Chair may request that a party provide additional information or submissions and, if this is done, the other party is given the chance to respond. The Chair may also hold a hearing if deemed necessary, although use of this option is rare. The Chair reviews all the evidence, legal issues, relevant legislation and case law in coming to a determination on the matter.[12]

The Chair provides the findings and recommendations to the Commissioner of the RCMP, the final decision-maker in the internal process for these cases, and to the parties. The Commissioner must consider the Committee's recommendations, and if he or she decides not to follow them, must provide an explanation for not doing so in his or her reasons.[13]

The mandate of the External Review Committee differs significantly from that of the CPC. The Committee focuses on reviewing labour relations decisions made within the RCMP, at the appellate level of the process. Files are referred to the Committee after the initial decision has been made. The Committee has

no direct contact with the public. The CPC's mandate, as discussed below, is the review of public complaints against the RCMP. The CPC may operate either as a form of appellate review body for RCMP investigations and decisions about complaints or, when the Chair invokes the public interest, as an external review body of first instance. It may receive complaints from members of the public or the Chair may initiate complaints, investigations or hearings.[14]

The Audit and Evaluation Branch also performs an internal accountability function within the RCMP. It provides risk management services with respect to internal controls, activities and culture. Its mandate includes ensuring compliance with laws, regulations and internal policies, and evaluating services. The Branch submits reports to an audit committee and the RCMP Commissioner, and also communicates with the Auditor General.[15]

The mandate of the Audit and Evaluation Branch is to provide risk-based assurance services to senior management on the soundness of risk management strategies and practices; management control frameworks, systems and practices; and information for decision making and reporting. The Director General of the Branch is accountable to the RCMP Commissioner and the Audit Committee for providing assessments on the adequacy and effectiveness of the RCMP's processes for controlling its activities and managing its risks; reporting significant issues related to the processes for controlling RCMP activities, including potential improvements to those processes, and providing information concerning such issues through to resolution; periodically providing information on the status and results of the annual audit plan and the sufficiency of resources to meet the Branch's mandate and objectives; and coordinating with other control and monitoring functions such as risk management, compliance, security, legal, ethics, environmental and external audit.[16]

Audit and Evaluation Branch officers and civilian members have some autonomy within the Force, but are not independent from it. They remain subject to its command structure. While the Branch performs important work, it is not focused on national security matters or on ensuring respect for rights and freedoms.

The role of the Audit Committee is to provide advice and counsel to assist the RCMP Commissioner in discharging his or her responsibilities for risk management, the design and operation of management control frameworks, and the quality of financial and other performance information used for decision making; ensure that the results of internal audits are incorporated into the RCMP's priority setting, planning and decision-making processes; strengthen the independence and effectiveness of the internal audit function; emphasize the accountability of managers; provide the Commissioner with advice on the im-

pacts of government-wide initiatives aimed at improving management practices; and facilitate communication between senior management, the internal audit function, central agencies and the Office of the Auditor General.[17]

The third internal accountability mechanism is the board of inquiry. The Commissioner of the RCMP or the Minister of Public Safety (formerly the Solicitor General) are empowered under section 24.1 of the *RCMP Act* to establish a board of inquiry to investigate and report on a broad range of matters involving the Force, including training, conduct, performance of duties, discipline and administration. Such boards are given broad powers to summon individuals and receive evidence under oath. The rights of persons affected by a board of inquiry are set out in the Act. Unless the RCMP Commissioner or Minister of Public Safety directs otherwise, investigations and board of inquiry hearings are conducted in private.[18]

2.5
PERSONNEL INVOLVED IN THE NATIONAL SECURITY MANDATE

RCMP personnel directly involved in national security activities, including individuals working in the National Securities Directorate and Criminal Extremism Analysis Section[19] at the headquarters level and in NSISs and INSETs at the divisional level total 328: 231 regular RCMP members, 67 on secondment from other police forces and government agencies, and 30 civilians.[20]

It is difficult to arrive at a precise number of RCMP personnel involved in national security matters because, in many cases, there is overlap with other departments and areas. I discuss the extent of such overlap below.

2.6
RECRUITING AND TRAINING

The basic requirement for a regular RCMP member to be recruited into a position related to national security is several years of experience in criminal investigation work. When recruiting members to a specialized investigative team, managers look for specific skills that may be needed to strengthen the team. The criteria considered include the following:

- top secret security clearance;
- experience in investigating major cases (especially in the case of supervisors);
- specific skills, such as affidavit writing or file management;
- source development capabilities;
- interpersonal skills;

- "above average interest" in worldwide current events;
- specialized investigational experience; and
- above average written and oral communication skills.

Training is available for members working in national security. The most pertinent courses are the National Security Enforcement Course and a Bill C-36 anti-terrorism course designed and supervised by the Department of Justice. Approximately 90 percent of INSET/NSIS members have completed these courses. Training is also available in the following subject areas:

- Secure Criminal Information System (SCIS);
- National Criminal Databank;
- terrorist financing;
- source development and handling;
- proceeds of crime;
- hostage negotiation;
- major case management;
- Criminal Intelligence Officer position;
- cross-cultural issues and cultural awareness;
- surveillance techniques;
- immigration and passports;
- Internet investigations; and
- threat assessment.

Criteria for recruiting civilian members into national security positions depend on the requirements of the specific positions. An analyst position, for example, has the following minimum requirements:

- top secret security clearance;
- Bachelor's degree;
- several years of experience in researching, writing, analyzing and editing documents, as well as experience in a publishing, research or analytical environment;
- experience with computers and word processing;
- above average oral and written communication skills; and
- ability to satisfy the language profile for the position.

Training for civilians employed in national security work includes courses in intelligence analysis at the Canadian Police College and many of the other courses available to regular members of the RCMP as set out above. I have made

a number of recommendations with respect to improvements to training in my Factual Inquiry report.

3. SCOPE OF RCMP'S CURRENT NATIONAL SECURITY ACTIVITIES

The following descriptions of each of the RCMP's branches and units engaged in national security activities illustrate the scope of these activities.

3.1 NATIONAL SECURITY INTELLIGENCE BRANCH

The National Security Intelligence Branch (NSIB), located at RCMP National Headquarters, is responsible for the assessment, coordination, monitoring and direction, when necessary, of all national security investigations and intelligence at the national and international levels. Its primary mandate is to collect and analyze intelligence in relation to the RCMP's national security mandate. It is also responsible for identifying potential strategic approaches to national security investigations and producing tactical analytical products (TAPs), intelligence products that make the case for the commencement of criminal investigations. On occasion, the NSIB will task INSETs or NSISs to assist with TAP preparation.

The process for creating TAPs begins with review and analysis of information received by the NSIB from a variety of sources, including CSIS,[21] Canada's allies, other police forces, other intelligence agencies, other domestic government departments and agencies[22] and the community. This information is analyzed and prioritized in a manner consistent with the priorities set by Criminal Operations (CROPS) officers at the annual tactical priorities meeting.[23] Prioritization is also informed by discussions with CSIS. In preparing TAPs, the NSIB also uses RCMP-generated information and information requested from domestic and foreign agencies[24] to supplement the unsolicited information.

Once a TAP is complete, a decision is made about whether or not to proceed with a tactical project (criminal investigation). In matters that proceed to the criminal investigation stage, the file is delivered to the NSOB for coordination and oversight of the investigation. The complexity and scope of a TAP determines who, within the RCMP, is responsible for authorizing release of the TAP to the field. Where the TAP is extensive and investigation will likely require a significant investment of resources, a presentation is made to the Director General, National Security and, in some cases, the Assistant Commissioner, CID, whose authority is required to approve release of the TAP to the appropriate divisions for investigation. In such instances, transfer of the package to a field

unit also entails holding a meeting with all units concerned, including the relevant Division Criminal Operations Branch and the INSET/NSIS commander. Where the TAP is not as complex and investigation will not likely be resource-intensive, the TAP may be forwarded to a division for follow-up upon approval of the Officer in Charge (OIC), NSIB. In the majority of cases, the TAP or portions of it are shared with CSIS.

In addition to producing TAPs, the NSIB is involved in the day-to-day flow of national security information within the RCMP. A significant portion of national security information received by the RCMP comes through the NSIB, which is the RCMP's primary contact point for intelligence agencies that have information to relay. While this information may be used in the production of TAPs, some of it may also need to be directed to the field even before a TAP is produced.

Another area of responsibility for the NSIB is answering requests for information from entities outside the RCMP. Requests from intelligence agencies and other government departments, both domestic and foreign, are directed to the NSIB, while those from police agencies are generally directed to the NSOB.

The final main area of responsibility for the NSIB is the briefing of senior members of the Force on issues related to national security.

The following are some of the sections or groups that come within the responsibility of the NSIB:

Terrorist and Criminal Extremist Special Projects Group

The Terrorist and Criminal Extremist Special Projects Group is responsible for the coordination and development of intelligence relating to terrorist activity and criminal extremism[25] from a national perspective, in support of national security investigations and the deployment of counter-terrorism strategies. Specifically, the Group is responsible for promoting and implementing counter-terrorism and anti-terrorist strategies, activities, procedures, policies and standards in order to identify and understand how extremist organizations recruit, operate and maintain their organizations. It produces intelligence packages to focus enforcement efforts. It also develops relationships and maintains liaisons with other entities in the domestic and international law enforcement communities. The Group also collects and collates information, intelligence and evidence to support the listing of terrorist entities pursuant to section 83.05 of the *Criminal Code*.[26] The RCMP prepares criminal intelligence reports for the Minister, who uses them, together with security intelligence reports prepared by CSIS, to make recommendations regarding listing to the Governor in Council. Also in regard to listing, the Group assists the Department of Justice in judicial

reviews, monitors appeals and reviews of listings, and assists with the revocation of charitable registrations of terrorist groups.

Anti-terrorist Financing Group

The Anti-terrorist Financing Group supports counter-terrorism strategies, financial intelligence gathering and financial investigations. It also monitors financial operations from a national perspective and implements counter-terrorism financing strategies, activities, procedures, policies and standards. It is the main entry point for information provided to the RCMP by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

Critical Infrastructure Intelligence Section

Managed jointly by the NSIB and the Criminal Analysis Branch of CID, the Critical Infrastructure Intelligence Section focuses on threats to critical infrastructure. Its work includes producing threat and risk assessments, indications and warnings, and intelligence assessments relevant to critical infrastructure, as well as providing support for investigations related to threats to critical infrastructure.

3.2
NATIONAL SECURITY OPERATIONS BRANCH

The National Security Operations Branch (NSOB), also located at National Headquarters in Ottawa, focuses on coordinating investigations related to national security across the country. It is also responsible for ensuring compliance with RCMP policies (including policies relating to national security investigations); preparing subject profiles, case briefs and briefing notes for senior management; and assisting the Commissioner in his responsibility for informing the Minister of high-profile national security investigations that may give rise to controversy.

The NSOB is responsible for providing Headquarters' approval for all national security investigations undertaken by INSETs and NSISs. This includes an intake responsibility in respect of work originating with the NSIB and other sources both internal and external to the RCMP. Work comes into the NSOB in a variety of ways. The TAPs produced by the NSIB, which I discuss above, represent the genesis of approximately 10 percent of the files overseen by the NSOB. Other files are started as a result of the receipt of information from various sources both within and outside the RCMP.

Information received by the NSOB is initially assessed by either the Officer in Charge (OIC) or the Operations NCO. The first step in the assessment is to

determine whether or not the information involves criminality or potential criminality. If none is apparent, the matter may be referred to CSIS. In some instances, a determination of criminality is made at the outset, but further investigation leads to the conclusion that no criminality is involved. In such an event, the investigation stops and the information obtained may be handed over to CSIS. Nevertheless, information gathered in such an investigation remains on the SCIS database (the RCMP's secure database reserved for national security information and intelligence, which I examine in greater detail below) until it is deleted in the normal course of operations.

The second matter decided at the outset is whether the information relates to national security. Again, this is not always a permanent determination. National security crimes overlap with many other forms of criminal behaviour. If there is a deemed national security link, a file is treated as a national security file and all national security policies and procedures apply even if the investigation is not being conducted by an INSET or NSIS.[27] If, ultimately, it is determined that there is no national security link, the investigation is stopped or handed over or back to another area within the RCMP or another police agency.

Whenever the OIC or Operations NCO decides to open an investigation on the basis of information received, the file is assigned to a reviewer within the NSOB. Reviewers play a pivotal role within the NSOB as the headquarters coordinators of the national security investigations in their portfolios. Virtually all national security investigations handled by the RCMP are assigned an NSOB reviewer, unless they are "open and shut" cases that last only a very short time. The reviewer coordinates the flow of information between Headquarters and the field officers assigned to the matter; finds specialized resources within the RCMP to support the file; interacts with domestic and foreign police agencies,[28] CSIS and RCMP liaison officers abroad; and ensures compliance with RCMP policies and procedures, including national security policies and procedures. Another part of the reviewer's role is to make sure that all RCMP investigations with a deemed national security nexus (even those that originate or continue to be investigated outside of INSETs or NSISs) are coordinated through Headquarters.

The NSOB is also responsible for oversight of information sharing with domestic police agencies. While exchanges of information may occur at the field level, especially when RCMP personnel are co-located with other police agency personnel,[29] the NSOB must be kept advised of any such exchanges. The INSET Officer in Charge is responsible for approving this type of exchange. Because of its interaction with RCMP liaison officers abroad, the NSOB has also been involved in sharing information with foreign police agencies through liaison officers. Approval for such information exchanges is through the NSOB. As I note

above, information exchanges with foreign intelligence agencies are approved by the NSIB.

The NSOB includes Source Development Units (SDUs), which are responsible for developing human sources for national security investigations. They report to and take their instructions from INSETs. In practice, an INSET will identify gaps in investigations on which it is working and task an SDU to develop human sources to help fill those gaps. However, the existence of SDUs does not prevent INSETs from carrying out their own source development.

3.3 THREAT ASSESSMENT BRANCH

The primary role of the Threat Assessment Branch is to maintain the National Threat Assessment Program (NTAP), which provides the RCMP with support for its protective responsibilities, which include protection of embassies, consulates or missions within Canada; internationally protected persons;[30] airports, carriers and air routes; and the Canadian executive cadre. The Branch monitors events and prepares threat assessments on national security issues that may have an impact on threats posed to Canada or to Canadian interests abroad.

The Branch has three units:

International Protective Intelligence Unit

The International Protective Intelligence Unit develops threat assessments for foreign embassies, consulates and missions within Canada. It also provides threat assessments in respect of foreign visitors to Canada (internationally protected persons) and major events in Canada, and handles background checks for Order-in-Council appointments.

Civil Aviation Protective Intelligence Unit

The Civil Aviation Protective Intelligence Unit identifies flights and routes in Canada that may face terrorist action or other threats and provides threat assessments to Canadian and international airports and air carriers. It also supports the Canadian Air Carrier Protective Program, which assigns RCMP officers to certain Canadian flights.

Canadian Executive Protective Intelligence Unit

The Canadian Executive Protective Intelligence Unit develops threat assessments relating to the Canadian executive cadre (including the Prime Minister, Governor General, Cabinet ministers, members of Parliament, senators and Supreme Court, Federal Court and Tax Court judges) both inside Canada and when they

travel abroad. It is also responsible for coordinating and maintaining the VIP Surveillance Subject Program, which identifies, investigates, assesses and monitors individuals who have shown a criminal or "abnormal" interest in the Canadian executive cadre, government officials or internationally-protected persons.

The Threat Assessment Branch also includes a *Public Safety Act* project coordinator, whose function it is to provide support to the Minister of Public Safety in respect of the *Public Safety Act*.

3.4
CRIMINAL EXTREMISM ANALYSIS SECTION

The Criminal Extremism Analysis Section (CEAS) is administered outside the National Security Directorate by the Criminal Analysis Branch. However, Section analysts perform tactical and strategic analysis in support of the national security program. The Section produces three types of intelligence:

- strategic intelligence, which involves assessments in support of operational and policy decision making by senior managers of the RCMP, including decision making in relation to resources allocated to investigations (this includes "Sleipnir"[31] threat measurement assessment and an annual report for consideration by Criminal Operations (CROPS) officers, when they determine national strategic and tactical priorities for all RCMP operations, including national security);
- current intelligence, including assessments in support of operational and policy decision making by the Threat Assessment Branch and Protective Policing Services; and
- tactical intelligence, in the form of charts and assessments in support of investigations.

Tactical analysts in CEAS are given specific clients and a tactical analyst is assigned to each of the NSOB, NSIB and the Anti-Terrorism Financing Group. These analysts also provide analytical support directly to INSETs and NSISs at the divisional level, upon request. Tactical analysts in the divisions also support the INSETs. Specific areas of expertise developed in CEAS include terrorism / criminal extremism; distinct types of criminal activities used by terrorists, such as chemical and biological terrorism, money laundering and suicide bombing; and the intentions, capabilities and activities of specific terrorist groups and movements operating in Canada.

3.5
NSISs, INSETs AND IBETs

NSISs and INSETs

National Security Investigation Sections (NSISs) and Integrated National Security Enforcement Teams (INSETs) operate at the divisional level and have primary responsibility for carrying out criminal investigations in national security matters. Created in 1988, NSISs are made up entirely of RCMP personnel. There were originally 14 sections. After 9/11, four were converted to INSETs, integrated teams comprising both RCMP officers and personnel from provincial and municipal police forces and non-police agencies. INSETs are an illustration of the RCMP's integration strategy. Integrated Border Enforcement Teams (IBETs) are also involved in national security activities.[32] Integrated units are not restricted to national security matters and are also employed in other areas, such as organized crime.

In addition to RCMP members, INSETs may have members from provincial and municipal police forces and from various agencies such as CSIS, the Canada Border Services Agency (CBSA), Citizenship and Immigration Canada (CIC), the Canada Revenue Agency and other federal and provincial agencies. 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.

O-INSET is moreover co-located with Ontario's Provincial Anti-Terrorism Section (PATS), representatives of the Attorney General of Canada and Attorney General of Ontario, and the Combined Forces Special Enforcement Unit (CFSEU), the mandate of which centers around organized crime. This latter co-location facilitates communication between O-INSET and the CFSEU. In the event of a national security emergency requiring a significant increase in strength to fulfill the RCMP's national security role, the CFSEU would be a likely source of personnel. The improved communication arising from co-location would allow a smoother transition than would be the case if personnel with no knowledge of the INSET's operations were deployed.

INSET activities are coordinated and overseen by RCMP National Headquarters. According to the RCMP, it is fully accountable for the operations of INSETs, and RCMP policies and rules apply to the actions of INSET members. Members of other police services seconded to an INSET are made

Supernumerary Special Constables in the RCMP. There are agreements in place between the RCMP and other police services regarding this status. One such agreement was examined during the Policy Review process. It provides that the officer from a municipal service shall be supervised by the RCMP, but shall remain under the jurisdiction of the municipal service's disciplinary process, as well as the appropriate civilian oversight agency. Pursuant to the agreement, the municipal service agrees to hold harmless and indemnify the RCMP in respect of claims arising from the conduct of the officer. Information obtained by officers seconded to the INSET from other agencies may not be passed on to those other agencies except through normal national security channels.

As I mention above, the focus of INSETs is the investigation of national security crimes. To gain a better understanding of how INSETs operate, the Commission conducted a detailed examination of O-INSET. In 2003, O-INSET opened some 1,174 new files, worked on 12 projects and responded to nine mini-crises. Projects are major investigations reflecting the RCMP's national tactical priorities, as determined by the CROPS officers. Mini-crises are short-term emergencies. O-INSET gave the threat to bomb an El Al flight destined for Toronto in 2003 as an example of a mini-crisis.

O-INSET has a centralized input coordination function, with all external tasking coming through the O-INSET Intake Officer. As is the case with intake at the NSOB, two initial determinations are made by the Intake Officer: whether or not there is a sufficient national security nexus, and whether or not there is a sufficient criminal nexus. Tasks that do not meet these criteria are rejected or, on occasion, where there is an insufficient criminal nexus, are sent directly to CSIS by the Intake Officer.

A large volume of external tasking comes to O-INSET through the NSOB, which means that a significant amount of screening for the above-noted criteria has been completed before the matter arrives at O-INSET. Such tasking includes requests for assistance from foreign agencies. The RCMP informed the Commission that all requests for assistance from foreign agencies (even those that may be classified as "life and death") must go through RCMP National Headquarters. If a foreign agency contacts an INSET directly, it is referred to Headquarters.

Information that could trigger a national security investigation may also be passed on to the INSET Intake Officer by other domestic police agencies. Again, the Intake Officer decides whether the INSET will take on the work. The NSOB is notified of the matter as soon as a file is generated. Where a discrete piece of information is passed on to the INSET and does not lead to investigation or leads to only minimal investigation by the INSET, the NSOB may be notified

through the uploading of the information into the SCIS database. A hypothetical example given to the Commission by O-INSET was a telephone call reporting that an envelope containing an unidentified white powder had been found. The investigation of such a matter might be completed before any file was formally opened. In such a case, pre-approval for the investigation would not be obtained from the NSOB. Rather, the NSOB would be notified as the investigation was being carried out.

Information from the public received by an INSET is also screened through the Intake Officer before any action is taken, as is information not related to INSET officers' files that comes to the officers' attention in the course of investigations. In addition, the Intake Officer reviews police reports, such as the Canadian Police Information Centre printouts of virtually all crimes reported, to determine whether any might have a national security nexus.

The Intake Officer also monitors investigations in other areas for indications of a national security nexus. If there is a deemed national security link, the INSET becomes involved. Whether the file is moved to the INSET or INSET officers work with the originating department depends on the nature of the national security link. According to the RCMP, in all such cases, full reporting on the file takes place through the INSET to the NSOB, and all national security policies and procedures apply.

O-INSET's work is divided roughly into day-to-day investigations and long-term projects. Day-to-day investigations may be subdivided into short-term investigations and mini-crises. A matter that falls in the former category will usually be handled by a member of O-INSET's Quick Response Team. Mini-crises and exigent circumstances may necessitate on-the-spot decision making, precluding prior "formal" approval from RCMP Headquarters. In such circumstances, both National Headquarters and the Division Criminal Operations Branch are notified immediately of any action taken. In addition, both are kept apprised of developments, and subsequent reviews and approvals are sought as soon as possible.

Longer-term projects involve a more formalized approval process. They begin with strategic analysis of criminal intelligence, focusing on emerging trends, such as what groups or entities appear to be involved in criminal behaviour with national security implications. The analyses are sent to RCMP Headquarters as part of the priority-setting process. Each spring, strategic priorities are set by National Headquarters in Ottawa. Work continues on a strategic priority until such time as the investigation stops or the matter becomes a tactical priority. Tactical priorities are set each fall. When a matter becomes a tactical priority, the purpose of the investigation becomes the disruption of criminal

activities and/or the laying of criminal charges. Both strategic and tactical priorities are ultimately determined by the Criminal Operations Branch. The Division Criminal Operations Branch is the first line of reporting and approval before a major investigation is undertaken. The Branch reviews investigative plans to ensure they comply with policy and procedure and then forwards them, with its support and approval, to the NSOB, where they are subjected to further review. The ultimate authority is the Assistant Commissioner, CID.

Both strategic and tactical priorities involve investigation and collection of information. While prosecution of criminals is a goal, not all information collected meets the criteria of evidence. In any event, all such information remains in the SCIS database until removed in the ordinary course of operations.[33]

Although this is not usual procedure, at the time the Commission met with O-INSET, it had conducted a joint investigation with the FBI. Moreover, the FBI or other law enforcement agencies have at times conducted criminal investigations involving subjects also being investigated by the RCMP. In those cases, information was shared and the agencies co-operated with one another. On one occasion, FBI personnel were involved as observers in an investigation in Toronto because it related to an alleged threat to American interests. According to the RCMP, investigations in all such cases were coordinated centrally.

O-INSET has its own Source Development Unit, which is tasked by INSET members who identify human source needs. Once developed by the Source Development Unit, sources are handed over to the investigating officers who require them.

O-INSET also includes a Special Operations Center. This is a technologically advanced room with video screens on the walls and five or six rows of computer stations. The Center is available for monitoring/coordinating major events, such as the El Al incident mentioned above or a visit to Toronto by a foreign dignitary. Computer stations are available for the use of each of the INSET partners, providing them with access to their respective home networks. Information may then be shared in the context of the event being monitored or coordinated. None of the terminals has SCIS access, but three O-INSET offices in the Center do have access to that system, and one also has links to Canadian embassies and high commissions abroad. While foreign agencies do not have stations within the Special Operations Center, they can be connected to the Center by phone, computer or video link as necessary.

IBETs

Integrated Border Enforcement Teams (IBETs) also have a mandate related to national security. IBETs, which are referred to in the 32-point Action Plan

attached to the Smart Border Declaration,[34] are responsible for enhancing border integrity and security by identifying, investigating and interdicting persons and organizations that pose a threat to national security or are engaged in organized criminal activity. This includes threats from terrorism, as well as the smuggling of drugs, humans, cigarettes and other substances. There are IBETs deployed in 25 locations along the Canada-U.S. border. Unlike INSETs, IBETs include both U.S. and Canadian law enforcement agencies. They may have personnel from the CBSA, U.S. Immigration and Customs Enforcement, U.S. Customs and Border Protection, state, provincial and local police agencies on both sides of the border, and the U.S. Coast Guard, in addition to RCMP personnel. However, international personnel act as liaison resources only.[35] IBET members pass information to INSETs if the information or intelligence relates to a national security offence. INSETs take the lead in any ensuing investigation, supported by the IBET as required.

To gain a better understanding of how these teams operate, the Commission conducted a detailed examination of the Windsor IBET. It found that the IBET in question — indeed, as I understand it, IBETs in general — do not have a significant national security role. Currently, their main focus is the illegal movement of goods and individuals across the Canada-U.S. border between official ports of entry. With respect to national security, IBETs act as "eyes and ears" for INSETs at the border, passing on to them any information they identify as related to national security. In addition, members of IBETs are available to be tasked by INSETs. The Windsor IBET has received such taskings from time to time, with O-INSET taking the lead.

The Windsor IBET is made up of the following core partners: the RCMP, the CBSA, U.S. Immigration and Customs Enforcement, the U.S. Coast Guard and U.S. Customs and Border Protection. It also has one member seconded from the Ontario Provincial Police (OPP). In addition, two members of O-INSET are co-located with the Windsor IBET. IBET core partners are not integrated as a team in the same way as INSET members. For example, partner personnel do not go out on an investigation with RCMP officers. Each partner works independently of the others. The primary purpose of co-location is to facilitate information sharing.

One of the O-INSET officers co-located with the IBET reviews IBET activity reports for anything of interest from a national security perspective and reports such information to O-INSET. Access to SCIS and other national security information is through the INSET only.

In addition to its operations or investigative side, the IBET has an intelligence section, which is involved in producing two intelligence products: the

monthly IBET Division Report and the annual Canada-U.S. Between-Ports Risk Assessment (BPRA). The Division Report takes raw information obtained by the IBET and processes it into intelligence. Its purpose is to establish patterns of criminal activity and determine the priority to be assigned to investigating individuals and organizations involved in criminal activities that would be of serious consequence in the community. The focus of the report is the illegal movement of goods and people. It contains protected information, but no national security or top secret information. Although primarily prepared for the IBET's use, the Division Report is funnelled through RCMP divisional intelligence into a monthly divisional intelligence report.

The BPRA, compiled with the cooperation of the IBET's core partners and other law enforcement agencies, profiles criminal activity in terms of geography, demographics, infrastructure, roots and the criminal organizations involved. The Commission was informed that the primary purpose of the BPRA is the identification of risks associated with the illegal movement of goods and people across the border. However, its review of a BPRA revealed that it contained national security information, including information about suspects and possible links to terrorist groups. When it enquired about this, it was told that the information had been supplied by the INSET, but had not been considered top secret. The BPRA is distributed to IBET core partners in Canada and the United States. IBET partners meet regularly to exchange information. No national security information may be shared at the meetings.

4.
OVERLAP WITH OTHER AREAS OF RCMP

The foregoing description of the RCMP's national security activities may suggest that such activities are wholly distinct and separate from the Force's other law enforcement activities. This is not accurate. While national security activities are subject to different policies and different chains of command than other RCMP activities, and while the personnel engaged in those activities generally work in separate branches, sections and units, there is overlap between those activities and the Force's other activities, and between the personnel assigned primarily to national security operations and those assigned elsewhere. As I discuss in Chapter XI, such overlap has important implications for the issue of a review mechanism, particularly in regard to the required scope of the mechanism's powers.

One reason for the overlap is the previously mentioned fact that not all criminal investigations start out as national security investigations and not all investigations that begin as or become national security investigations remain so.

To give a simple illustration of the first circumstance, an RCMP officer might stop a driver on suspicion of impaired driving and, while investigating, discover explosives in the vehicle. Further investigation could yield information to suggest the possible commission of a national security offence. The potential for this type of overlap is illustrated by the nature of the terrorist offences set out in the *Criminal Code*. As I note in Chapter III, these include activities that may otherwise be illegal and become terrorist offences when perpetrated in furtherance of the objectives of a terrorist group. Moreover, the RCMP informed the Commission that there have been investigations that began as ordinary criminal investigations, were transferred to an INSET following identification of a potential national security nexus, and were then transferred back when it was determined that there was no national security nexus.

The overlap between the RCMP's national security operations and other areas of activity also extends to its personnel. As I mention in the discussion concerning INSETs above, in some cases where a possible national security nexus is discovered, the INSET does not take over, but an INSET officer works with the originating department on the investigation. Even when the investigation is overseen by the INSET, non-INSET RCMP personnel continue to work on it. Although IBET personnel appear at the present time to be primarily engaged in investigating crimes related to the smuggling of goods or people, they nevertheless are available to assist INSETs. Similarly, in parts of Canada where there are no INSETs or NSISs, ordinary RCMP officers assist in national security investigations. Finally, in cases of emergency, the RCMP may be compelled to use personnel from other areas of the Force. As I note above, the co-location of the CFSEU with O-INSET is deemed beneficial, as CFSEU personnel could conveniently be called upon in the event of a national security crisis situation.

There is overlap with other police agencies as well. An investigation begun by a provincial or municipal police force may develop into a national security investigation. In such an instance, it may be transferred to the RCMP or continued in conjunction with it. I discuss the interaction between the RCMP and other police agencies in Section 6 below.

5. INFORMATION AND INTELLIGENCE MANAGEMENT, RETENTION AND SHARING

An important component of the RCMP's national security activities involves the collection, management, retention and sharing of information and intelligence. While the broad range of information and intelligence collected and retained by the RCMP includes some that is directly related to potential prosecutions or

could be related to prosecutions, it also includes some better described as "contextual" or background information or intelligence. I have not undertaken an analysis of the nature of the contextual information and intelligence collected and stored by the RCMP. However, I did make recommendations in my Factual Inquiry report with regard to the mandate of the RCMP and the importance of ensuring that the RCMP intelligence gathering function is restricted to the RCMP's law enforcement mandate.

In this section, I describe the storage and dissemination of such information. The discussion is divided into three topics: where national security information acquired by the RCMP comes from and what information is entered into the database; how the information is stored and maintained; and how it is disseminated.

5.1
INFORMATION COMING INTO THE RCMP

At the core of the RCMP's national security information management system is the Secure Criminal Information System (SCIS), a classified database that stores all information and intelligence with a national security dimension. SCIS is separate from all other RCMP databases. There are other criminal intelligence databases, including databases that are shared with other police agencies. An example is the Automated Criminal Intelligence Information System (ACIIS), which is available to all police agencies that are members of Criminal Intelligence Service Canada. However, the RCMP informed the Commission that national security information and intelligence in its possession is stored exclusively on SCIS.[36]

National security information and intelligence entered into SCIS comes from a variety of sources. Some is obtained internally, as a result of investigations by field officers. A significant portion is acquired from external sources, both domestic (CSIS, other police agencies and government departments, for example) and international, including foreign police and intelligence agencies. Information is entered into SCIS either by CID or by INSET or NSIS officers.

The decision to include information in SCIS is left to the judgment of the person entering it. The criteria applied are straightforward: relevance and importance to a national security investigation. The overall approach is one of broad inclusion,[37] for a number of reasons. First, the RCMP is bound to ensure that all investigation files are complete, in accordance with the standards set by the Supreme Court of Canada in the *Stinchcombe* case.[38] Complete files must include both inculpating and exculpating information concerning the accused. Information often includes some about individuals with whom the target of the

investigation has come into contact. The RCMP has noted in this regard that seemingly benign information can provide a potential accused with alibi evidence. Further, given that an individual may surface numerous times during the course of an investigation, having information in the file about that individual ensures that he or she is not repeatedly reinvestigated. The RCMP has also noted that the status of an individual may change during the course of an investigation. An individual who is a complainant, witness or person of interest in the early stages may ultimately be implicated in a crime.

The broad inclusive approach for national security information is also based on a risk analysis undertaken by the RCMP. The RCMP has indicated that, given the extremely serious consequences of national security crimes, there is too much at stake not to take an inclusive approach in deciding what information is to be entered into the data bank.

Certain information about the quality of the information is also entered into SCIS. In many cases, both the source and the information itself are classified according to the following scale:

- **Reliable (R)** is a combination of proven accuracy of information and proven dependability as a person. Every effort must be made to validate information before grading it reliable.
- **Believed Reliable (BR)** applies if the qualifying conditions of reliable are not yet met, but the existing knowledge of the source is favourable and it is believed he/she will eventually prove reliable.
- **Unknown Reliability (UR)** applies if there is insufficient experience with the source for assessment or when information cannot be verified.
- **Doubtful Reliability (DR)** applies if there is doubt about the source or the information.
- Information for court purposes must include a "**C**" in the assessment, e.g., **BRC**, Believed Reliable – can be used for court purposes.[39]

These ratings are not always included with information. For example, in cases where a field officer observed conduct himself or herself, it is assumed such information is of the highest quality. In addition, information received from outside sources may not be classified or may be classified differently. In such circumstances, all available information on the quality of the source and information is uploaded into the system. I made several recommendations in the Factual Inquiry report with respect to the assessment of the reliability and accuracy of information.

Much of the information received by the RCMP from outside sources contains caveats, or restrictions on the use to which the information can be put and

on further dissemination. I discuss caveats in more detail below. I raise them here merely to note that any caveats are entered into the system as well.

Finally, the level of protection or classification (e.g., Top Secret) of the information is also recorded in the system.

5.2
INFORMATION STORAGE AND MAINTENANCE

SCIS is a protected system and it is RCMP policy to classify all information in the data bank. However, the system is designed to allow any RCMP program area to access it under specific conditions. The Commission was advised that general access is restricted to RCMP personnel involved in national security matters who have the appropriate security clearance, on a need-to-know basis. Non-RCMP members seconded to INSETs also have access to SCIS, but for INSET investigative purposes only.[40] Non-RCMP members not seconded to INSETs (members of other agencies with which the RCMP is conducting a joint investigation, for example) and non-RCMP members assigned to IBETs do not have direct access to SCIS. However, access to specific information can be provided on a need-to-know basis and information in the system can be shared with others on the same basis.

The RCMP's Secure Criminal Information System Section performs periodic quality reviews of the data entered into the system to ensure the integrity of the information and compliance with RCMP policies and procedures. Such reviews must also be conducted by each of the unit commanders in the divisions.

All police files, regardless of the storage medium, have a retention and disposal schedule developed by the Information Management Branch, in accordance with various legislative requirements. All retention and disposal schedules must conform to federal legislation and policies and be approved by the National Archivist. When a "concluded date" is entered for a particular occurrence, the system automatically generates a purge date for the removal of the information. It should be noted that, given their nature, many national security investigations remain open and files are therefore not subject to purge for a considerable length of time. When a file is set to be purged, its contents are either destroyed or archived as historical data. Historical files are typically major national security-related criminal investigations, such as the investigation into the bombing of the Air India flight or the attacks on the World Trade Center. These investigations are considered to be of such importance that the file contents are stored indefinitely. The RCMP informed the Commission that such files are reviewed regularly and if it is determined that they no longer satisfy this criterion, they are destroyed.

5.3 INFORMATION SHARING AND DISSEMINATION

The RCMP obviously makes its national security information and intelligence available for internal purposes. While National Headquarters assumes responsibility for coordination, RCMP members of NSISs and INSETs have access to such information and intelligence as needed. Other programs and units within the RCMP may also be given access, depending on requirements.

The RCMP also shares national security information and intelligence with other agencies, both domestic and foreign. It is bound by agreement and, in some circumstances, required by legislation to share information with others. For example, the RCMP is obligated under the CSIS-RCMP Memorandum of Understanding[41] to provide CSIS with information relevant to the CSIS mandate. Certain international treaties and conventions contemplate the sharing of information related to terrorism and other national security matters. Moreover, there are times when circumstances, such as emergencies, will require the RCMP to share information.

Although National Headquarters generally handles requests for information and decisions as to whether and what information will be provided to other agencies, informal information sharing regularly takes place at the field officer level. For example, in circumstances where there is a joint investigation with another police agency, information exchanges may take place on an officer-to-officer basis.

The RCMP has well in excess of 1,000 MOUs with other agencies on matters such as training and sharing of police technologies and services, and there are a number of written agreements in place respecting the sharing of various types of data such as fingerprints, criminal records and DNA. In contrast, however, RCMP national security information exchanges are not generally governed by formal written agreements, with the exception of the CSIS–RCMP MOU.

There are few ministerial directives and RCMP policies dealing directly with the exchange of national security information and intelligence. While a number of directives and policies relate to agreements with other entities, they are not interpreted as applying to all such interactions. For example, the April 2002 Ministerial Directive on RCMP Agreements is interpreted by the RCMP as applying only to those agreements that would bind the Government of Canada. This includes agreements to supply training, equipment or know-how to another country, but not agreements regarding information exchanges. I disagree with this interpretation.

A more specific directive, the Ministerial Direction Regarding National Security Related Arrangements and Cooperation, issued in November 2003, covers exchanges of information by the RCMP, but is restricted to arrangements and co-operation with foreign security and intelligence organizations. It does not apply to foreign law enforcement agencies. Thus, while the directive and related policy would apply to arrangements and co-operation between the RCMP and the CIA, they would not apply to interactions between the RCMP and the FBI. This directive requires the RCMP to have a written record of oral agreements with foreign security or intelligence agencies, seek prior ministerial approval, and report annually to the Minister on the status of written and oral arrangements with foreign security or intelligence organizations.

During this Inquiry, the RCMP has been working on developing an MOU template and guide respecting criminal information sharing (including national security information sharing) to help manage the exchange of information and intelligence with outside agencies and ensure compliance with applicable laws and regulations. This generic MOU will codify guiding principles and expectations governed by appropriate legislation and serve as a management tool for information and intelligence sharing. However, the RCMP has told the Commission that the template is not intended to replace case-by-case information sharing among police agencies in accordance with accepted principles.

Despite the absence of formal written agreements, the RCMP has relationships and information sharing arrangements with many other police agencies in Canada and abroad. According to the RCMP:

> Virtually every major investigation has multi-jurisdictional aspects, as such information sharing among enforcement agencies is crucial to the successful resolution of these investigations.
>
> To negotiate and maintain written agreements with all agencies that provide or receive information internationally and domestically would effectively bring investigations and international cooperation to a halt.
>
> There are over 18,000 law enforcement agencies in the U.S. alone.
>
> Some agencies, especially security intelligence agencies, refuse to enter into written agreements and prefer to rely upon verbal agreements and professional standards within the law enforcement and intelligence community to protect their information.[42]

Consequently, national security information sharing is both frequent and relatively informal.

The RCMP told the Commission that relationships are governed by common understandings and protocols. Some are quite clear. An example is the use of

caveats, which I discuss below. However, others involve relatively general statements, such as statements to the effect that decisions with respect to information sharing are to be guided by "the broader policy objectives and values of the Canadian government."[43]

Some guidance pertaining to information sharing is provided in the RCMP *Policy Manual*. For example, in respect of enquiries from foreign governments, the RCMP's *Operational Manual* provides that:

> The RCMP will not become involved or appear to be involved in any activity that might be considered a violation of the rights of an individual, unless there is a need to comply with the following international conventions:
>
> 1. United Nations Conventions on the Prevention and Punishment of Crimes Against Internationally Protected Persons, including Diplomatic Agents, article 4(b) or through membership in such bodies as Interpol;
> 2. the 1979 International Convention Against the Taking of Hostages;
> 3. the 1971 Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation (Montreal);
> 4. the 1970 Convention for the Suppression of the Unlawful Seizure of Aircraft (The Hague); or
> 5. the 1963 Convention on Offences and Certain Other Acts Committed on Board Aircraft (Tokyo).[44]

In the Factual Inquiry report, I expressed some serious reservations about this approach, as it appears to exempt some terrorism investigations from the primary requirement of not being involved in rights violations.

The Manual also provides that:

> The disclosure of information to an agency of a foreign government that does not share Canada's respect for democratic or human rights may be considered if it:
>
> 1. is justified because of Canadian security or law-enforcement interests,
> 2. can be controlled by specific terms and conditions, and
> 3. does not have a negative human rights connotation.[45]

Guidance is also provided by the *Canadian Charter of Rights and Freedoms* and Canadian privacy legislation. Deputy Commissioner Garry Loeppky testified in the Factual Inquiry hearings that the RCMP would not provide information to a foreign agency if it knew that the agency would use the information to violate the rights of a Canadian citizen.[46] However, I am not aware of any guidelines covering more specific issues, such as what level of certainty is required that no rights violation will occur before information can be passed on,

or who should make the assessment about whether such level of certainty exists.[47] As I indicated in my recommendations in the Factual Inquiry report, more formalized rules and guidelines relating to information sharing are required.

RCMP policy[48] cautions that disclosure of personal information must be made in accordance with the *Privacy Act*. That legislation generally prohibits the exchange of personal information without the consent of the person to whom the information relates, subject to specific exceptions, two of which are commonly relied upon by the RCMP. The first is "consistent use disclosure," which provides that, where personal information is collected for one law enforcement purpose, it may be released for another such purpose without the consent of the individual involved. The term "law enforcement purpose" is interpreted to include law enforcement in other jurisdictions. The second exception is "public interest disclosure," which allows disclosure in circumstances where the public interest in disclosure clearly outweighs any privacy interest. Disclosure is also allowed under agreements or arrangements with other domestic police bodies or security and intelligence bodies and their international counterparts. This exception requires written requests for information and permits disclosure of only that portion of personal information actually required. Other exceptions set out in RCMP policy are relied on less frequently by the RCMP. The decision about whether an exception applies is made by the individual who releases the information.

It is important to note that the use of caveats by the RCMP and the agencies from which it obtains information is common. Caveats outline the conditions under which information is provided to or by another agency and specify directions/conditions respecting its use and further dissemination. The RCMP *Operational Manual* sets out the following caveats for the dissemination of national security information by the RCMP:

1. The following condition must be included in all outgoing correspondence, messages and documents being passed to CSIS, other federal government departments, and any Canadian police force.

   This record may be subject to mandatory exemption under the Access to Information and Privacy Acts. If access is requested under that legislation, no decision to disclose should be taken without prior consultation with the Departmental Privacy Coordinator of the RCMP.

2. The following conditions must also be included in all outgoing correspondence, messages and documents being passed to other domestic and foreign law enforcement agencies/departments.

> This document is the property of the RCMP. It is loaned to your agency/department in confidence and it is not to be re-classified or further disseminated without the consent of the originator.
>
> This document is the property of the Government of Canada. It is provided on condition that it is for use solely by the intelligence community of the receiving government and that it not be declassified without the express permission of the Government of Canada.[49]

The RCMP told the Commission that there is a well-established understanding in law enforcement and security communities that caveats similar to the ones set out in the RCMP *Operational Manual* are implied, even when they are not stated explicitly. I made recommendations in respect to the use of caveats in the Factual Inquiry report.

In addition to caveats, reliability ratings assigned to information entered into the SCIS database are provided to outside agencies when information is shared.

6. INTEGRATION AND INTERACTION WITH OTHER FORCES AND AGENCIES

The final topic I address in this chapter is the integration and interaction of the RCMP and other national security actors. Since 9/11, there has been increasing participation by a growing list of federal actors in the response to threats to Canada's national security, in particular the response to terrorist threats. In Chapter V, I describe the national security activities of 22 federal actors and selected provincial and municipal police agencies. Concurrent with the growth in number of national security actors, there has been an increase in interaction and integration among such agencies.[50] This to some extent is an inevitable consequence of Canada's multi-agency approach to addressing threats to national security. Several agencies may, for their own reasons, have an interest in the same threats or events. It makes sense, from the viewpoint of efficiency and also to ensure that each agency has all relevant information at its disposal, to have such agencies co-operate and share information in appropriate circumstances.

The changing nature of crime has made integration a critical element of effective policing. I agree with the submissions on this point made by Paul Kennedy, Chair of the CPC, during the Policy Review public hearings. He identified four factors that characterize this change. The first is globalization, which has resulted in the virtually worldwide rapid movement of goods and people. In the criminal context, this has manifested itself in transnational organized

crime, including terrorist crime. The second is the now-widespread availability of sophisticated means of communication, including the Internet, and publicly available encryption. The latter provides private individuals with means of communication that are difficult to apprehend and decipher. The availability of such new forms of communication has changed criminal behaviour. For example, fraud no longer requires face-to-face interaction or even interaction by phone or mail. The Internet gives criminals relatively instantaneous access to millions of people in many jurisdictions. The third factor noted by Mr. Kennedy is the fact that criminals are forming new partnerships. The traditional silos of organized crime groups are breaking down and being replaced by new, sometimes temporary alliances that cross jurisdictional boundaries. The final factor is the emergence of new threats, including threats of terrorism. While terrorism is not new, the last 10 years have seen the proliferation of new forms of terrorism with a strong international component.[51]

As a result, to quote Mr. Kennedy:

> [M]odern policing reality is that some of these challenges can't be addressed by individual police forces acting alone. That is just the reality. There is an obvious need for police to combine resources, both human and financial, and to maximize unique skillsets. . . .
>
> To address these challenges police forces have integrated their operations and they have adopted intelligence-led policing models which engage multiple partners at the municipal, provincial, federal and international level. This is the new norm. . . .
>
> This inter-agency co-operation finds expressions at all levels of the public safety framework. In other words, it isn't just police doing this.[52]

Similar views and conclusions were expressed at the public hearings by Commissioner Giuliano Zaccardelli of the RCMP,[53] Commissioner Gwen Boniface of the OPP[54] and Chief Vince Bevan of the Ottawa Police Service (OPS).[55]

Today, integration and interaction with other police forces and government agencies have become key parts of the RCMP's national security activities, and there is every indication that they will continue and likely increase. I discuss some of the interaction that takes place (between the RCMP and CSIS and in INSETs and IBETs, for example) in Chapter II and earlier in this chapter, and provide other examples of integration and interaction in Chapter V. Below, I describe in general terms the types of interaction engaged in by the RCMP in carrying out its national security mandate and the range of other agencies with which it interacts.

Interaction between the RCMP and other national security actors generally fits into one of two categories: formal integration and less formal interaction.

6.1 INTEGRATION

Formal integration involves entities made up of personnel from various agencies, under the control and direction of one agency. The RCMP is currently involved in three formally integrated units: INSETs, IBETs, and the Integrated Threat Assessment Centre (ITAC). INSETs, which are described in detail above, are the RCMP's primary integrated national security investigation units. While their main function is investigative, they also perform intelligence analysis. INSET members seconded from other police services, both provincial and municipal, are fully integrated into all INSET functions. While INSETs are headed by members of the RCMP, individual investigations may be led by officers whose home agencies are provincial or municipal police services. This degree of integration does not occur with respect to persons seconded from non-police agencies. For example, CSIS personnel seconded to INSET do not participate as police officers. Instead, their role is to provide the INSET with the expertise gained as CSIS members.

IBETs, which are also described above, represent a different form of integration. Even police personnel seconded to an IBET from provincial or municipal services do not generally assist the IBET's RCMP officers with investigations, at least not directly. The IBETs are more akin to co-location arrangements than to full integration in this respect, their primary purpose being information sharing. IBETs also include U.S. agencies, both police and civilian.

At the time the Commission was looking into the RCMP's national security activities, the Force also had Integrated Immigration Enforcement Teams (IIETs), comprising mainly RCMP and CBSA personnel. The Commission visited the Toronto IIET, which was co-located with the RCMP's Immigration Task Force (ITF). Most of the work done at the Toronto IIET was immigration warrant apprehension, which was driven by the CBSA, which transferred work to both the IIET and the ITF. In the course of its operations, the IIET passed relevant information on to the INSET, and it was open to the INSET's taking over or supervising IIET investigations.

There were plans for the IIETs to have their own national security projects (such as passport fraud) and to be tasked by INSETs to undertake investigations. However, on April 1, 2005, the RCMP dismantled the IIETs and redeployed the resources to INSETs. The ITF (which includes CBSA personnel) has taken

over the IIET warrant apprehension function, and supports INSETs by providing both information and investigatory assistance as required.

The last formally integrated entity with which the RCMP is currently involved in the national security area is the Integrated Threat Assessment Centre, or ITAC, which I describe in detail in Chapter V. It is a unit comprising personnel from many federal and provincial national security actors, the objective of which is to develop comprehensive national security threat assessments. ITAC differs from INSETs in that it is not under the direction and control of the RCMP. Instead, the head of ITAC (who, at the time the Commission met with ITAC, was an RCMP officer seconded to the Centre) reports to both the Director of CSIS and the Prime Minister's National Security Advisor.

Other potentially integrated operations are under development. For example, as part of its National Security Policy, the government has announced the creation of Marine Security Operations Centres (MSOCs), the role of which will be to detect, assess and respond to marine threats to national security. MSOCs will be headed by Canadian Forces Maritime Command, Department of National Defence (DND), and include staff from the CBSA, Transport Canada, the RCMP and the Canadian Coast Guard. MSOCs are currently at the development stage and the precise rules and relationships among participants have not yet been finally settled.[56]

6.2 INTERACTION

In addition to participating in formally integrated units, the RCMP interacts with other agencies involved in national security activities on a less structured basis. Interaction may be with other federal national security actors, provincial and municipal police services, and foreign agencies.

6.2.1 Other Federal National Security Actors

The RCMP interacts with a broad range of federal actors in the national security field, including CSIS, the CSE, CIC, the CBSA, DFAIT, FINTRAC, the Canada Revenue Agency, Transport Canada, the Canadian Air Transport Security Authority (CATSA), DND and the Canadian Coast Guard. Details concerning such interaction are set out in Chapter V and I do not repeat them here.

The vast majority of the interaction involves information sharing. In some instances, however, it takes the form of operational assistance. An illustration is the joint RCMP-CIC investigation[57] into the Ottawa Business College in Toronto that eventually led to the arrest of 33 people, all but one of whom were from

Pakistan.[58] These arrests received extensive media coverage and were also the source of a public complaint against the RCMP.[59] The joint investigation arose out of an assignment given by the Government of Canada to the RCMP and CIC that involved "identifying, locating, and processing individuals illegally in Canada who were identified as originating from" source countries, including Pakistan, that had been identified as terrorism threats to Canadian interests.[60] In May 2003, it came to the attention of the RCMP and CIC that the Ottawa Business College was providing fraudulent student documents to allow individuals to remain in Canada illegally. The RCMP and CIC identified 31 individuals to be investigated and arrested pursuant to the *Immigration and Refugee Protection Act*. Investigation of those 31 determined that some had engaged in "suspicious" behaviour that, according to the CPC, could be viewed as supporting the premise that they might pose a threat to national security.[61] Arrests were made under the *Immigration and Refugee Protection Act*. The RCMP's role was to assist CIC with the execution of its arrest warrants. The investigations and arrests were conducted jointly by RCMP and CIC officers.

6.2.2 Provincial and Municipal Police Agencies

The RCMP also interacts regularly with municipal and provincial police agencies across Canada on matters related to national security. This includes interaction in the context of integrated units such as INSETs, secondments to the RCMP, including secondments to national security units such as NSISs, joint investigations and also less structured interaction. The interaction includes both information sharing and operational activities.

Under the *Security Offences Act*, the RCMP has primary responsibility for the investigation, prevention and prosecution of criminal activities related to national security.[62] However, this does not mean that there is no involvement in such investigations by provincial or municipal police forces. Such involvement can take a number of forms.

It is important to bear in mind that it is not always clear at the outset of an investigation whether or not it will be a national security investigation. During the public hearings, OPS Chief Vince Bevan provided a hypothetical example of a 911 call to the Ottawa Police reporting that an individual with a gun has entered a downtown building. Inside the building are offices for private businesses and for a federal minister. The Ottawa Police have jurisdiction over the entire building, but not for the Minister — the Minister's safety and security are the RCMP's responsibility. The Ottawa Police would stay in constant contact with the RCMP, but might not know what the suspect's motives are, or whether the

Minister is present in the office. As more information is obtained and corrected, jurisdiction over the incident might shift back and forth between the RCMP and the Ottawa Police.[63]

Even in cases where a national security nexus is identified and the RCMP becomes involved, there is often a continuing role for municipal or provincial police forces. Many national security investigations have local implications. For example, a terrorist threat in a major Canadian city could raise many issues within the jurisdiction of the municipal or provincial police force concerned, requiring its involvement as well as that of the RCMP. The RCMP has entered into formal agreements with a number of provincial and municipal police services to set out protocols and procedures for dealing with national security criminal investigations, including procedures for determining which agency will take the lead in an investigation and what the reporting responsibilities will be. These agreements recognize that the jurisdiction and responsibilities of local police forces do not necessarily end because national security interests are involved and that criminal threats to national security are more effectively addressed when all levels of police work together. I provide a description of the range of such co-operative endeavours in Chapter V.

RCMP and other law enforcement representatives who made submissions to the Commission emphasized the importance of co-operation and integration between the RCMP and local police forces in national security policy. Such co-operation represents "a strategic response to the complications arising out of jurisdictional issues, the compartmentalization of information, disparate expertise, and the financial burden to be shared in complex investigations."[64]

6.2.3 U.S. and Other Foreign Agencies

The RCMP has extensive interaction with foreign law enforcement agencies, particularly those in the United States, and such interaction has increased since the events of 9/11. It also interacts with foreign security intelligence agencies, although it has indicated to the Commission that such contacts are less frequent. As I discuss above, interaction between the RCMP and foreign security intelligence agencies is subject to the terms of a ministerial directive issued in November 2003, which requires consultation with CSIS and DFAIT, as well as ministerial approval before such agreements are entered into. The directive also requires that all such agreements be in writing. There are no similar requirements with respect to agreements with foreign law enforcement agencies.

Most interaction with both foreign law enforcement agencies and intelligence agencies is for the purpose of information sharing. The importance of

international co-operation in response to threats of terrorism has been recognized by the international community, particularly since 9/11. UN Security Council Resolution 1373 (2001) calls upon all states to:

- Find ways of intensifying and accelerating the exchange of operational information, especially regarding actions or movements of terrorist persons or networks; forged or falsified travel documents; traffic in arms, explosives or sensitive materials; use of communications technologies by terrorist groups; and the threat posed by the possession of weapons of mass destruction by terrorist groups;
- Exchange information in accordance with international and domestic law and cooperate on administrative and judicial matters to prevent the commission of terrorist acts; and
- Cooperate, particularly through bilateral and multilateral arrangements and agreements, to prevent and suppress terrorist attacks and take action against perpetrators of such acts.[65]

Other international conventions such as the United Nations Convention against Transnational Organized Crime and the International Convention for Suppression of Terrorist Bombings and treaties such as the International Convention for the Suppression of the Financing of Terrorism also require co-operation and information sharing by law enforcement agencies.

As I note above in the discussion on dissemination of information, there are few MOUs or other written agreements governing the relationship between the RCMP and foreign agencies. Also as I note above, the RCMP has internal policies and procedures respecting both the acceptance and dissemination of information from foreign agencies. In the Factual Inquiry report, I made recommendations for improvements to those policies and procedures.

In addition to sharing information, the RCMP has carried out joint investigations with foreign police services. Such investigations are undertaken when an investigation has cross-border implications. While each police force is restricted to matters within its own jurisdiction, joint investigations may involve joint planning, execution and information sharing. In the context of joint investigations, RCMP officers have asked foreign police forces to interview witnesses and have travelled to other countries to participate in interviews conducted by foreign police agencies.

Notes

1 Unless separate references are provided, the information in this chapter was obtained by the Commission in interviews with RCMP personnel and in follow-up correspondence to such interviews.

2 R.S.C. 1985, c. R-10, s. 5.

3 Exhibit P-12, Tab 22, Arar Commission Factual Inquiry.

4 Ibid., Tab 23.

5 Ibid., Tab 24, pp. 3–5.

6 Ibid., pp. 6–8.

7 Ibid., pp. 9–10.

8 *Royal Canadian Mounted Police Regulations*, S.O.R./ 88-361, ss. 37–58.7.

9 RCMP letter to Commission counsel, June 7, 2004, including attachments [RCMP letter of June 7, 2004].

10 Ibid., Appendix A, "Adjudications Branch."

11 "Submissions of the RCMP External Review Committee" (Written submission, Arar Commission Policy Review Public Submissions), November 3, 2005.

12 Ibid.

13 Ibid.

14 Ibid.

15 RCMP letter of June 7, 2004 (see note 9).

16 Ibid., Appendix B, "Internal Audit Charter for the RCMP."

17 Ibid.

18 *Royal Canadian Mounted Police Act*, R.S.C. 1985, c. R-10, ss. 24.1(1)–24.1(11) (as am. by *An Act to amend the Royal Canadian Mounted Police Act and other Acts in consequence thereof*, R.S.C. 1985, c. 8 (2nd Supp.)).

19 I describe the Criminal Extremism Analysis Section in Section 3.4 of this chapter.

20 An additional 163 (including 108 regular RCMP members, 18 on secondment from other police forces and government agencies, and 18 civilian members) are assigned to Integrated Border Enforcement Teams, which play a support role in national security investigations (described in Section 3.5 of this chapter). Figures current as of January 2006.

21 CSIS provides approximately 30 percent of the information received by the NSIB.

22 Other domestic government departments and agencies include the Communications Security Establishment, the Department of National Defence, Citizenship and Immigration Canada, the Financial Transactions and Reports Analysis Centre of Canada, Foreign Affairs and International Trade Canada, the Department of Justice and the Canada Border Services Agency.

23 The CROPS prioritization process involves setting priorities for the RCMP as a whole. It takes place primarily at the divisional rather than the headquarters level.

24 For example, the RCMP has in the past tasked the Communications Security Establishment by identifying individuals overseas on whom more information is required.

25 The RCMP defines "criminal extremism" as the commission of criminal acts for ideological motives or in furtherance of ideological goals. The motivating ideologies may be political or religious. This is intended to exclude crimes committed for personal gain alone and crimes committed for other personal reasons.

26 In Chapter III, I discuss the listing of terrorist entities pursuant to s. 83.05 of the *Criminal Code*, R.S.C. 1985 c. C-46 (as am. by the *Anti-terrorism Act*, S.C. 2001, c. 41).

27 RCMP internal policies provide that all anti-terrorism investigations are to be conducted by NSISs or INSETs and, as a rule, all national security investigations are in fact undertaken by these units. In a limited number of cases, however, such investigations are conducted by other

units, in close co-operation with an INSET or NSIS. This occurs, for example, when a national security nexus has not yet been clearly established.

28 As noted farther on, information sharing in the case of domestic police agencies is often direct, at least between INSETs and the domestic police agency.

29 As I discuss in connection with INSETs and IBETs, RCMP national security personnel often share office premises with other national security actors.

30 As noted in Chapter III, policing with respect to internationally protected persons is included within the RCMP's national security mandate by virtue of the *Security Offences Act*, R.S.C. 1985, c. S-7.

31 Sleipnir is an analytical technique developed by the RCMP to rank organized groups of criminals in terms of their relative capabilities, limitations and vulnerabilities. The name is taken from the eight-legged horse belonging to Odin in Old Norse mythology.

32 Until 2005, the RCMP also had Integrated Immigration Enforcement Teams (IIETs). As discussed later in this chapter, in April of that year, IIETs were disbanded and their resources redeployed to INSETs.

33 See further discussion below.

34 *Smart Border Declaration: Building a Smart Border for the 21st Century on the Foundation of a North American Zone of Confidence*, Ottawa, Canada, December 12, 2001, online, Foreign Affairs and International Trade Canada, www.dfait.gc.ca/can-am/main/border/smart_border_declaration-en.asp (accessed July 20, 2006).

35 Canadian and U.S. agencies also work on joint investigations outside the context of IBETs.

36 Information and intelligence originally collected as part of another type of investigation may also be stored on other databases.

37 The RCMP *Informatics Manual*, Part I.4.D.2, provides that SCIS will be used for all national security criminal investigations and intelligence sequential records in the Criminal Intelligence Program that are initiated and concluded within a defined time frame. Any and all relevant material, whether it is unclassified, such as open source, classified or designated, may be uploaded to SCIS, as long as it is in support of national security investigations or intelligence files.

38 *R. v. Stinchcombe*, [1991] 3 S.C.R. 326.

39 Exhibit P-12, Tab 44, *Criminal Intelligence Program Guide*, Arar Commission Factual Inquiry, p. 7.

40 Such individuals are required to sign an agreement stating that they will not query SCIS for personal use or disseminate any information obtained from SCIS to outside agencies, including their home agencies.

41 Exhibit P-12, Tab 49, Arar Commission Factual Inquiry.

42 Responses from the RCMP to Questions Posed by the Arar Commission Policy Review, July 16, 2004, pp. 35–36.

43 Ibid.

44 Exhibit P-12, Tab 31, Arar Commission Factual Inquiry, s. M3a.

45 Ibid., s. M3b.

46 Loeppky testimony, Arar Commission Factual Inquiry Public Hearing (June 30, 2004), pp. 826–827.

47 See my recommendation in the Factual Inquiry report regarding rules and guidelines about when and how information should be exchanged.

48 Exhibit P-12, Tab 27, Arar Commission Factual Inquiry, s. L.2.

49 Exhibit P-12, Tab 27, Arar Commission Factual Inquiry, Appendix I-3-8.

50 In this section, "integration" means bringing personnel from various agencies together to work as a cohesive unit or entity under the control and direction of one agency. "Interaction" refers to less structured co-operative endeavours, ranging from information sharing to joint agency

operations, where the personnel involved remain under the control and direction of their respective home agencies. Having noted this distinction, in the remainder of this Report, I generally use the term "integration" to refer to the full range of co-operative activities.

51 Paul Kennedy, Chair of the Commission for Public Complaints Against the RCMP, Transcript of Arar Commission Policy Review Public Hearing (November 17, 2005), pp. 330–333.

52 Ibid., p. 333.

53 Giuliano Zaccardelli, Commissioner of the Royal Canadian Mounted Police, Transcript of Arar Commission Policy Review Public Hearing (November 18, 2005), pp. 626–635.

54 Gwen Boniface, Commissioner of the Ontario Provincial Police, Transcript of Arar Commission Policy Review Public Hearing (November 18, 2005), pp. 635–639 [Boniface, Transcript].

55 Vince Bevan, Chief of the Ottawa Police Service, Transcript of Arar Commission Policy Review Public Hearing (November 18, 2005), pp. 661–663 [Bevan, Transcript].

56 Responses from the RCMP to Questions Posed by the Arar Commission Policy Review, April 11, 2006.

57 Since the reorganization of CIC into CIC and the CBSA, the CBSA would be the entity to conduct the CIC portion of the investigations.

58 See Canada, Commission for Public Complaints Against the RCMP, *Chair's Final Report – Incident Related to National Security* (Ottawa: The Commission for Public Complaints Against the RCMP, 2006) (Chair: Paul E. Kennedy) [Chair's Final Report].

59 The CPC's investigation of this complaint exonerated the RCMP: ibid.

60 Chair's Final Report, p. 2.

61 Ibid., p. 3.

62 R.S.C. 1985, c. S.-7, s.6.

63 Bevan, Transcript, pp. 655–56.

64 Boniface, Transcript pp. 637–638.

65 UN SCOR, 56th Sess., 4385th mtg., UN Doc. S/RES/1373 (2001), art. 3, online, UN Security Council, http://daccessdds.un.org/doc/UNDOC/GEN/N01/557/43/PDF/N0155743.pdf?OpenElement (accessed February 1, 2006).

V
Canada's National Security Landscape

1.
INTRODUCTION

In this chapter, I describe Canada's national security landscape, with an emphasis on the interaction of federal departments and agencies with the RCMP. During the Policy Review, it became apparent to me that the RCMP's national security activities involve a significant degree of interaction, integration, co-operation and information-sharing with numerous federal, provincial, territorial and municipal actors. The federal government draws upon the expertise and mandates of several federal departments and agencies in pursuing an increasingly integrated and coordinated approach to national security. This is consistent with international trends. Operationally, the RCMP works with provincial and municipal police forces on national security matters.

During this Inquiry, I asked the federal government to identify those departments and agencies involved in "national security." The Privy Council Office informs me that the following federal departments and agencies have what it calls "key" national security responsibilities:

- Canada Border Services Agency (CBSA)
- Canadian Security Intelligence Service (CSIS)
- Communications Security Establishment (CSE)
- Department of Finance
- 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)[1]
- Department of Justice
- Department of National Defence (DND) and the Canadian Forces (CF)
- Health Canada/Public Health Agency of Canada

- Integrated Threat Assessment Centre
- Privy Council Office (PCO)
- Public Safety and Emergency Preparedness Canada (PSEPC)
- Royal Canadian Mounted Police (RCMP)
- Transport Canada
- Canadian Air Transport Security Authority (CATSA)

PCO identified the following departments and agencies as having national security responsibilities:

- Agriculture and Agri-Food Canada
- Canadian Food Inspection Agency
- Canada Revenue Agency (CRA)
- Canadian Heritage
- Citizenship and Immigration Canada (CIC)
- Environment Canada
- Natural Resources Canada
- Canadian Nuclear Safety Commission
- Treasury Board Secretariat (TBS)

I describe the significant national security responsibilities of these departments and agencies[2] in this chapter.[3]

Provincial, territorial and municipal police forces also have an important role in Canada's national security landscape. While a complete examination of the national security role of non-federal actors is beyond the scope of my mandate, I briefly review the role of federally-led permanent integrated teams, joint forces operations and provincially-led anti-terrorism teams, and I provide examples of day-to-day interaction by provincial and municipal police services with the RCMP and CSIS.

2.
CANADIAN SECURITY INTELLIGENCE SERVICE

2.1
RELEVANT LEGISLATION

- *Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C-23 (*CSIS Act*)

2.2
MANDATE

The Canadian Security Intelligence Service (CSIS) is Canada's civilian security intelligence agency. The Director of CSIS, under the direction of the Minister of Public Safety, has control and direction over CSIS and all matters connected with CSIS.[4]

CSIS is mandated to collect, analyze and retain information and intelligence regarding activities that, on reasonable grounds, may be suspected of posing a threat to the security of Canada. CSIS reports to and advises the federal government on these threats.[5]

The *CSIS Act* defines a "threat to the security of Canada" as:

(a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage,
(b) foreign-influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person,
(c) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state, and
(d) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada.[6]

Lawful advocacy, protest or dissent, unless carried on in conjunction with any of the above activities, is not included in the definition of threats to the security of Canada.[7]

CSIS' primary role is to advise government. CSIS collects and analyzes information and intelligence, and provides the Government of Canada with intelligence reports about activities that may threaten the security of Canada. The information comes from many sources, including:

- members of the public;
- foreign governments and their agencies;
- human sources;
- technical interception of telecommunications (e.g., wire-taps) and electronic surveillance of targeted persons or places (e.g., placing "bugs");[8]
- other government national security actors; and

- open sources, including newspapers, periodicals, academic journals, foreign and domestic broadcast, official documents and other published materials.[9]

CSIS must obtain a judicial warrant to intercept communications, obtain documents or information or enter premises covertly. To obtain a warrant, CSIS must have permission from the Minister of Public Safety to apply to a Federal Court judge. It must then demonstrate on evidence that there are reasonable grounds to believe that the warrant is necessary to investigate a threat to the security of Canada, or the capabilities, intentions or activities of foreign states or foreign nationals.[10]

CSIS analyzes and assesses information, and converts that information to security intelligence for the Canadian government and CSIS' partners in the security and intelligence community. CSIS provides both operational and strategic analyses. Operational analysis combines intelligence gathered by CSIS with information from other sources to provide a finished evaluation on specific threats. These might be case-specific or country-specific threats. Strategic analysis "aims to develop comprehensive, policy-relevant intelligence assessments." For example, CSIS provides the Government of Canada with reports on emerging trends and issues that could affect Canada's security, and with context on specific threats and their security implications. Strategic analysis aims to develop comprehensive, policy-relevant intelligence assessments either as stand-alone products produced by the Research Analysis and Production Branch, or in conjunction with other agencies within Canada's intelligence community under the auspices of the Privy Council Office.

2.3 PRIORITY AREAS

CSIS has six priority areas with respect to investigating and reporting on threats to Canada's security. I discuss these below, and in each area, I identify CSIS' primary role in relation to other members of the Canadian national security landscape. The six priority areas are

- terrorism;
- proliferation of weapons of mass destruction;
- espionage and foreign-influenced activities;
- transnational criminal activity;
- information security threats; and
- security screening and assessments.

2.3.1 Terrorism

In the area of terrorism, CSIS investigates the threat or use of violence against persons or property for the purpose of achieving political, religious or ideological objectives. CSIS dedicates most of its counter-terrorism resources to religious extremism, which the Government of Canada considers the most serious threat to the safety of Canadians at the present time. CSIS also continues to monitor individuals and organizations that may be involved in other forms of terrorism, such as state-sponsored terrorism and domestic terrorism. According to CSIS, domestic terrorism "includes the threat or the use of violence by groups advocating for issues such as the environment, anti-abortion, animal rights, anti-globalization, and white supremacy, and the dissemination of militia messages by groups in the United States, and secessionist violence."[11]

CSIS has six major areas of activity directed to the counter-terrorism mandate.

1. *Threat assessments*. CSIS prepares and disseminates evaluations about the scope and immediacy of terrorist threats posed by individuals and groups in Canada and abroad. Examples include assessing threats to the G8 meeting in Kananaskis, Alberta, in June 2002; and assessing the threat posed by Sunni Muslim extremism. CSIS traditionally chairs the interdepartmental Threat Assessment Working Group, which usually meets quarterly. Participants and invitees include the RCMP, DFAIT, the Integrated Threat Assessment Centre, PCO, Transport Canada, the CBSA, PSEPC and DND.
2. *Community interviews*. CSIS conducts interviews within communities to assess the likelihood of violence taking place in response to international political developments.
3. *Security screening*, which I discuss below.
4. *Assistance to enforcement*. CSIS' role in security certificates, discussed below, is an example.
5. *Liaison and co-operation*, pursuant to which CSIS provides information and briefings to law enforcement, security intelligence and other agencies.
6. *Advice to government*. As will be discussed in this chapter, in its counter-terrorism mandate, CSIS provides intelligence to, and receives information and intelligence from, numerous federal departments and agencies as well as the RCMP.

2.3.2
Proliferation of Weapons of Mass Destruction

CSIS investigates issues relating to weapons of mass destruction, including chemical, biological, nuclear and radiological weapons development programs undertaken by foreign governments and terrorists organizations. It develops assessments of potential threats within Canada or against Canadian interests. These assessments may be distributed throughout the broader domestic and foreign intelligence community, and to other departments and agencies of the Government of Canada.

To both gain and disseminate information about threats, CSIS works closely with several federal government departments and agencies, including DFAIT, DND, the CBSA, the National Research Council and the Canadian Nuclear Safety Commission.

2.3.3
Espionage and Foreign-Influenced Activities

CSIS' counter-intelligence activities are aimed at investigating espionage and foreign-influenced activities, and reporting on them to the Canadian government and, where relevant, to law enforcement agencies. CSIS also has a specific mandate to assist the Minister of Foreign Affairs and the Minister of National Defence in collecting information or intelligence relating to the activities of any foreign state or group of states,[12] any person who is not a Canadian citizen or permanent resident, or any organization other than a corporation incorporated under Canadian law.[13] During the Cold War years, CSIS focused its intelligence collection on traditional state threats related to political and military matters. Now, the threat tends to be the illicit acquisition of economic and technological information. Economic espionage — defined as illegal, clandestine or coercive activity by foreign governments to gain unauthorized access to economic intelligence, including proprietary information or technology — is one aspect of this part of CSIS' mandate. CSIS also investigates threats from foreign-influenced activities, including transnational criminal activity; cyber-related attacks; and activities directed against Canada's expatriate communities or covert attempts by foreign governments to influence the Canadian government or Canadian opinion in favour of a foreign government's interests. CSIS provides information to the RCMP pursuant to the espionage mandate, in addition to DND and DFAIT.

2.3.4
Transnational Criminal Activity

The globalization and sheer scale of criminal activity is a growing problem in Canada and around the world. CSIS estimates that five to seventeen billion dollars is laundered in Canada each year. CSIS collects and analyzes strategic intelligence, which it provides to Canadian government departments and agencies to identify the nature and extent of transnational crime in Canada and the threat to national security. It investigates threats to the integrity of Canadian financial institutions in key sectors of the Canadian economy; examines public institutions and programs to detect corruption and fraud; and investigates attempts by major transnational criminal groups to establish operational bases in Canada.

In the context of its work against transnational criminal activity, CSIS may exchange information with the RCMP and with foreign intelligence and law enforcement agencies. It gives strategic intelligence to Canadian police agencies to provide an overview of the threat environment, an assessment of the extent of the threat, and an identification of risk areas. CSIS may also provide police agencies with timely tactical information that will allow them to arrest and prosecute. It may provide information to the CBSA and CIC for lookout purposes, and may receive disclosure from and provide information to FINTRAC. However, it is important to note that CSIS does not share all its information with other agencies. For example, it would not share caveated information from foreign partner agencies or information about the identity of sources.

2.3.5
Information Security Threats

CSIS investigates threats posed by foreign countries, terrorists and hackers against critical information systems and infrastructure. It defines Canada's critical infrastructure as consisting of:

> physical and information technology facilities, networks and assets (e.g., energy distribution networks, communications grids, house services, essential utilities, transportation and government services), which, if disrupted or destroyed, could have a serious impact on the health, safety, security and economic well-being of Canadians.[14]

Cyber-related attacks are defined broadly as using information systems or computer technology as either a weapon or a target. CSIS states that politically motivated cyber-related attacks may be undertaken by groups associated with domestic tensions (e.g., "radical opposition movements to economic

events such as the G8, economic summits or environmental practices"),[15] or geo-political tensions like those related to the presence of Western forces in Iraq and Afghanistan.

Three conditions must be present for CSIS to initiate an "information operations" investigation. The incident must (1) be a computer-based attack; (2) appear to be orchestrated by a foreign government, terrorist group or politically motivated extremist; and (3) be done for the purpose of espionage, sabotage, foreign influence or politically motivated violence (terrorism). In its information security threat mandate, CSIS works closely with the RCMP, DND, the CSE and PSEPC. CSIS also exchanges information with foreign security intelligence agencies to remain apprised of the global threat environment, and participates with the Government of Canada in G8 efforts to address cyberthreats.

2.3.6
Security Screening and Assessments

Security screening is one of CSIS' main operational responsibilities, and one in which it receives information from and provides information to a number of other Canadian government departments and agencies. CSIS conducts five main screening programs, as follows.

2.3.6.1
Government Screening

The Government Screening Program provides security assessments for all government departments and institutions[16] except the RCMP, which runs its own screening service. Federal employees, members of the armed forces, or persons under contract to a government department who have access to classified government assets or information in the performance of their duties must hold security clearances. For Foreign Affairs and International Trade Canada, CSIS provides security assessments on locally engaged staff (foreign nationals) who handle unclassified material at Canadian missions abroad. The Government Security Policy defines three levels of security clearance: Confidential (Level I), Secret (Level II) and Top Secret (Level III).

Most levels I and II security clearance requests are done electronically from checks in CSIS databanks. If questionable information is revealed, a full field investigation may be required. All top secret security clearances require a full field investigation, which includes CSIS record checks; interviews of friends, neighbours and employers; local police checks; and sometimes applicant interviews. While CSIS assists the originating department by providing the assessment of an individual's reliability and loyalty to Canada, under the Government Security

Policy, all departments have exclusive authority to grant or deny security clearances. The Security Intelligence Review Committee (SIRC) reviews security clearance denials.

With the permission of the Minister of Public Safety, CSIS may enter into arrangements to provide security assessments to any provincial government or government department.[17] With the consent of the minister responsible for policing in the province, CSIS may enter into arrangements to provide security assessments to any provincial police force.[18]

2.3.6.2
Sensitive-Site Screening

CSIS conducts security screening for individuals with access to secure areas in airports, the Parliamentary Precinct (for those with access to the Houses of Parliament), and nuclear power stations (it gives this information to the Canadian Nuclear Agency). CSIS also provides security assessments to the CBSA on truck drivers who apply for a border pass under the Canada-U.S. Free and Secure Trade program.

Transport Canada requires security assessments on personnel who need access to restricted areas in Canada's international airports. Transport Canada collects information from the employee and transmits it to both CSIS and the RCMP, which conduct security screening and criminal records checks, respectively. When it receives these assessments, Transport Canada makes the final decision to grant or refuse clearance. Transport Canada is developing a clearance system for rail workers and workers at major ports, as well as a background check program for truckers who transport dangerous goods across the Canada-U.S. border, and CSIS will likely provide security assessments for these programs as well.

CSIS also conducts checks of visitors, employees or members of the news media who require access to "designated security perimeters during events conducted under a federal government sponsorship."[19]

2.3.6.3
Foreign Screening

CSIS provides security assessments to the governments of foreign states, to foreign agencies and to international organizations such as the North Atlantic Treaty Organization (NATO) on Canadian residents who wish to reside in another country or are being considered for classified access in another country. These are done only with the consent of the Canadian citizen, and are all approved by the Minister of Public Safety after consultation with DFAIT.[20]

2.3.6.4
Immigration and Citizenship Screening

The primary task of CSIS' Immigration Screening program is to provide security-related advice to CIC and the CBSA to prevent persons who are inadmissible under the *Immigration and Refugee Protection Act (IRPA)*[21] from entering or gaining status in Canada. CSIS does security screening on approximately ten percent of applicants wishing to immigrate to Canada or to acquire refugee status in Canada.[22]

CSIS provides security screening on Canadian visitor visa applicants and prospective immigrants where the applicant's background presents security concerns. CSIS maintains liaison offices in several Canadian missions abroad, which assist in providing the security screening in the foreign locations. It also provides CIC or the CBSA with security assessments on applicants for permanent residence and Canadian citizenship.

CSIS also assists CIC and the CBSA in enforcement efforts, primarily in admissibility, deportation and security certificate proceedings. These are discussed in the "Assistance to Enforcement" section below. I discuss the national security aspects of the immigration and naturalization process in greater detail in the CBSA and CIC sections.

2.3.6.5
Refugee Screening

CSIS also provides support to CIC and the CBSA in the front-end screening process for refugee claimants. The refugee screening process is discussed in more detail in the CIC section of this chapter.

2.4
ASSISTANCE TO ENFORCEMENT

CSIS plays an important role in the issuance of security certificates to have persons removed from Canada who have been found inadmissible on national security grounds. *IRPA* provisions allow a certificate to be prepared and signed by the Minister of Public Safety and the Minister of Citizenship and Immigration when a permanent resident or foreign national is found to be inadmissible on grounds of security, espionage, violating human or international rights, serious criminality or organized criminality.[23] The CBSA is responsible for these relevant sections of the *IRPA*.

A security intelligence report prepared either by CSIS or, rarely, by the RCMP is the basis for a security certificate request. The request is presented to

both the Minister of Public Safety and the Minister of Citizenship and Immigration. The CBSA analyzes the security intelligence report, focusing on evaluating an individual's admissibility under the *IRPA*.[24] The CBSA may analyze a broader range of factors than might concern either CSIS or the RCMP. The CBSA then prepares a recommendation for the Minister of Citizenship and Immigration about the certificate. CSIS, or on rare occasions, the RCMP, will prepare a recommendation for the Minister of Public Safety. PSEPC also provides the Minister of Public Safety with independent advice on the security certificate process.

CSIS states that several conditions must be met before it considers preparing a security intelligence report:

- The individual must be assessed as posing a significant threat to the security of Canada.
- CSIS must have sufficient threat-related information and intelligence.
- That information must be reliable and from multiple sources.
- The removal must be of strategic value in light of CSIS' investigative priorities.
- CSIS must have sufficiently releasable open-source information to support the unclassified summary document.[25]

Foreign nationals are automatically detained after the two ministers sign the certificate.[26] In the case of permanent residents subject to security certificates, the Minister of Public Safety and the Minister of Citizenship and Immigration may issue a warrant for the arrest and detention of the person if they believe the person presents a danger to the security of Canada or the safety of any persons.[27]

Once signed by the two ministers, the certificate is referred to a Federal Court judge, who determines whether the certificate is reasonable. The Government can seek the removal of an individual from Canada based on classified information. The Federal Court judge may hear and rely upon all or part of the information or evidence received in the absence of the subject and the subject's counsel if the judge determines it would be injurious to the national security or safety of any person to hear the evidence in public.[28] After reviewing the classified information, the judge determines how much information will be included in an unclassified summary to be given to the subject of the certificate and the subject's counsel. The *IRPA* requires that the summary include sufficient information for the individual to be reasonably informed of the circumstances giving rise to the certificate, but does not include anything that in the judge's opinion would be injurious to national security or the person's safety.

CSIS states that information likely to be withheld from the subject could include, but is not limited to:

> Details concerning human or technical sources, intelligence-gathering techniques and methods of information communicated in confidence from a foreign agency.[29]

If the Court finds the certificate to be reasonable, the certificate constitutes a removal order, and the individual may be deported immediately, subject to a pre-removal risk assessment discussed in the CIC section of this chapter. There is no appeal from the determination of reasonableness.[30] From 1991 to March 2006, 27 security certificates were issued in relation to 26 individuals.[31] Certificates have been directed at a broad range of subjects, including people found to be inadmissible on the basis that the ministers reasonably believed they are, were or may become involved with Islamic, Sikh or Tamil terrorism, Russian espionage, secular Arab terrorism and right-wing extremism.[32]

CSIS may also provide the CBSA and CIC with information to be used to flag "lookouts," to alert immigration and CBSA officers abroad and at ports of entry to Canada about the threats to national security posed by suspected and known terrorists seeking admission to Canada. The CSIS information will then form part of a determination by CIC and CBSA officers to refuse applications from individuals suspected of involvement in terrorist activities. I discuss lookouts in more detail in relation to the CBSA, below.

2.5 INFORMATION DISCLOSURE PRACTICES

To fulfill its mandate, CSIS may co-operate with any federal or provincial department, or, with the permission of the minister responsible for policing in a province, any police force in a province.[33] Similarly, with the permission of the Minister of Public Safety, CSIS may co-operate with international organizations, foreign governments or their constituent institutions.[34] Any written agreement between CSIS and a provincial or foreign entity, as described above, must be forwarded to the Security Intelligence Review Committee.[35]

CSIS may disclose information it obtains in the performance of its duties under the *CSIS Act* or as required by law.[36] CSIS may also disclose information to police officers if the information could be used to investigate or prosecute any alleged contravention of federal or provincial law.[37] Information that is relevant to Canada's international affairs or national defence may be disclosed to the Minister of Foreign Affairs, the Minister of National Defence or their designates, respectively;[38] or to any federal minister or other person if the Minister of Public Safety believes disclosure is essential in the public interest and that interest

clearly outweighs any invasion of privacy that could result from disclosure.[39] Where public interest disclosure is made, the Director of CSIS must submit a report to SIRC as soon as practicable.[40]

2.6
INTERACTION BETWEEN CSIS AND THE RCMP

I have discussed the interaction between CSIS and the RCMP in chapters II and IV. The primary form of interaction between the two agencies is the exchange of information. A significant portion of the national security-related information and intelligence that the RCMP receives comes from CSIS; thus, a significant amount of the RCMP's national security work is initiated by information received from CSIS. The CSIS/RCMP MOU[41] requires CSIS to provide the RCMP with information and intelligence that may assist the RCMP in fulfilling its national security-related responsibilities. However, CSIS is not obliged to share information that would disclose a source's identity nor to pass on information that a third party has caveated. When the RCMP conducts an investigation based on CSIS information, it provides CSIS with updates on the status of the investigation. The RCMP also provides CSIS with national security information and intelligence that it has collected. The two organizations share information both orally and in writing, although the RCMP informs me that a smaller portion of information is shared verbally and only after written communication has taken place.

CSIS is intended to be the prime Canadian contact with foreign intelligence agencies (as opposed to foreign policing agencies), and so CSIS sometimes acts as a conduit between the RCMP and these agencies. At other times, a foreign intelligence agency may contact the RCMP directly, and in such cases, the RCMP keeps CSIS informed. Direct exchanges of information take place primarily with agencies with which the RCMP has a long-standing relationship, such as the FBI.

Beyond information exchange, the RCMP and CSIS also provide each other with operational support and assistance. For example, when federal security is required at special events, CSIS provides threat assessments and other intelligence products to the RCMP. The Privy Council Office is also involved in these arrangements. The RCMP assists CSIS by conducting security assessments in geographical locations not serviced by CSIS, and by providing operational assistance with respect to CSIS's Protective Security mandate.

To foster co-operation between the two agencies, the RCMP and CSIS have in place a secondment, or exchange, program with the stated purpose of furthering each organization's understanding of the other's mandates. All four INSETs[42] have CSIS employees seconded to the teams. In addition, the RCMP has a CSIS manager in charge of its Threat Assessment Section at Headquarters at the

officer level, while an RCMP inspector is seconded to CSIS Headquarters at the management level. In the case of INSETs, it is the understanding of both organizations that CSIS members are present to provide their expertise, and there is no reporting back to CSIS. Similarly, I am informed that RCMP members seconded to CSIS do not report back to the RCMP.

In addition, different branches of the RCMP's Criminal Intelligence Directorate (CID) work very closely with CSIS Headquarters personnel on issues such as threat assessments. The RCMP's Anti-Terrorist Financing Group works closely with its counterpart at CSIS, and both agencies represent Canada on an international working group, the purpose of which is to exchange information and best practices related to terrorist financing and to improve international investigations in this field. CSIS also consults with the RCMP concerning listing terrorist groups under the new *Criminal Code* provisions.[43]

CSIS and the RCMP have formed a joint management team that meets regularly to discuss operational and intelligence issues of interest to both agencies.

2.7 OPERATIONS ABROAD

Unlike many countries such as the United States, the United Kingdom and Australia, Canada does not have a human source-based foreign intelligence service. However, CSIS is empowered to conduct operations abroad related to threats to the security of Canada. CSIS may conduct foreign covert operational activities, and often co-operates with intelligence services from another country, for example in establishing joint operations to obtain information of mutual security concerns.

CSIS states that it now has more people deployed abroad on a full-time basis than ever before, as well as more people operating from offices in Canada but assigned overseas on a part-time basis for a particular case or investigation.[44]

Other federal government departments that collect foreign intelligence abroad may share information with CSIS, including DFAIT, DND and the CSE. However, these agencies do not work for CSIS, and only some of the information they collect is shared with CSIS. CSIS also has employees posted abroad as security liaison officers. Finally, CSIS has more than 250 information-sharing arrangements with foreign security and intelligence organizations.

3.
INTEGRATED THREAT ASSESSMENT CENTRE

3.1
RELEVANT LEGISLATION

- *Anti-terrorism Act*, S.C. 2001, c. 41
- *Canadian Security Intelligence Service Act,* R.S.C. 1985, c. C-23 (*CSIS Act*)

3.2
MANDATE

The Integrated Threat Assessment Centre (ITAC) was created in 2004 following the release of the National Security Policy,[45] and replaced the CSIS Integrated National Security Assessment Centre.[46] The National Security Advisor at the Privy Council Office and the Director of CSIS have joint responsibility for ITAC's direction. The National Security Advisor provides overall policy direction, while the Director of CSIS is responsible for ITAC's day-to-day functions.[47]

ITAC produces comprehensive, integrated assessments of threats to Canada's national security and distributes them as required. The Centre focuses on terrorist trends, and on domestic and international events related to terrorism.

ITAC prepares and disseminates both classified and unclassified threat assessments. It produces classified weekly reports called Intelligence Digests that it sends to different departments within the Canadian security and intelligence community. ITAC also evaluates specific threat information.[48] Its weekly Threat Assessment Priority List keeps other government agencies up to date on its work. Within the Canadian federal government, ITAC shares its assessments directly with the RCMP, DND, DFAIT, PSEPC, Transport Canada, the CBSA, PCO, CSIS, the CSE, Health Canada and the Department of Justice. Transport Canada will provide threat assessments to CATSA as required. PSEPC also disseminates classified and unclassified ITAC assessments to various federal and provincial agencies and officials. Federal agencies include the Canadian Food Inspection Agency, the Canadian Nuclear Safety Commission, Environment Canada and the Department of Finance. ITAC provides unclassified assessments to private sector entities.

ITAC exchanges threat assessments with other international threat assessment centres, principally the Joint Terrorism Analysis Centre in Britain, the National Counterterrorism Center in the United States, the National Threat Assessment Centre in Australia and the Combined Threat Assessment Group in

New Zealand.[49] Relevant threat assessments are shared with international partners, unless the data is marked "for Canadian eyes only." On a case-by-case basis, ITAC may share information with other foreign partners. For example, it shared an assessment on illegal immigration and terrorism with NATO members, and an unclassified version of an assessment on the potential for terrorists to use the avian flu virus as a biological weapon with the Libyan, Saudi Arabian and Egyptian intelligence services. Currently, over half of the reports that ITAC disseminates within Canada are from foreign partner agencies. At the time of writing, the Centre has distributed a total of 532 assessments, of which it produced 126. ITAC adds a Canadian perspective to foreign reports before disseminating them, as it considers appropriate.

Government departments and agencies may task ITAC directly by directing requests on specific topics to ITAC's interdepartmental Production Advisory Committee.

As well as assessing threats within Canada, ITAC helps to shape travel advisories and conducts risk assessments for Canadian missions, interests and persons abroad. It may also undertake assessments that do not deal directly with terrorism, as determined by the Director of ITAC in consultation with ITAC's Management Board.

ITAC is specifically designed to facilitate information sharing among different government departments. The Centre operates within CSIS for administrative purposes, but many of its personnel are seconded to CSIS from other agencies. In 2006, ITAC had members from the RCMP, the CBSA, PSEPC, the Correctional Service of Canada, the CSE, DND, DFAIT, PCO, Transport Canada and the Ontario Provincial Police. A member from the Sûreté du Québec will soon be added. ITAC expects to reach its full complement of 46 employees in 2006. Other agencies, which do not provide secondees to ITAC but do provide information and obtain threat assessments, include Health Canada and the Public Health Agency of Canada, the Canadian Food Inspection Agency, Elections Canada and Environment Canada.

The role of ITAC secondees is to bring information from their home agencies into ITAC. ITAC personnel from different government departments have access to the same information and databases they would in their home organization. However, secondees do not share all information in their home databases with ITAC — only relevant information is shared, with the permission of the originating agency. In addition, the originating agency may place caveats on disclosure beyond ITAC. The RCMP secondee to ITAC has access to a Secure Criminal Information System terminal at ITAC. Agencies involved with national security matters also provide information to ITAC voluntarily or in response to

a request. However, ITAC cannot require a partner agency to conduct a specific investigation. No formal policies are in place governing the voluntary provision of information, but ITAC's senior management and the partner agencies have discussed the types of information that ITAC would like to receive. ITAC expects partner agencies to provide terrorist threat-related information on a timely basis.

ITAC does not collect or share raw intelligence data, although it does receive and disseminate personal information about identifiable individuals. To the extent possible, ITAC assesses the accuracy of information from both domestic and foreign sources before including it in intelligence assessments. While information from partner agencies will be used in ITAC reports, the reports themselves are CSIS property and subject to CSIS rules for disclosure and dissemination.

4. COMMUNICATIONS SECURITY ESTABLISHMENT

4.1 RELEVANT LEGISLATION

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

4.2 MANDATE

The Communications Security Establishment (CSE) is Canada's national cryptologic agency. The CSE uses technologically advanced methods and equipment to obtain information from foreign intelligence targets in support of federal government intelligence priorities. Unlike CSIS, the CSE does not collect intelligence from human sources. Instead, it collects signals intelligence — technical and intelligence information obtained from electronic emissions, including communications. The CSE shares this intelligence with other federal departments and agencies according to its mandate and federal government intelligence priorities, which include Canadian defence and foreign policy matters.[50] The CSE also works to protect electronic information and information infrastructures that are important to the federal government.

The CSE had its genesis in 1941 as part of the allied World War II effort. It was then known as the Examination Unit and was located in the National Research Council. In 1975, the CSE was transferred by order in council to the Department of National Defence.[51] The Government of Canada did not publicly acknowledge the CSE's functions until 1983,[52] and gave it a statutory basis

in 2001. The Chief of the CSE, under the direction of the Minister of National Defence, has the management and control of the agency.[53] The Chief reports to the Deputy Minister of National Defence for financial and administrative matters, and to the National Security Advisor at the Privy Council Office for policy and operations matters. The Minister may issue written directions to the Chief of the CSE concerning the carrying out of the Chief's duties and functions.[54]

The CSE has a three-part mandate that is set out in the *National Defence Act* as follows:

(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 (the "(a) mandate");
(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 (the "(b) mandate"); and
(c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties (the "(c) mandate").[55]

By law, the CSE's foreign intelligence activities pursuant to the (a) mandate may not be directed at Canadians or any person in Canada.[56] In relation to the interception of communications by government authorities, the term "private communications" is used to refer to communications that begin or end in Canada and that the person who began the communication would reasonably expect to remain private.[57] The Minister of National Defence may authorize the CSE to intercept private communications in Canada for the sole purpose of obtaining foreign intelligence, provided that the interception is directed at a foreign entity located outside Canada.[58] Before these ministerial authorizations were introduced in 2001,[59] the CSE was prohibited from intercepting communications that an intelligence target abroad sent to or received from Canada. Generally, ministerial authorizations last for one year. Four (a)-mandate ministerial authorizations were in place as of March 2006. Pursuant to its (a) mandate, the CSE may use or retain the private communications collected under ministerial authorization only if they are essential to international affairs, defence or security. All other private communications are destroyed.[60]

Under its (a) mandate, the CSE shares with both CSIS and the RCMP national security-related foreign intelligence with a domestic connection. For example, if the CSE incidentally acquired a communication from a terrorist located abroad communicating with someone in Canada and that communication had intelligence value, the CSE would share the information with CSIS.[61]

The RCMP and the CSE communicate to ensure that the CSE is aware of the types of information in which the RCMP may be interested. A select number of RCMP members receive, electronically or through a CSE Customer Relations officer, certain CSE intelligence reports that meet the RCMP's intelligence needs. The CSE may ask for information from its own foreign intelligence partners in response to an RCMP request. It may also task its partners to gather intelligence related to such requests. If the intelligence generated from these sources relates to the RCMP's mandate, the CSE may share it with the RCMP. Such sharing takes place at Headquarters level. A ministerial directive governs the CSE's information sharing with law enforcement agencies. I am told that the CSE provides the RCMP with foreign intelligence relatively infrequently. In most cases, the intelligence provided is general in nature and gives an overview of a specific situation in another country.

The CSE produces foreign intelligence reports on an ongoing but irregular basis. These reports are based on the federal government's intelligence requirements and are shared, electronically or through a CSE Customer Relations officer, with hundreds of different client groups within various federal departments and agencies, according to the stated intelligence needs of these bodies.[62] It is important to note that although the CSE provides foreign intelligence to many different government clients, each client receives only intelligence that is necessary to its functions and mandate. If the CSE receives a request for information from a domestic agency that is not in line with Government of Canada foreign intelligence priorities, the CSE states that it would not be able to provide that information. The Department of Foreign Affairs and International Trade is the CSE's largest intelligence client, partly because DFAIT manages Canada's foreign relations on behalf of all Canadian departments and agencies.

Under the (b) mandate, the CSE helps to protect electronic information and information infrastructures of importance to the Government of Canada. The information infrastructure does not have to be federally owned — it can be a provincial or private interest such as a hydroelectric system.

With respect to information technology security, the CSE provides guidance and strategic advice to the Government to ensure its critical information systems are secure. For example, the CSE may advise on cybersecurity, cryptographic equipment and secure communications. Under this mandate, the CSE may work with partners such as the Canadian Forces Information Operations Group (CFIOG). The information technology security mandate generally does not involve the interception of communications. However, there is provision for obtaining ministerial authorization where the (b) mandate activity requires the interception of private communications. Solely to protect the Government of

Canada's computer systems or networks, the Minister may authorize the CSE to intercept private communications subject to certain statutory conditions. These include conditions that the Minister considers advisable to protect Canadians' privacy, such as restricting the use, retention and disclosure of information derived from the interception.[63]

Ministerial authorizations given to the CSE under its (a) and (b) mandates may also include a direction to the Canadian Forces to support the CSE in its activities.[64] Where the Canadian Forces collects signals intelligence in support of the CSE, the Forces' collection activities are subject to the CSE's mandate and review mechanisms.[65] I discuss the interaction between the CSE and the Canadian Forces in more detail in the section on DND.

Under its (c) mandate, the CSE may provide technical and operational assistance to federal law enforcement and security agencies. This assistance is primarily technical. The CSE's (c) mandate is tied to the legislative authority of the requesting agency. Under its (c) mandate, the CSE provides the RCMP with technical assistance such as obtaining information from an encrypted hard drive. The (c) mandate also allows the CSE to give the RCMP technical and operational assistance, including for the RCMP's own intelligence collection programs, at the RCMP's request, and to assist in criminal investigations. The task must be within RCMP authority, and the CSE must have proof of this authority in some form.

Since 2002, the CSE has significantly increased its security intelligence focus and collection capabilities. It has added many new staff and expanded its office space to three additional buildings.[66] The CSE's Office of Counterterrorism now operates seven days a week, and security and counter-terrorism requirements are top collection priorities. Approximately 80 percent of the CSE's efforts are currently directed towards supporting military operations or related to national security.[67] The agency's technical collection capabilities have been enhanced, allowing for closer technical integration with allied signals intelligence agencies.[68] The CSE says that it has gathered intelligence on foreign terrorist targets that has been used to protect Canadians and Canada's allies.[69]

The CSE works very closely with the Canadian Forces Information Operations Group in the collection of foreign intelligence.[70] It also has personnel integrated into key Canadian agencies[71] — currently CSIS, ITAC and the Canadian Forces Information Operations Group — and deploys Client Relations officers to the RCMP, CSIS, DFAIT, DND, PCO and other major federal government departments. The function of these officers is to provide intelligence reports to and receive intelligence requirements from federal government clients.

In its foreign intelligence reports, the CSE does not include the names of Canadian citizens or permanent residents, or information that may identify citizens of Canada, the U.S., U.K., Australia or New Zealand. A domestic agency asking for access to such information must justify access under criteria set by the CSE.[72] Justification must pertain to one or more specific categories of federal government intelligence priorities, and include an explanation of how such information would be useful to the department's or agency's activities.

The CSE has a close and long-standing foreign-intelligence-sharing relationship with the signals intelligence agencies in the United Kingdom, the United States, Australia and New Zealand,[73] and has integrated personnel into these allied agencies.[74] Normally the CSE does not share information with these agencies that relates to the interception of private communications, although it may provide relevant intercepted information relating to national or alliance security. However, the CSE does not disclose identifying information it may have collected on a Canadian citizen except in response to a formal request, after consultations with relevant Canadian security and intelligence partners, and provided that the request meets CSE criteria. Improving information sharing is a current CSE priority.[75]

5.
DEPARTMENT OF NATIONAL DEFENCE

5.1
RELEVANT LEGISLATION

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

5.2
MANDATE

The federal government is the only authority in matters of defence and the protection of Canadian sovereignty. The Department of National Defence (DND) portfolio includes the department itself (including 20,000 civilian employees), the Canadian Forces (CF), and 3,600 Canadian Rangers who provide a military presence in remote and sparsely populated areas of the country.[76] The Canadian Forces consist of approximately 62,000 regular forces and 22,000 reservists.[77] The Minister of National Defence is responsible for the department and is accountable to Parliament for its activities. The Minister also provides direction to the CSE on the performance of its functions, and is accountable to Cabinet and to Parliament for all CSE activities.[78]

The Department of National Defence and the Canadian Forces collaborate with other federal and provincial departments in areas such as counter-terrorism, counter-proliferation, emergency management, illegal immigration and drug trafficking.[79] The Department of National Defence recently announced a major reorganization that will focus considerable resources on defending Canadian territory proper, as opposed to foreign military missions to defend Canada's interests and allies abroad.[80]

DND/CF maintain a large and sophisticated intelligence capability that is able to support the Canadian government in general and the Canadian Forces in particular worldwide. Defence Intelligence, which consists of both military and civilian employees, plays an important role in Government of Canada and departmental policy formulation; in decisions on the purchase of weaponry and most other equipment for DND/CF; in the research and assessment burden of large intelligence problems or questions with allies;[81] and most importantly, in intelligence collection, analysis and dissemination to directly support ongoing or anticipated operational deployments or engagements of CF personnel or assets. Functionally, Defence Intelligence and its clients span the entire realm of DND and the CF, as well as reaching out into the wider Canadian and allied intelligence community.

The Chief of Defence Intelligence (CDI) coordinates intelligence gathering and collection for DND/CF. DND/CF gather and analyze intelligence related to domestic threats, as well as information to support foreign operations. Defence Intelligence capabilities run the entire spectrum of intelligence-gathering practice and analysis. However, DND/CF Intelligence focuses largely on foreign-based threats, and foreign military capabilities and operations. One of the military's unique intelligence capabilities is gathering and producing imaging and mapping information for Canadian or international territory. Defence intelligence relies on CSIS and the RCMP for domestic human intelligence gathering.

The CSE, the Canadian Forces Information Operations Group (CGIOG)[82] and the Canadian Forces SIGINT Operations Centre (CFSOC) are the principal signals intelligence organizations in Canada. The CSE provides strategic and tactical signals intelligence support to both the CF and DND, and in this capacity is an important provider of raw or semi-processed signals intelligence. In addition to routine distribution of signals intelligence from the CSE, DND/CF maintain signals intelligence assets specific to the military, the most important of which are the CFIOG and CFSOC. The CFIOG has a mandate for signals intelligence activities delegated by the CSE, which include support to domestic and international military operations. Signals intelligence support to military operations gives commanders direct access to essential intelligence products and has

become a priority for CF-controlled signals intelligence assets, either through remote capabilities or assets located in operational theatres. The CFSOC is tasked with requests by different CF components and by the CSE. The CFSOC has developed virtual analytical teams that use expertise from civilian agencies like DFAIT and CSIS, as well as different military intelligence disciplines. These virtual analytical teams provide a continuum of support from the tactical to the strategic level and have the potential to provide complete intelligence products. DND/CF may intercept private communications that begin or end in Canada[83] only to assist civil authorities and under the direction of these authorities.[84] However, under CSE authority, and pursuant to a ministerial authorization, the CFIOG may gather foreign intelligence by intercepting private communications that begin or end in Canada.

5.3
DOMESTIC NATIONAL SECURITY ACTIVITIES

Domestically, military intelligence maintains close links and information-sharing relationships with all members of the Canadian national security community. The Canadian Forces are also becoming increasingly integrated with civilian government departments and the RCMP in intelligence sharing and mutual operational support in anti-terrorism efforts.[85] DND/CF have representation at PCO, DFAIT, CSIS, the CSE, Transport Canada, ITAC and the Marine Security Operations Centres, as well as numerous exchange positions worldwide. CSIS and the CSE are also represented at the Department of National Defence. Defence Intelligence does not task the RCMP or other government departments and agencies, although it may request additional information on an existing issue or analysis on a specific topic. The other government department can either accept or refuse the request.

As a general rule, military intelligence will provide information about general security threats to CSIS, and will provide criminal intelligence information and products to the RCMP.[86] DND/CF uses criminal intelligence for the following reasons:

- to reveal the existence of criminal organizations or other significant criminal activities;
- to identify the members of such organizations; and
- to establish their criminal activities, internal administration, movements, sources of income and vulnerabilities.[87]

In return, the military usually receives finished intelligence products from CSIS, but receives raw information from the RCMP. For example, DND/CF might

receive information from the RCMP about Defence personnel who have been linked to criminal activity or about criminal activity that seems to be directed towards a military base or other assets.

There are currently no formal guidelines covering information sharing with the RCMP or CSIS. However, a recent review of Defence Intelligence recommended developing policies on information sharing, collection and storage. Defence Intelligence now has information-sharing memoranda of understanding (MOUs) with CSIS, the CSE, the RCMP, DFAIT, Transport Canada, Health Canada and Natural Resources Canada. Additional MOUs are contemplated or being developed with PSEPC, the CBSA, CSIS and the RCMP; and additional general written policies concerning intelligence analysis and sharing are under development within CDI.

The Canadian Forces Joint Information and Intelligence Fusion Capability — which exists only in concept at the time of writing — is intended eventually to provide a joint, interdepartmental, all-source intelligence fusion capability to the Government of Canada. This intelligence fusion capability would include both military and civilian intelligence capabilities.

National security activities may also involve the military police. There are approximately 1,300 military police in Canada and overseas in places like Afghanistan. Most military police officers are assigned to active military units, where they provide policing functions but also serve as members of the Canadian Forces. Approximately 110 military police members are a part of the Canadian Forces National Investigation Service (CFNIS). This is a special unit that is under the operational chain of command (i.e., the chain that applies to the Army, Navy and Air Force). Members of the CFNIS investigate the more serious criminal or military offences and conduct "sensitive" investigations — those involving a DND senior officer or equivalent civilian employee, and those involving sensitive material or instances that could discredit DND. There are also approximately 40 military police in the National Counter-Intelligence Unit (NCIU) under the command of the Deputy Chief of Defence Staff, within J2/Director General Intelligence. Some military police members serving in the NCIU may participate in joint operations with the RCMP or other agencies through INSETs or IBETs[88] where there is a military nexus.

Generally speaking, the RCMP takes the lead on national security investigations, although the military police, likely through the CFNIS, could be involved depending on the facts. The military may obtain national security information — top secret or otherwise — through formal channels. It generally passes such intelligence acquired by other means to the RCMP.

While members of the NCIU who are also military police work as liaisons with IBETs and INSETs, there are no DND or CF secondments to either of these integrated teams.[89] Contact between INSETs, IBETs and the NCIU varies because the NCIU conducts liaison activities only where there is a clearly defined threat to the security of DND or the CF.[90] Canada's military police may also be involved peripherally with other RCMP national security investigations, and military intelligence may be used to assist other RCMP operations. In addition, the NCIU may enlist the help of police or security agencies to obtain search warrants or warrants for the interception of communications to assist in a military counter-intelligence investigation where the subject of the investigation or operation is a DND employee or a CF member.[91]

DND/CF also may provide armed assistance to the RCMP. The CF Armed Assistance Directions[92] establish the procedures for requesting and providing armed assistance by the Canadian Forces to the RCMP for the purpose of resolving disturbances affecting the national interest. Therefore, the Canadian Forces may provide armed assistance to the RCMP in national security matters after a series of administrative steps take place. These steps include a request from either the RCMP Commissioner or the Minister of Public Safety to the Minister of National Defence requesting aid to the civil authority. Any and all DND/CF assets can be brought to bear as the Minister of National Defence directs, including Joint Task Force Two (JTF 2), the military counter-terrorism unit.[93] JTF 2's counter-terrorism mandate is to provide an immediate response, as a force of last resort, to terrorist events or major disturbances affecting the national interest. To ensure the appropriate use of JTF 2, this formal request procedure is in place to guide officials when asking for assistance. The Joint Nuclear, Biological and Chemical Defence Company is also available to provide assistance in the case of a biological, nuclear or chemical emergency. The Government Operations Centre coordinates the deployment of this unit.[94]

6.
CANADA BORDER SERVICES AGENCY

6.1
RELEVANT LEGISLATION

- *Canada Border Services Agency Act*, S.C. 2005, c. 38 (*CBSA Act*)
- *Canadian Food Inspection Agency Act*, S.C. 1997, c. 6
- *Customs Act, R.S.C.* 1985, c. 1 (2nd Supp.)
- *Export and Import Permits Act*, R.S.C. 1985, c. E-19

- *Export Control List*, S.O.R./89-202, as amended
- *Immigration and Refugee Protection Act*, S.C. 2001, c. 27 (*IRPA*)
- *Immigration and Refugee Protection Regulations,* S.O.R./2002-227
- *Passenger Information (Customs) Regulations*, S.O.R./2003-219

6.2 MANDATE

The Canada Border Services Agency (CBSA) was created in December 2003 by order in council.[95] Essentially, the CBSA combines the enforcement, intelligence and interdiction functions of Citizenship and Immigration Canada,[96] the customs program of the former Canada Customs and Revenue Agency,[97] and the primary food and plant inspection functions of the Canadian Food Inspection Agency.[98] The CBSA received a statutory mandate in November 2005[99] and is responsible to the Minister of Public Safety.[100] It has a mandate to manage the movement of goods and people into Canada and the movement of goods out of Canada at all ports of entry. This mandate includes both facilitation and enforcement activities. To help fulfill its mandate, the CBSA may enter into agreements with foreign states and international organizations.[101]

The CBSA has approximately 12,000 employees located at about 1,200 service points in Canada and 39 locations abroad.[102] All border guards at points of entry into Canada work for the CBSA. However, official border posts ("points of entry") exist only in certain places along Canada's land borders and coastlines. In all places along the border where there is no official port of entry, but where people may still cross into or out of Canadian territory, the RCMP is responsible for enforcing Canadian laws with respect to the flow of goods and people into and out of the country.

The CBSA has seven principal branches: Admissibility; Enforcement; Human Resources; Innovation, Science and Technology; Comptrollership; Operations; and Strategy and Coordination. The CBSA Enforcement Branch houses the CBSA's intelligence capability, which includes a threat analysis and assessment directorate, a national security directorate and a borders intelligence directorate. The Branch also deals with immigration screening, fraudulent travel documents, investigations, detentions, removals, counter-terrorism, counter-proliferation, strategic exports and contraband.

The CBSA defines national security threats according to the federal national security policy.[103] In relation to the movement of people, the CBSA looks for individuals linked to terrorism, espionage, subversion, organized crime and war crimes. In relation to the movement of goods, the CBSA looks for information

on the movement of goods linked to terrorism. Its activities in this regard include intercepting and seizing illegal arms, working on counter-proliferation initiatives and ensuring export control to embargoed countries.

CIC and the CBSA share responsibility for administering Canadian immigration laws, which govern the movement of people into Canada, the removal of non-citizens from Canada, and laws related to obtaining or losing citizenship.[104] Both the CBSA and CIC are responsible for preventing people from entering or remaining in Canada if they are not legally entitled to do so. The *Immigration and Refugee Protection Act* sets out a number of reasons why individuals are not allowed to enter or remain in Canada, even if they would otherwise be entitled to come to Canada or to live here. These individuals are referred to as being "inadmissible" to Canada. People may be declared inadmissible

1. because they are reasonably believed to pose a national security threat on the basis that they: [105]
   (i) have engaged in espionage or subversion against a democratic government or institution;
   (ii) were involved in undermining a government or institution using force;
   (iii) have engaged in terrorism;
   (iv) are a danger to the security of Canada;
   (v) have engaged in acts of violence that could endanger the lives or safety of people in Canada; or
   (vi) are a member of an organization that it is reasonably believed engages, has engaged or will engage in espionage, subversion or terrorism as described above.
2. because they are reasonably believed to be involved in major human rights violations abroad, including war crimes;[106]
3. because they are reasonably believed to have a criminal record for an offence punishable by ten or more years imprisonment, either in Canada or abroad ("serious criminality");[107]
4. because they are reasonably believed to be linked to a criminal organization, human smuggling/trafficking or money laundering ("organized criminality");[108] or
5. for a variety of other reasons that do not relate to national security.[109]

In some cases, people who are inadmissible for reasons of security or organized criminality may be allowed to enter or remain in Canada if they satisfy the Minister of Citizenship and Immigration that their presence in Canada would not harm the national interest.[110] CIC has the lead role in relation to persons

who are inadmissible for serious criminality,[111] while the CBSA takes the lead for national security, organized criminality,[112] war crimes and gross human rights violations. CIC and the CBSA collaborate closely, and sometimes officers from one agency will be designated to perform functions that fall within the responsibility of the other agency.[113]

Generally, the CBSA focuses on the security of Canada's borders, including threats and risks to Canada.[114] The CBSA collects intelligence and detects people who are in Canada illegally. It also arrests, detains[115] and removes[116] inadmissible persons, and develops and implements admissibility policies relating to security, war crimes and organized crime.

The CBSA also enforces customs laws, which regulate the goods and currency that may enter and leave Canada.[117] The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* requires large cross-border financial transactions and the transport of currency or monetary instruments across the border to be reported to Canadian authorities.[118] CBSA officers have the power to search individuals, baggage, conveyances and mail for currency that is unreported,[119] and may seize currency or monetary instruments that are not reported or that are reasonably believed to be the proceeds of crime.[120] CBSA officers must record in writing the reasons for all such seizures.[121] This responsibility includes reporting certain cross-border financial transactions to Canada's financial intelligence agency, FINTRAC, and/or to the RCMP. CBSA Customs also has responsibility for enforcing restrictions on the export of strategic goods (e.g., goods that potentially could be used to make sophisticated weaponry).

The CBSA has a large mandate — over 94 million travellers are processed annually, and over two billion dollars worth of trade goods cross Canadian borders each day. As with the other government departments that I discuss, much of the CBSA's activity is beyond the scope of this chapter. The vast majority of the CBSA's work is focused on law enforcement. Thus in this section, I have chosen to focus my discussion on the police powers of CBSA officers; CBSA's intelligence capabilities; CBSA's national security activities relating to the screening of people and goods; CBSA participation in integrated teams; and CBSA information-sharing policies, practices and agreements.

6.3
POLICE POWERS OF CBSA OFFICERS

When performing their duties under customs and immigration legislation, CBSA officers generally have the same powers as police officers,[122] including powers of arrest,[123] detention,[124] search[125] and seizure.[126]

Under the *Customs Act*, CBSA officers at border crossings can also stop travellers for further questioning, and take breath and blood samples.[127] Under the *IRPA*, CBSA officers can question, search and detain non-citizens.[128] A CBSA immigration officer may issue an arrest warrant for a permanent resident or a foreign national, if the officer suspects that the person poses a threat to the public or is in Canada illegally.[129] Foreign nationals (other than refugees) also may be arrested and detained by CBSA officers without a warrant on the same grounds.[130] At the border, an immigration officer may detain a non-citizen where the officer suspects that the person poses a national security risk, among other reasons.[131]

CBSA officers may carry batons and pepper spray, and are trained in the use of force. At the time of writing, CBSA officers do not carry firearms. However, the federal government has recently announced plans to begin arming CBSA officers at border posts.[132]

CBSA officers may refer violations of the *Immigration and Refugee Protection Act* to the RCMP for investigation and prosecution, and all RCMP members are also appointed as immigration officers.[133] By law, all RCMP officers are designated as Customs[134] and Excise[135] officers, and the RCMP has primary responsibility for enforcing customs laws in remote areas and on reserves created under the *Indian Act*.[136] RCMP officers acting as immigration and customs officers are governed by the *RCMP Act* and RCMP operational or administrative policies, not by CIC or CBSA policies and directives.[137]

6.4
CBSA INTELLIGENCE

The intelligence capabilities of CBSA's Immigration and Customs branches have been blended into a single CBSA intelligence reporting structure. The Intelligence network is composed of the National Headquarters Intelligence Branch, eight Regional Intelligence units within Canada, and a group of Migration Integrity officers (MIOs) working abroad. The Intelligence network is involved in planning, collecting, analyzing and disseminating intelligence concerning threats to people and goods, including immigration, visitor and refugee programs, and intelligence relating to the smuggling and transport of strategic goods.[138]

The National Headquarters Intelligence Branch provides direction and support with respect to individuals who may be involved in terrorism, organized crime, war crimes, illegal immigration, smuggling of contraband or the illegal movement of strategic goods. The CBSA is one of four partners involved in war crimes apprehension, and the Headquarters Intelligence Branch holds most

classified intelligence information related to modern war crimes and suspected war criminals.[139] The branch is the focal point for intelligence-based decision making on individual cases, as well as policy and programming for the CBSA.[140] The Regional Intelligence units provide support to Canadian field offices.[141] CBSA Intelligence produces a large volume of strategic threat assessments relating to border security issues in both the customs and immigration fields. These assessments rarely contain personal information, and are disseminated to the RCMP and other agencies, both domestic and international, as the CBSA sees fit.

Approximately 45 Migration Integrity Officers work out of Canadian diplomatic posts abroad, together with international partners, to stop illegal immigration, including human smuggling and trafficking. One of the MIOs' major functions is to assist airlines in determining whether to allow individuals to board. MIOs also have an anti-fraud role in detecting and intercepting fraudulent travel documents,[142] provide some media reporting, report on interceptions of individuals suspected of travelling with false documents, and analyze information relating to country conditions.

MIOs feed information directly to CBSA regional offices in Canada. In addition, they provide the RCMP Criminal Intelligence Directorate with information about terrorist or national security threats and fraudulent documents,[143] and human trafficking operations or organized crime where a Canadian citizen or permanent resident is suspected of involvement. MIOs also may inform CBSA officials in Canada about suspicious persons en route to Canada. These reports include names and aliases, dates of birth, passport numbers, addresses, routing information and details about family members and known associates.

Internationally, Migration Integrity officers work with local immigration and law enforcement authorities, airline staff and overseas migration officers from the United Kingdom, the United States, Australia, the Netherlands, the Nordic countries and Germany. Canadian MIOs co-operate with these partners on fraud investigations and airport assistance, and share information on trends, emerging passport issues (e.g., fraud in a particular country) or criminal profiles. In some circumstances, MIOs may also share information of a personal nature about suspicious persons enroute to Canada with the local authorities of closely allied states.

The Customs side of the CBSA also maintains an intelligence capability, and has an active information-sharing relationship with the RCMP[144] and with American Customs counterparts, as discussed below.[145]

6.5
IMMIGRATION DETENTION FACILITIES

The CBSA has legal responsibility for immigration detention facilities, including those used to house security certificate detainees. The facilities are staffed by personnel from the Correctional Service of Canada.[146]

6.6
NATIONAL SECURITY ACTIVITIES

6.6.1
Screening of People Entering Canada

At the border, CBSA officers screen travellers entering Canada — both citizens and non-citizens — for compliance with immigration and customs laws. The CBSA conducts three major types of screening: (i) for suspected violations of customs or other laws; (ii) of non-citizens arriving in Canada, to identify those who may be inadmissible under the *Immigration and Refugee Protection Act*; and (iii) of temporary visa applicants, applicants for permanent residence and citizenship, and refugee claimants jointly with CIC. The CBSA does all immigration screening at border crossings, while CIC screens within Canada and abroad, with advice and assistance from the CBSA.

The CBSA maintains databases to help its officers enforce both customs and immigration laws. The initial stages of the screening process use electronic data-matching or risk-assessment algorithms.

6.6.2
Lookouts

CBSA Intelligence is responsible for placing and maintaining "lookouts," electronic file records that flag or identify particular travellers or vehicles according to risk indicators or intelligence.[147] Customs lookouts identify individuals of interest in relation to any type of ongoing criminal or national security investigation. For example, a lookout may be placed for a person who is known to smuggle strategic goods out of Canada in violation of the *Export and Import Permits Act*. Customs lookouts may be issued for both Canadian citizens and foreigners, and do not necessarily have to relate to suspected violations of customs laws. The CBSA and CIC use immigration lookouts (or "*IRPA* lookouts") to identify inadmissible persons. Grounds for inadmissibility include national security reasons, suspected involvement in war crimes, serious crime and organized crime, including money laundering and terrorist financing.[148] *IRPA* lookouts

also may be issued for Canadian citizens suspected of involvement in human trafficking or smuggling. Front-line CBSA officers may add lookout flags with a supervisor's permission. For such flags to remain in the Customs database, however, CBSA Intelligence subsequently must approve them. Flags in the Immigration databases need not be subsequently approved to remain in those databases.

A lookout includes basic biographical information about an individual and a brief description of the reason that the individual has been flagged. The substance of the lookout and the background information on which it is based are not provided to front-line officers, although this information may be obtained upon request. Lookouts do not determine whether a non-citizen may enter Canada. Where a flagged person is encountered at a border crossing or during the visa or immigration process, the CBSA officer decides whether to allow the person to enter Canada based on the background information substantiating the lookout and information from the individual in question.[149] A customs lookout also may lead a CBSA officer to question or search a citizen or a non-citizen to obtain information about the possible commission of an offence.

Other agencies generally provide the CBSA with the information on which an *IRPA* lookout flag is based — usually CSIS, the RCMP, DND, the CSE or American law enforcement partners. Key American partners include the U.S. Terrorist Screening Center, which maintains American terrorist watch lists, and the U.S. National Targeting Center, which processes customs and Immigration lookouts.[150] The CBSA also creates its own immigration lookouts based on information in its case management and intelligence databases. The RCMP and CSIS may also ask the CBSA to place either or both of customs and immigration lookouts.

Customs lookouts are generated from CBSA information, including Customs case files maintained by CBSA Intelligence, and a mix of information from other agencies that investigate criminal activity that crosses the border. These other agencies include the RCMP, local or provincial police forces, CSIS, the CSE, DND, Transport Canada, Environment Canada, the Coast Guard, the CRA, Health Canada, the Canadian Food Inspection Agency, Natural Resources Canada and the Canadian Nuclear Safety Commission; and U.S. partner agencies, including the U.S. Customs and Border Patrol, the U.S. National Targeting Center and the U.S. Terrorist Screening Center.

Immigration lookout flags may remain in force indefinitely.[151] Customs lookouts are reviewed every 90 days. Unlike *IRPA* lookouts, customs lookouts do not necessarily relate to admissibility to Canada and are therefore more likely to be deleted over time.

6.6.3
Advance Passenger Information/Passenger Name Record Information Program

Under the *Customs Act*, the Minister of Public Safety may require any person or class of persons arriving in Canada to provide personal information before arrival.[152] This information falls into two categories. Advance Passenger Information (API) is basic identifying data about a traveller, including name, birthdate, gender, passport or other travel document information, and citizenship or nationality. Passenger Name Record information (PNR) relates to a traveller's itinerary and reservation, and includes any information about a person contained in a transportation carrier's reservation or departure control records.[153] Such information could include, for example, details about e-mail addresses, credit card billing or special health requirements.[154]

The CBSA may share API/PNR data that it collects with other government agencies for national security or defence purposes, where there are reasonable grounds to believe that the information relates to a real or suspected threat to Canada's security or defence.[155] Information that could identify an individual is removed 72 hours after arrival, but CBSA keeps the depersonalized PNR data for various intelligence, research and analytical purposes. PNR data that has been in the CBSA's possession for longer than 72 hours may be reconnected to information that identifies a specific individual if disclosed for national security purposes.[156] CBSA policy provides that PNR data may be disclosed only for the following:

- reasons consistent with the purposes for which it was collected — that is, to prevent terrorism or terrorism-related crimes, and organized crime that is transnational in nature;
- where disclosure is necessary for the protection of the important interests of the data subject or other persons, particularly in relation to significant health risks;[157]
- to comply with subpoenas, court orders, or requirements for the production of information during the course of judicial proceedings; and/or
- in accordance with the *Customs Act,* the *IRPA*, the *Privacy Act* and other relevant, enabling information-sharing legislation.[158]

Under the *Customs Act,* the CBSA may provide PNR data to a police agency that takes custody of an individual arrested by CBSA officers for a customs offence.[159] The *Customs Act* also allows the CBSA to disclose PNR data to regulatory agencies whose acts CBSA Customs administers at the border.[160] For

example, PNR data related to the enforcement of Part II of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* may be disclosed to FINTRAC.[161] The CBSA may also disclose PNR data to Health Canada to identify travellers arriving in Canada who may have been exposed to highly contagious diseases.[162]

The CBSA may share PNR information with governments of foreign states under written agreements or arrangements.[163] The other country must agree to protect the information in a manner similar to that in which PNR data is protected in Canada.[164]

The CBSA's collection and analysis of API/PNR data is not connected to the Canadian no-fly list (Transport Canada) or the American no-fly list. Further, the transmission of API/PNR data to the CBSA under the *Customs Act* is not connected to the requirement that airlines provide PNR data upon request to Transport Canada or the planned provision of such information by Transport Canada to CSIS and the RCMP for flights in Canada.[165]

6.6.4 National Risk Assessment Centre

The CBSA's National Risk Assessment Centre (NRAC) was established in January 2004 as a function of the *Smart Border Declaration* between Canada and the United States.[166] The Centre is staffed by CBSA personnel and a small number of personnel from the Canada Revenue Agency.

NRAC has three main functions: (1) to receive API/PNR data and analyze it for risk; (2) to receive terrorist watch list information from the United States; and (3) to receive and analyze advance commercial information for risk. I discuss these below.

NRAC receives API/PNR information about inbound airline passengers from air carriers prior to landing.[167] NRAC cross-references API against its internal Immigration and Customs enforcement databases to match passengers against lookout flags or identify any previous issues with arriving individuals. PNR information is fed into a risk-analysis system that risk-scores passengers using algorithms developed from a large database of information. The algorithms are designed to identify constellations of factors that the CBSA states indicate increased risk. Passengers considered to be at high-risk for possible involvement with terrorism, as well as other serious crimes including smuggling and trafficking of drugs or people,[168] are subject to closer questioning upon arrival in Canada. Canada and the United States use the same risk-analysis system. A similar system, the Integrated Primary Inspection Line, is used to process

the movement of travellers into Canada at selected ferry, bus, cruise ship and rail locations.[169]

Pursuant to a 2005 memorandum of understanding,[170] NRAC automatically shares with the U.S. National Targeting Center API information for air passengers arriving in or transiting through Canada for whom terrorism or serious crime-related lookouts have been issued. It is anticipated that PNR information will shortly be shared for any traveller who receives a risk-score above a certain threshold. Under the 2005 MOU, Canada and the United States automatically share lookouts relating to potentially serious violations of customs or immigration laws.[171]

Under a 1997 agreement, the U.S. Terrorist Screening Center provides its terrorist watch list and any updates to CBSA's National Security Division.[172] The U.S. list contains biographical information that is used to create *IRPA* lookouts for terrorist suspects.[173] The CBSA does not receive information about Canadian or U.S. citizens under this program.[174] Temporary visa, immigration and refugee applicants, as well as travellers to Canada, are screened against this list using the lookout process. If CBSA or CIC officials encounter an individual whose name appears on the U.S. terrorist watch list, they notify the U.S. Terrorist Screening Center via the CBSA's National Security Division[175] and obtain more information on the substance of the lookout.[176] As with other lookouts, CBSA personnel (and/or CIC personnel) will decide whether the individual in question is admissible to Canada based in part on this additional information. CBSA or CIC officials will report their decision on the person's admissibility and the results of the examination of the individual to the U.S. Terrorist Screening Center and to designated U.S. Customs and Border Patrol officials.[177]

As its third function, NRAC also conducts similar electronic risk assessments based on advance commercial information, including marine and air cargo manifests. CBSA officers and their counterparts at U.S. Customs and Border Protection co-operate closely in the screening of cargo, particularly marine cargo. For example, NRAC will receive details of shipping cargo manifests from shippers 24 hours before a ship bound for Canada is loaded. NRAC runs these electronic reports through a risk-assessment computer program similar to that used for the API/PNR program.[178] The CBSA has begun implementing a program that requires air carriers to provide information about the shipper and details of the contents of all cargo prior to arrival in Canada,[179] and will eventually implement similar systems for commercial goods shipped by rail and by road. Based on the NRAC risk assessment, CBSA targeters will gather more information about high-risk cargo. This information gathering may involve CBSA Intelligence as well as other agencies.

6.6.5 Cargo Security Mandate

Under the *Smart Border Declaration*, Canadian and American border officers may jointly inspect marine cargo bound for their respective countries at the first port of arrival in North America. American Customs officials are stationed at the ports of Halifax, Montreal and Vancouver, while Canadian officials are stationed at the ports of Seattle-Tacoma and Newark.[180] When in Canada, American Customs officials have access to American databanks only, and make their own targeting decisions based on internal information and guidelines. The same is true of CBSA officers working at American ports. However, home country personnel conduct the actual examinations of cargo containers. There is no formalized information-sharing system associated with this initiative, although there may be some informal, ad hoc sharing of information.

Currently, American Customs officers are present at key ports outside North America to screen marine container shipments bound for the United States prior to loading. This initiative, known as the Container Security Initiative, aims to disrupt terrorist activity that targets marine shipping.[181] Canada is planning to join this initiative and is currently negotiating with several countries about deploying CBSA officials at important shipping ports.[182]

In addition, the American Department of Homeland Security has deployed four gamma-ray scanning systems to capture images of rail cargo on Canadian soil.[183] These machines scan only rail shipments bound for the United States. CBSA and RCMP agents will provide support to U.S. Customs personnel should any high-risk security threats be detected.[184]

The CBSA also enforces the *Export and Import Permits Act*. The Act requires exporters of certain strategic goods such as munitions and missile technology, goods related to atomic energy, nuclear proliferation, or chemical or biological weapons,[185] and goods to certain countries[186] to obtain an export permit from the Minister of Foreign Affairs. Goods being exported without permits may be seized at the border and forfeited. CBSA officers administering this act have all the powers provided for in the *Customs Act* in relation to goods, including police powers of search, detention, seizure and forfeiture.[187] To administer this act, the CBSA collects information on exporters and importers of strategic goods and conducts intelligence analyses.

6.6.6 Participation in Integrated Teams

6.6.6.1 The CBSA and the RCMP

The CBSA participates regularly in joint initiatives with other Canadian government agencies, including the RCMP, to deal with issues of joint concern. The CBSA sends a representative to ITAC, which I discussed earlier in this chapter, and to INSETs and IBETs, which I discussed in Chapter IV. The CBSA's participation in these teams has a border control nexus. In any integrated team environment, CBSA information is maintained in separate databases, and the CBSA informs me that only relevant, focused information is brought forward to the team as a whole. The CBSA controls the further use or dissemination of its information in integrated environments.

The CBSA may also request ad hoc RCMP assistance for major enforcement operations.[188] In the context of such operations, the RCMP and the CBSA jointly develop a strategic plan, which the RCMP then approves. During joint operations, the CBSA assists the RCMP as the Force requests, and directs CBSA officers and resources in consultation with the RCMP.[189] The RCMP may also assist the CBSA in arresting, transporting and removing individuals when the two agencies determine that the situation is potentially dangerous.[190]

The CBSA also participates in several other permanent integrated teams with the RCMP, including:

- the RCMP's joint ports and waterfront investigation teams, which conduct investigations and gather intelligence concerning organized crime and national security matters at ports and marinas;[191]
- the RCMP's Integrated Proceeds of Crime units, which aim to track and seize proceeds of crime, including smuggling of contraband. Representatives from the Canada Revenue Agency[192] and the Department of Justice also participate in these integrated units;[193]
- the RCMP's Combined Forces Special Enforcement Unit as part of the Border Agency's mandate to screen travellers and immigrants for links to organized crime;[194] and
- Integrated Market Enforcement Teams, which deal with capital markets fraud.[195]

In addition, RCMP members from the RCMP's Airport Federal Enforcement Section may respond to specific requests for assistance from the CBSA.

The RCMP and the CBSA share information about Canadian citizens and permanent residents through both formal and informal co-operative information-sharing practices. The two bodies exchange strategic and tactical intelligence as well as intelligence on individual cases in the national security field.[196] Tactical intelligence may include information about enforcement activities, strategies and policies.[197] Informal information sharing occurs regularly between individual RCMP and CBSA officers: for example, a CBSA officer will contact a local RCMP member whenever contraband is seized at a border crossing. The CBSA and the RCMP share information with each other by request and on their own initiative.[198]

The following list describes some of the ways that the CBSA and the RCMP share information:

- The CBSA must provide the RCMP with access to any evidence, statements, intelligence or internal notes in its possession related to the prosecution of criminal offences by the RCMP.[199] Generally, however, where the CBSA makes an arrest for a criminal offence, the CBSA controls the evidence until the point of a criminal prosecution.
- Upon request, the RCMP provides the CBSA with evidence to prosecute offences under the *Immigration and Refugee Protection Act* or other legislation.[200]
- The RCMP may request CBSA assistance in prosecuting offences that require the consent of the Attorney General of Canada to initiate proceedings.[201] For example, the Attorney General of Canada's consent is required to prosecute offences against United Nations personnel, terrorist-financing offences, or terrorist activities that occurred outside Canada where the accused is not a Canadian citizen.[202] Consent is also required to prosecute the offence of human smuggling under the *IRPA*.[203]
- The RCMP notifies the CBSA of any permanent resident or foreign national who has been charged under any act of Parliament so that the CBSA may take appropriate action.[204]
- The CBSA notifies the RCMP of the deportation of any individual with a serious Canadian or foreign criminal record. The RCMP notifies the CBSA of the extradition of any non-citizen from Canada.[205]
- The CBSA may, on its own initiative, share information obtained in immigration and customs interviews with the RCMP.[206] If the CBSA conducts an interview or examination based on lookout information from the RCMP, the CBSA reports back to the RCMP any information that it obtains.

- The RCMP may provide information to the CBSA for use in immigration and customs interviews, and may request that the CBSA seek clarification of specific points during an interview.
- RCMP and CBSA officers may conduct joint interviews of travellers, immigrants or refugees at points of entry into Canada. Such RCMP assistance may be requested where national security concerns arise.[207]
- Most CBSA officers can retrieve information from certain RCMP databases. A small number of CBSA personnel may also add or modify information relating to CBSA prosecutions under the *Customs Act* in one RCMP database.[208] The CBSA may disseminate information obtained from these databases only in accordance with the information-sharing legislation that I discuss above, and in some circumstances, with the RCMP's permission.
- The CBSA and the RCMP, along with CIC and CSIS, are designing a system to transmit electronically information used for screening immigrants from overseas CIC officers to CSIS and the RCMP in Canada. This system will interface with the shared CIC/CBSA immigration database.
- The RCMP and CSIS may conduct joint threat assessments. On request, the RCMP will give the CBSA a threat and risk assessment on the safety of CBSA staff and the public with respect to CBSA activities relating to litigation, investigation and the removal of individuals.[209]
- The CBSA uses the RCMP to pass information to local police forces.
- The RCMP may request that the CBSA allow otherwise inadmissible individuals to enter or remain in Canada to assist with police operations or criminal proceedings.[210]
- The CBSA may request that an individual be included in the RCMP's witness protection program.[211]
- The RCMP and the CBSA may exchange personnel.

The RCMP, the Department of Justice and the CBSA also work together in the Interdepartmental Operations Group to investigate, prosecute and/or deport suspected war criminals from Canada.[212]

6.6.6.2 The CBSA and Other Agencies and Departments

The *CSIS Act* mandates CSIS to advise the Government of Canada, the Minister of Citizenship and Immigration, and the Minister of Public Safety on matters concerning the security of Canada that relate to citizenship or immigration.[213] CSIS and the CBSA work very closely at both regional and headquarters levels to ensure that individuals who are either inadmissible to Canada or of interest

to CSIS are intercepted and examined by the CBSA. CSIS officers are stationed at major points of entry to provide advice on national security threats in the context of immigration legislation. In addition, although the coordination of lookouts between CSIS and the CBSA is done at the headquarters level, when the CBSA encounters the subject of an *IRPA* or Customs lookout, it advises CSIS at a regional level. The CSIS regional investigator will be the first-line responder. Depending on the nature of the lookout, CSIS may or may not participate in interviewing the person who is the subject of the lookout.

The CBSA and CSIS also have agreed to exchange information and intelligence upon request for both law enforcement and investigative purposes,[214] and CBSA officers may collect information for CSIS. Except in urgent situations, CSIS requests for information would be sent to CBSA Headquarters and then relayed to the appropriate field office. CBSA Intelligence officers may contact CSIS directly when national security concerns arise, and CSIS personnel may also conduct joint interviews with CBSA officers that are not related to lookouts.

The CBSA is also a member of the Interdepartmental Marine Security Working Group led by Transport Canada, and has officers at the Marine Security Operations Centres discussed in the Transport Canada section below.

In a crisis situation, the CBSA would also send a representative to the Government Operations Centre, which I discuss in relation to PSEPC, and to the RCMP's National Operations Centre.

The CBSA participates in several national security initiatives involving both Canadian and American authorities. The RCMP is the CBSA's main Canadian partner in joint Canada/U.S. border enforcement, while the Department of Homeland Security and the U.S. Coast Guard are its key American partners.

6.7 INFORMATION SHARING

The CBSA is permitted by law to disclose information for the "purposes of national security, the defence of Canada or the conduct of international affairs."[215] Under this provision, the CBSA shares information with both domestic and foreign agencies. In addition, Customs and Immigration information is shared according to the provisions of the *Customs Act*, *the Immigration and Refugee Protection Act* and the *Privacy Act*.

- Customs information sharing, including the sharing of API/PNR data, is regulated by section 107 of the *Customs Act*.[216] Under the *Customs Act*, Customs information related to national security or the defence of Canada may be disclosed to officials in other government departments that have

responsibility for national security matters.[217] These departments include CSIS, DND, the RCMP, PCO, the CSE, PSEPC, Transport Canada, the Canadian Coast Guard, and the Department of Fisheries and Oceans.

- The *Customs Act* also authorizes the disclosure of information for law enforcement purposes in various circumstances,[218] including where the CBSA officer reasonably believes that the information relates to the investigation or prosecution of indictable criminal offences or import/export offences.[219]
- CBSA Customs may also share information about the cross-border movement of people with CBSA Immigration for the purposes of administering or enforcing the *Immigration and Refugee Protection Act*.[220]

The *Immigration and Refugee Protection Act* allows the CBSA to share immigration information for the purposes of national security, the defence of Canada and the conduct of international affairs.[221] For these purposes, the CBSA may share with CSIS, the RCMP, DFAIT, the CSE, PSEPC and DND. CBSA Immigration also may disclose personal information to the RCMP, CSIS, SIRC or any other federal investigatory body[222] to enforce Canadian law or carry out a lawful investigation.[223] Such information may also be shared with any provincial or foreign government or international body for law enforcement or investigatory purposes under the terms of an agreement.[224]

Approximately 150 government arrangements and agreements reference the sharing of immigration and citizenship information.[225] These include federal-provincial agreements, agreements with domestic agencies and non-governmental organizations such as the Red Cross, arrangements with the United States and other foreign governments, and arrangements with various airlines concerning the transportation of persons into Canada.[226] Currently, the most important international information-sharing agreements in the immigration field are the *Statement of Mutual Understanding* between Canada and the United States, which I discuss in the section on CIC, and the TUSCAN/TIPOFF Aide-Memoire with the United States, which I discuss below.

By law, the CBSA exchanges certain information with FINTRAC, Canada's financial intelligence agency.[227] The CBSA reports to FINTRAC importations and exportations of currency or monetary instruments over $10,000 and information about currency seizures.[228] The CBSA may also disclose additional information about importations or exportations if it suspects that the information would help FINTRAC detect, prevent or deter money laundering or terrorist financing.[229] CBSA officers also disclose information received under this part of the Act directly to the RCMP where the information would be relevant to the prosecution

or investigation of money laundering or terrorist financing.[230] By law, the CBSA must record the reasons for any such disclosures.[231]

FINTRAC discloses information to the CBSA if it has reasonable grounds to suspect money laundering or terrorist financing, or if it determines that the information is relevant to an offence of evading payment of taxes or duties,[232] or to an individual's inadmissibility to Canada for reasons of national security, criminality, involvement in war crimes, organized crime, money laundering or terrorist financing.[233] FINTRAC may also make disclosures to the CBSA if it suspects that an individual has committed a human smuggling or trafficking offence, or has made misrepresentations in the course of the immigration or refugee process.[234]

Finally, the CBSA receives information from CIC domestically and abroad, from front-line CBSA officers in Canada, local Canadian law enforcement agencies, business sources and partnership agreements, and anonymous tips, and through its informant program. Information from anonymous tips and informants is scrutinized closely.

6.7.1 International Partners

The CBSA's most extensive foreign information-sharing relationship is with the Customs and Border Protection Branch of the U.S. Department of Homeland Security.

CBSA Customs shares information with U.S. Customs counterparts under the 2004 *Memorandum of Understanding for the Automated Exchange of Lookouts and the Exchange of API for High Risk Travellers*, discussed above, and under a 1984 treaty.[235] The treaty is complemented by a 1982 memorandum of understanding on the sharing of selected Customs intelligence information, including personal information, between what is now CBSA Customs, the RCMP, and the U.S. Customs and Border Agency.[236] The Privacy Commissioner has recommended that the CBSA seek to update and strengthen its personal information-sharing agreements with the United States, including by establishing processes to protect trans-bordered personal information.[237]

The CBSA has 15 mutual assistance agreements in force in the customs field and close to 25 agreements under negotiation with various countries.[238] The most commonly used agreements are with the United States, the United Kingdom and France. Under these agreements, the CBSA will often share its analytical products, including trend analysis, with international partners. International partners may request assistance with respect to the movement of people, and occasionally partners will share lookout information.

In the immigration field, Canada and the United States share information under a *Statement of Mutual Understanding* in relation to the sharing of immigration information, and under a 1997 agreement for the exchange of terrorist watch lists, which I have discussed above in relation to the National Risk Assessment Centre.

Canada has signed memoranda of understanding to exchange immigration-related information with Australia,[239] the Netherlands,[240] the U.K.,[241] New Zealand[242] and Hong Kong.[243] Not all these arrangements are currently operational, however.[244] In general, these arrangements permit the sharing of information, including personal information, to enforce or administer immigration and citizenship laws and regulations, as applicable.

7.
CITIZENSHIP AND IMMIGRATION CANADA

7.1
RELEVANT LEGISLATION

- *Citizenship Act*, R.S.C. 1985, c. C-29
- *Immigration and Refugee Protection Act*, S.C. 2001, c. 27 (*IRPA*)

7.2
MANDATE

The Department of Citizenship and Immigration (CIC) and the CBSA have joint responsibility for managing immigration and entry to Canada by non-citizens. In broad terms, CIC's mandate is to maximize the benefits associated with migration and the mobility of persons. CIC focuses on the selection, settlement and integration of immigrants and refugees in Canada. In the context of non-citizens, the CBSA, on the other hand, focuses on enforcement, threats and risks to Canada.

CIC and the CBSA collaborate closely, and officers from one department sometimes perform functions that fall within the responsibility of the other.[245] In addition, individual cases may move from one department's mandate to the other's as circumstances change. For example, some individuals may begin the immigration or refugee admission process without being considered a threat, and so fall under CIC's mandate. If these individuals are later ordered removed from Canada because they are found to be inadmissible, the CBSA takes over management of their files. On the other hand, individuals subject to deportation orders could regularize their status and so move from the CBSA's mandate to fall

within CIC's area of responsibility. Even with the creation of the CBSA, however, numerous CIC officials are still designated as peace officers, meaning that they have powers similar to those of a police officer. CIC also has several dedicated marine security officers who work in co-operation with the CBSA, port authorities and police agencies to target and prevent the entry of inadmissible individuals. As with all immigration officers, the *IRPA* gives marine security officers the power to detain, refuse entry to and report people who are inadmissible to Canada.

7.3
NATIONAL SECURITY ACTIVITIES

CIC is involved in two principal types of activities touching on national security. First, CIC screens temporary visa and immigration applicants, applicants for citizenship and refugee claimants, within and outside Canada. Second, CIC performs pre-removal risk assessments, which I discuss below.

Potential immigrants to Canada, refugee claimants and temporary-visa applicants are screened prior to entry to determine their admissibility under the *Immigration and Refugee Protection Act*. CSIS' role in front-end screening has been set out above. CIC is the lead agency in relation to criminality screening,[246] whereas the CBSA has primary responsibility for security screening, including screening for national security concerns and war crimes involvement.[247] CIC and the CBSA work closely together during this screening process.[248]

Where the CBSA has reason to be concerned that an individual may be inadmissible to Canada, a lookout flag may be attached to that person's name in the immigration database shared with CIC.[249] Based on the information in the lookout and any information gathered during the immigration or visa process, a CIC officer dealing with the file determines whether the case should be referred to the RCMP or CSIS for further investigation. The RCMP is notified if there are concerns about serious criminality, involvement in organized crime or war crimes.[250] CSIS is notified of concerns relating to threats to the security of Canada. The Counter Terrorism Section of the CBSA Intelligence network also assists with security screening.[251] If, after further investigation, the RCMP or CSIS finds no information to substantiate the concern, they send their report to CIC. If the concern is substantiated, the RCMP or CSIS sends a report to the CBSA and notifies CIC that concerns have been raised. The CBSA then provides advice to CIC. In both scenarios, the final admissibility decision remains in the hands of a CIC Immigration official with the appropriate delegated authority. The CBSA, the RCMP or CSIS is informed of the decision.

The front-end screening process for refugee claimants was introduced in 2001 to identify and filter potential security cases from the refugee claimant stream as early as possible in the determination process.[252] Individuals claiming refugee status at points of entry to Canada have an initial screening interview conducted by CBSA officers, while those applying from overseas are interviewed by CIC officers. Both CIC and the CBSA conduct screening interviews within Canada. Refugee claimants are photographed and fingerprinted, and this information is passed on to the RCMP and CSIS, which respectively conduct criminal record checks and security screening.[253] The refugee claimant screening program is conducted by the CSIS Security Screening Branch to provide security-related advice to the CBSA. RCMP or CSIS presence may also be requested during interviews with refugee claimants or applicants for temporary or permanent visas when national security concerns arise,[254] and may make oral recommendations to CIC Immigration personnel. Despite the involvement of CSIS and the RCMP in the screening process, after the initial interview, CBSA officers determine whether a refugee claimant who is present within Canada or at a point of entry should be detained or released before a hearing before the Immigration and Refugee Board.[255]

Under an annex to the *Statement of Mutual Understanding*, information about asylum seekers obtained during the interview and screening process may be shared with the United States.[256]

7.3.1
Pre-removal Risk Assessments

CIC personnel are responsible for conducting pre-removal risk assessments for certain non-citizens ordered deported from Canada.[257] Under the pre-removal risk assessment process, individuals subject to security certificates, immigration and visa applicants, and refugees declared inadmissible on grounds of national security, war crimes or organized criminality[258] may apply to the Minister of Citizenship and Immigration for protection from deportation on the basis that they would be at serious risk of death, torture or inhumane or degrading treatment after being deported from Canada.[259] In security certificate cases, the pre-removal risk assessment process occurs after the ministers of Public Safety and Citizenship and Immigration have signed the certificate, but before the Federal Court judge reviews that certificate.[260]

The pre-removal risk assessment process will recommend that the deportation order not be enforced only if there is a serious reason to believe that the risks the individual will face on return to their home country outweigh the risks

the individual poses to the Canadian public or the security of Canada, or the nature and severity of the acts the individual has committed.[261]

The Minister of Citizenship and Immigration delegates a CIC official to assess the risks the individual will face upon deportation. The decision concerning these risks to the individual must be made according to the rules of evidence,[262] which, for example, do not allow statements made outside of court to be used as proof except in very limited circumstances.[263] All the information used to determine the risk of torture or inhuman or degrading treatment is disclosed to the individual in question.[264] A different CIC official then determines whether it is reasonable to believe that the person poses a danger to national security (referred to as a danger opinion).[265] At this second stage, the whole of the information on which the decision is based may not be disclosed to the individual, and the CIC official may consider any information, even if it would not be admitted in a court under the rules of evidence.[266] Next, the individual subject to the security certificate has an opportunity to make submissions on the risk assessment and the danger opinion.[267] Finally, another, senior CIC official balances any risk of torture against the risks that the individual poses to Canada and decides whether the individual should be granted protection from deportation.[268] A Federal Court judge then reviews the lawfulness of this decision.[269]

Individuals who are subject to security certificates, but against whom the deportation orders have been stayed, remain inadmissible to Canada. As a result, these individuals can be held in an immigration detention facility until they no longer face a serious risk of torture, inhuman or degrading treatment, or until a Federal Court judge orders their release at a detention review because the judge is satisfied that the individuals do not pose a danger to national security or to the safety of any person. CIC also reviews the stay if conditions in the individual's home country change.[270]

7.4 INFORMATION-SHARING ROLE

Intelligence analysis no longer falls within CIC's mandate, but is now a CBSA function. Although CIC no longer analyzes intelligence, it does collect and share intelligence and information within Canada and internationally.[271]

CIC's closest information-sharing relationship is with the CBSA. CIC relays information, data and raw intelligence to the CBSA, and receives intelligence information and products from the CBSA. Information provided by CIC to the joint CBSA/CIC database is discussed above in the section dealing with the CBSA. CIC has information-sharing agreements with both the RCMP and CSIS,[272]

but in light of the creation of the CBSA, both agreements are being renegotiated. However, CIC and the RCMP still co-operate and coordinate activities through regional joint committees.[273]

One of the key international immigration information-sharing agreements is the 2003 *Statement of Mutual Understanding on Information Sharing* (SMU) between Canada and the United States. The Statement provides a mechanism to exchange a wide variety of personal information between Immigration authorities in individual cases for the purposes of the SMU.[274] One of the purposes of the SMU is to share information about individuals who may pose a national security risk to either country.[275] Information may be shared upon request or on the initiative of either Canada or the United States.[276] The SMU provides that requests for information should normally be made in writing, or confirmed in writing as soon as possible after the request has been made.[277] In Canada, both CIC and the CBSA share information under this agreement. The agreement provides a mechanism for information sharing, while existing legislation and agreements in Canada and the United States govern the information that may be shared. Information on permanent residents may be shared by CIC for purposes consistent with the *IRPA*, subject to the *Privacy Act* and the Charter.[278] The types of information that can be shared include the following:

- fingerprints and biometric data;
- work history;
- marital status and family composition;
- education;
- telephone numbers;
- any documents submitted in support of an immigration application;
- relevant criminal or security intelligence; and
- any other information relevant to the request and consistent with the purposes of the SMU.[279]

Although the SMU includes confidentiality guarantees, information can be passed on, without written permission from the originating agency, to a number of specified entities for citizenship, immigration or "border management" functions.[280] The entities listed include the FBI, CIA and Department of Defense in the United States and the RCMP, CSIS, DFAIT and DND in Canada.[281] Information may also be shared with any relevant oversight or review agency.[282] Once information about a person has been shared, it is up to the recipient of the information to ensure that the information has not been changed or corrected before acting on it.[283]

An annex to the *Statement of Understanding* allows the automated, systematic sharing of information about refugee claimants.[284] At the time of writing, the Annex has been agreed upon but not yet implemented. Under the Annex, Canada and the United States will systematically compare basic identity data or biometrics (e.g., fingerprints) to identify refugee claimants who have had previous contact with authorities in either country. Where an applicant has had previous contact, all information relevant to the refugee claim, including information relating to criminal or security concerns, will be exchanged. Records that do not result in a match will be destroyed[285] When implemented, the Annex will allow the recipient to pass information on to other branches within each government for the purpose of determining or reviewing refugee status claims.[286] Information on citizens or stateless habitual residents of either country who are claiming refugee status in the other country will not be exchanged.[287] Written permission from the originating government will be needed before information can be shared with other foreign governments or international organizations.[288]

Canada and the United States also have two other information sharing agreements. The 1997 TUSCAN/TIPOFF Aide-Memoire provides for the sharing of data to prevent terrorists from entering North America.[289] Another more recent agreement deals with the return of refugee claimants to safe third countries.[290]

CIC's directives for sharing information under the *Statement of Mutual Understanding* state "officers designated to share information should ensure that the information being provided is not likely to result in danger to any person or to cause serious injustice."[291] Officers are also directed to ensure that only relevant and necessary information is disclosed, and are reminded that they may attach terms and conditions to the information shared.[292] Similarly, officers are directed to record all information shared under the agreement and to notify relevant American entities that received information has been updated or corrected.[293]

8.
TRANSPORT CANADA

8.1
RELEVANT LEGISLATION

Transport Canada works under various statutes. Some of the most important are the following:

- *Aeronautics Act*, R.S.C. 1985, c. A-2
- *Canada Marine Act*, S.C. 1998, c. 10
- *Canada Shipping Act*, R.S.C. 1985, c. S-9
- *Canadian Air Transport Security Authority Act*, S.C. 2002, c. 9, s. 2
- *Department of Transport Act*, R.S.C. 1985, c. T-18
- *Marine Transportation Security Act*, S.C. 1994, c. 40
- *Motor Vehicle Safety Act*, S.C. 1993, c. 16
- *Navigable Waters Protection Act*, R.S.C. 1985, c. N-22
- *Public Safety Act, 2002*, S.C. 2004, c. 15
- *Railway Safety Act*, R.S.C. 1985, c. 32 (4th Supp.)
- *Transportation of Dangerous Goods Act, 1992*, S.C. 1992, c. 34

8.2
MANDATE

Transport Canada is responsible for safeguarding Canada's transportation system, which includes transportation by air, rail, road and water. While the department does not run municipal mass transit, it takes the lead on national security matters in this area as well. Transport Canada sets policy and conducts inspections related to the safety and security of air, surface and maritime transportation and transport infrastructure.[294] Under this rubric, the department has responsibility for setting security standards for airports, surface transport, marine vessels (including cargo ships), ports and marine facilities. Inspectors enforce compliance with legislation and policies that govern transportation carriers.

Transport Canada has an intelligence branch that receives intelligence and transportation security information from CSIS, the CSE, DND Intelligence, CIC, the CBSA, the RCMP, Environment Canada and the Coast Guard. This information is analyzed to identify threats to Canada's transportation infrastructure. Transport Canada may then inform federal, provincial, municipal and private-sector transportation providers of credible national security threats relating to

transport, if the agency that gave the intelligence to Transport Canada agrees to its onward disclosure.[295]

8.3 TRANSPORT CANADA INTELLIGENCE

The department's intelligence analysis work is done in Ottawa by a group of roughly 15 people. Another 50 people are involved in processing security clearances for workers with access to sensitive areas in airports.[296]

The RCMP, CSIS, the CSE, DND, PCO, DFAIT, ITAC, the CBSA and other federal intelligence collectors regularly share intelligence reports with Transport Canada. Transport Canada receives the RCMP's Civil Aviation Protective Intelligence Unit's information bulletin, for example. The RCMP also provides Transport Canada with written threat assessments where the Force has specific intelligence on a potential threat involving a Transport Canada matter. Some intelligence reports may contain personal information, depending on the issue in question.

The department also may request intelligence to verify the credibility or reliability of previously obtained threat intelligence. Again depending on the issue, this intelligence may also include personal information. For example, Transport Canada could receive intelligence about a passenger on the U.S. no-fly list who is flying over Canadian airspace and who has been assessed by the United States as posing a threat to aviation security. Generally, the RCMP provides written threat assessments where they have specific intelligence on a potential threat. Transport Canada will then assess the information to determine whether it is relevant to transportation security. Most of the intelligence that the department receives from the RCMP relates to security clearances for employees working in restricted or sensitive areas in airports. Transport Canada also receives information from the Coast Guard relating to commercial vessel traffic, which it then evaluates from an intelligence perspective.

Transport Canada provides both classified and unclassified reports on transportation security. Within Transport Canada, intelligence is used to support departmental programs and operational responses. These reports give an assessment of a particular threat or issue related to transportation security — a report might discuss methods that terrorists use to circumvent security measures, for example. Personal information on suspected terrorists could be included where appropriate, but most reports would not include personal information. Transport Canada uses intelligence to design policies and make decisions. The department may also provide information obtained through its

inspections to the RCMP, but only if this information is of immediate law enforcement value.

8.4
TRANSPORT SECURITY INITIATIVES

Transport Canada has significant responsibility for integrating the national security capabilities of various federal government departments relating to transportation security. Its initiatives include the following:

- Leading the Interdepartmental Marine Security Working Group. The Group is made up of 16 different departments and agencies,[297] and includes a subworking group that examines legal issues related to the sharing of marine security information, and particularly the sharing of information by Marine Security Operations centres.
- Leading the creation of a secure information system intended to facilitate the sharing of marine security information (Maritime Information Management Data Exchange) and Marine Security Operations centres.[298]
- Leading the Interdepartmental Working Group on Aviation Security, which includes representatives from the RCMP, CSIS and the CBSA.
- Creating programs designed to increase scrutiny of air passengers.
- Leading the Interdepartmental Threat Assessment group for Railway Security, along with representatives from the RCMP, the Canadian Forces, CSIS, the CBSA, the CSE and DFAIT.
- Leading various cargo security initiatives.

I discuss some of Transport Canada's most important security initiatives below.

8.4.1
Maritime Security

8.4.1.1
Marine Security Operations Centres

Marine Security Operations Centres (MSOCs) are intended to detect, assess and respond to marine security threats. Transport Canada, DND/CF, the CBSA, the RCMP, and the Department of Fisheries and Oceans/Canadian Coast Guard send representatives to MSOCs.[299] MSOCs collect and analyze raw information and intelligence, largely related to marine domain awareness.[300] It is expected that MSOCs will share only finished intelligence products with other Canadian government agencies, although this sharing has not yet begun. This intelligence will

likely be shared on both a push and a pull basis, meaning that some intelligence products will be regularly made available for agencies that need the information, while tailored products will be developed for specific cases or in response to queries. Intelligence will be shared with the participating agencies, other government agencies that need the information, IBETs and INSETs.[301] MSOCs may be involved in sharing personal information, in accordance with relevant legislation. However, DND advises that MSOC agencies generally would not need personal information held by other organizations.

Although the overall planning and implementation of MSOCs is a Transport Canada initiative, the Canadian Navy leads operations at the MSOCs in Halifax, Nova Scotia, and Esquimalt, British Columbia.[302] The RCMP leads operations at a third, interim MSOC, on the Great Lakes–St. Lawrence Seaway that currently has representatives from only the RCMP and DND.[303] MSOCs have access to the Government Operations Centre in Ottawa, as well as to the Coast Guard marine communications and traffic services systems.[304] However, as in ITAC, each participating department has access to its own databases only.

Within a MSOC facility, a Coast Guard officer's role is to improve maritime situational awareness by collecting maritime data to be analyzed and used by MSOC partners. This information includes current weather and geographic conditions and real-time reports from personnel on Coast Guard vessels conducting surveillance, reconnaissance or other routine activities in relation to commercial vessel and pleasure craft traffic. In addition, Coast Guard officers within the MSOC maintain linkages to other Coast Guard maritime field resources to report or help confirm occurrences that may have national security implications, and support analytical intelligence activities at the MSOC.

8.4.1.2 MIMDEX

In 2003, the Interdepartmental Marine Security Working Group sponsored a study on the Maritime Information Management Data Exchange (MIMDEX). The study concluded that the various departments and agencies involved in maritime security did not have the necessary information infrastructure to bring together relevant security information. MIMDEX, which is not operational at the time of writing, will integrate various government departments (other than CSIS[305]) into a wide-area network. It will use information from existing government systems to provide a more complete marine status "picture," facilitate coordinated action and alert departments to targets of potential interest.[306]

8.4.2 Aviation Security

8.4.2.1 Security Screening

Transport Canada also conducts security clearances for airport employees who require access to restricted or sensitive areas.[307] The RCMP or CSIS collects the information, but any decision to refuse clearance lies with the Department of Transport.[308] Transport Canada is developing a system of clearances for port and rail workers, as well as a background-check program for truckers who transport dangerous goods across the Canada-U.S. border, which both countries will recognize.[309] Most of the interaction between the RCMP and Transport Canada concerns these security clearances.

8.4.2.2 Air Passenger Scrutiny

In relation to the air transport portion of its mandate, Transport Canada is creating a no-fly list of specified persons (called Passenger Protect) in conjunction with PSEPC portfolio agencies, including CSIS, the RCMP and the CBSA.[310] The list will include the names of individuals who the Minister of Transport believes pose "an immediate threat to aviation security."[311] Individuals whose names are listed will not necessarily be prevented from boarding an aircraft, but they may be subject to additional scrutiny and questioning before boarding the plane. Canadian security intelligence or law enforcement agencies, or foreign agencies such as the American Transportation Security Administration, could ask that a certain person be placed on the list. Transport Canada will review the proposal and make a recommendation to the Minister of Transport. In the case of requests from foreign agencies, the department will also seek advice from the RCMP and CSIS. Airlines will check passenger names against the list and any person whose name appears will not be allowed to board the plane. The list is expected to be put into place in early 2007, and will include some form of reconsideration mechanism.[312]

For the purposes of transportation security, Transport Canada may also ask airlines for API/PNR information[313] on specific passengers or on all passengers on specific flights. Such information includes name, nationality, passport number, dates of travel, amount of checked baggage, seat assignment, travel itinerary, method of payment and other booking information.[314] The *Aeronautics Act* allows Transport Canada to share this information — for the purposes of

transportation security only — with the Minister of Citizenship and Immigration, the Minister of Public Safety, the CEO of the Canadian Air Transport Security Authority, or designated CSIS and RCMP personnel. The law also allows the ministers of Public Safety and CIC, and the CEO of CATSA, to share the information with CBSA, CIC and CATSA employees. Information provided to designated CSIS or RCMP officials may be disseminated further in the same way as the information described below.[315]

Under the *Aeronautics* Act, and in conjunction with the Minister of Public Safety, Transport Canada is creating a system that will allow designated RCMP and CSIS officials to receive and analyze passenger information and match it against RCMP and CSIS databases,[316] or other information in their control, without a warrant.[317] Once the relevant legislation comes into force,[318] designated CSIS personnel will be able to disclose API/PNR information within CSIS or to other agencies for national security and transportation security purposes. Information disclosed within the Service could later be shared with domestic agencies with which CSIS has intelligence-sharing arrangements, or with foreign agencies as part of an ongoing investigation.[319] Designated CSIS personnel who share this information, either within or outside the Service, will be required by the *CSIS Act* to keep a record of the disclosure and the reasons for it for the purposes of review by SIRC or the CSIS Inspector General.[320]

Designated RCMP personnel will be able to share passenger information for transportation security purposes.[321] The RCMP, for example, could use this information to assign aircraft protection officers (commonly referred to as "sky marshals") on flights, or to arrest individuals prior to boarding.[322] Designated RCMP personnel also may share this information to enforce arrest warrants for indictable offences punishable by five years or more imprisonment, which are listed in proposed regulations;[323] and to enforce arrest warrants under the *Immigration and Refugee Protection Act* and the *Extradition Act*.[324]

The legislation is intended to provide CSIS and the RCMP with a continuous feed of all passenger information for all international inbound, outbound and domestic flights within Canada.[325] In addition, Transport Canada is considering implementing an automated passenger assessment system in the future.

The *Public Safety Act, 2002* included *Aeronautics Act* provisions that allow for the creation of the no-fly list, as well as case-by-case and systematic sharing of passenger information between Transport Canada, the RCMP and CSIS.[326] I have discussed the Act in more detail in Chapter III.

9.
CANADIAN AIR TRANSPORT SECURITY AUTHORITY

9.1
RELEVANT LEGISLATION

- *Aeronautics Act*, R.S.C. 1985, c. A-2
- *Canadian Air Transport Security Authority Act*, S.C. 2002, c. 9 (*CATSA Act*)

9.2
MANDATE

The Canadian Air Transport Security Authority (CATSA) is a Crown corporation established by the Canadian government as part of its response to the 2001 terrorist attacks on the United States. CATSA is responsible to Parliament through the Minister of Transport.[327] CATSA came into existence on April 1, 2002, and has a very specific mandate.[328] It is responsible for:

- screening air passengers and their belongings before passengers board the aircraft;
- operating, maintaining, acquiring, installing and positioning systems to detect explosives at designated airports;[329]
- transferring specified funds to the RCMP for the Canadian Air Carrier Protective Program, which places armed RCMP officers on certain flights designated by the Minister of Transport and all flights to Reagan National Airport in Washington, D.C.;
- implementing an enhanced identification card for non-passengers to control access to restricted areas at major Canadian airports. The new card includes biometric identifiers such as fingerprints and iris scans;
- random screening of non-passengers (flight crews, concessions employees, baggage handlers, etc.) accessing restricted areas at major airports; and
- contributing towards the financial cost of increased policing at airports.[330]

CATSA designs procedures for airport screening and trains screeners,[331] but contracts with private companies (screening providers) who employ the individual screeners themselves.[332] CATSA's mandate focuses on items rather than individual travellers: it is concerned with the items that passengers try to bring on board an aircraft.[333] However, CATSA's CEO may receive information from Transport Canada about specific individuals or individuals on board a specific flight to which there is an immediate threat.[334] CATSA is also responsible for

screening and verifying the identity of non-passengers who have access to restricted areas at designated airports.

Although all air passengers must submit to a search before boarding an aircraft, CATSA's screening officers have no police powers to arrest or detain individuals.[335] Therefore, like any private person, CATSA screening officers may arrest an individual whom they find committing a criminal offence or whom they reasonably believe has committed a criminal offence and is fleeing from the police or another authority.[336] In the case of such an arrest, the CATSA screening officer must deliver the suspect to a police officer or other authorized person as quickly as possible.[337] In practice, police officers would collect any personal information from an individual stopped by CATSA screeners. Further, CATSA screeners are instructed not to search specific individuals on behalf of police.

CATSA does not have responsibility for screening air cargo or airmail.

Since its mandate relates to screening for prohibited items, rather than for prohibited persons, CATSA generally does not collect any personal information on air passengers. However, CATSA would keep a traveller's personal information if trace amounts of explosives were detected on the individual's luggage or effects. CATSA's responsibility for screening and issuing biometric identification cards to non-passengers accessing restricted areas in airports does involve collecting personal information.

CATSA receives intelligence from Transport Canada. The underlying information may come from agencies such as CSIS, PCO, ITAC or the CBSA. If necessary, CATSA then drafts a bulletin using select, relevant information to disseminate to service providers and screening officers. CATSA would normally receive information about non-specific threats, not information about a particular individual. The RCMP or the local police force would have responsibility for dealing with a specific individual identified as a threat. While the Minister of Transport, or the Minister's delegate, may disclose personal information about airline passengers to CATSA's CEO for transportation security purposes,[338] this power had not been used as of March 2006.

10.
CANADIAN COAST GUARD

10.1
RELEVANT LEGISLATION

- *Canada Shipping Act*, R.S.C. 1985, c. S-9
- *Oceans Act*, S.C. 1996, c. 31
- *Vessel Traffic Services Zones Regulations*, S.O.R./1989-98

10.2
MANDATE

The Canadian Coast Guard is Canada's civilian maritime safety organization and the owner and operator of the federal government's fleet of civilian maritime vessels. The Coast Guard is a decentralized organization that has been designated as a Special Operating Agency within the Department of Fisheries and Oceans Canada. It is responsible to Parliament through that Minister. The Coast Guard administers its own programs and supports programs run by Fisheries and Oceans Canada and other government departments. It is responsible for marine search and rescue, marine communications and traffic management services, icebreaking, marine pollution response, aids to navigation in Canadian waters, and waterway channel maintenance.[339] In addition, the Coast Guard is often called upon to provide expertise and assistance in response to national emergencies. Unlike the members of the U.S. Coast Guard, Canadian Coast Guard officials are not armed and do not have police enforcement powers.[340]

Transport Canada and the Department of National Defence are the lead federal departments for maritime national security. The Coast Guard plays a supporting role.[341] However, the RCMP and the Coast Guard are increasingly integrating their on-water coordination and response operations, and the Coast Guard is involved in integrated national security intelligence initiatives. The Coast Guard's national security support generally relates to maritime domain awareness support activities or to on-water operations support activities. Most information the Coast Guard shares with other Canadian departments or agencies is in the public domain. However, the Coast Guard will put appropriate caveats on disclosure where advised to do so by legal counsel.

10.3
ON-WATER OPERATIONS IN SUPPORT OF NATIONAL SECURITY

The National Security Policy adopts the notion of a secure perimeter extending out and around North America. As a result, the role of the Canadian Coast Guard Fleet as a source of on-water platform and personnel support to the Canadian security community is being emphasized. The Coast Guard's role includes the following:

- Providing search and rescue and disaster response capacity for maritime national security emergencies. Coast Guard vessels are also used to transport RCMP emergency response teams and Canadian Forces JTF 2 teams responding to marine emergencies.[342]
- Serving on the Transport Canada-led Interdepartmental Marine Security Working Group.
- Being a partner in the RCMP/Coast Guard St. Lawrence Seaway–Great Lakes Marine Enforcement program.[343] The program uses Coast Guard vessels as platforms for RCMP officers to perform national security and law enforcement patrols on the St. Lawrence Seaway and the Great Lakes.[344]
- Participating in the DND Secure Fleet Communications initiative that will see the installation of secure communications as well as command and control equipment on the Coast Guard's large vessel fleet, allowing the integration of equipped Coast Guard vessels in the DND command and control realm.
- Supporting Canadian Forces, the RCMP, the CBSA, Transport Canada, Environment Canada, DFO Fisheries Management and Health Canada on-water operations through direct and indirect participation in on-water national security incidents.
- Collecting and collating vessel traffic data with respect to vessels in Canadian waters, by operating radar and marine communications systems, and by controlling marine traffic using the Coast Guard Marine Communications and Traffic Services (MCTS) program. The MCTS program tracks certain types of vessels in Canadian waters,[345] directs marine traffic in congested waterways, monitors and responds to distress calls, screens vessels intending to enter Canadian waters, and relays commercial and private correspondence from ships.[346] Transport Canada and DND are currently negotiating with the Coast Guard for access to its MCTS system. MCTS supports Transport Canada national security activities through an arrangement by which Coast Guard MCTS officers receive the notice of arrival information that Transport Canada requires for commercial vessels intending

to enter Canadian waters. This information is provided to the Coast Guard 96 hours before the vessel enters Canadian waters, verified by the Coast Guard and then forwarded to Transport Canada Marine Security for evaluation from an intelligence perspective.

- Providing maritime traffic data to other Canadian intelligence agencies through Marine Security Operations Centres, which are discussed in the Transport Canada section of this chapter, and upon request to the RCMP, DND/CF, Transport Canada and the CBSA. Through MSOCs, the Coast Guard provides maritime domain awareness input and analysis to IBET operations. Upon request, the Coast Guard will provide information about a specific vessel to other federal agencies. Most vessel traffic data is in the public domain and is accessible on the Internet.
- Upon request by the RCMP, providing vessels and crews to support IBETs, in intercepting illegal traffic in individuals and goods. More rarely, the Coast Guard supports INSETs conducting marine national security operations. The Coast Guard advises that it very rarely provides support to either IBETs or INSETs, and does not have a significant role in either of these integrated teams.

Although not a Coast Guard program, the data collected by aerial surveillance flights operated by the DFO Fisheries Management sector's Conservation and Protection Branch provides DND with surveillance data on maritime vessel activity off the Atlantic and Pacific coasts. Information from these flights includes sightings, vessel types, locations, identification and photography. The data is useful for the effective deployment of other resources such as military and Coast Guard vessels.

11. FINANCIAL TRANSACTIONS AND REPORTS ANALYSIS CENTRE OF CANADA

11.1 RELEVANT LEGISLATION

- *Proceeds of Crime (Money Laundering) and Terrorist Financing Act,* S.C. 2000, c. 17 (*PCMLTFA*)
- *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations*, S.O.R./2002-184
- *Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations*, S.O.R./2001-317

11.2 MANDATE

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) collects, analyzes and discloses information on suspicious and other prescribed financial transactions in Canada. The agency's main function is to support law enforcement and security intelligence investigations into terrorist financing and money laundering. The terrorist financing aspect of FINTRAC's mandate was created by the *Anti-terrorism Act*,[347] which I have discussed in more detail in Chapter III. FINTRAC is responsible to the Minister of Finance[348] and was created to act at arm's length from law enforcement, CSIS and other bodies to which it is authorized to disclose information.[349] Protecting personal information is explicitly included in FINTRAC's mandate.[350]

Although it may receive information from any source, FINTRAC tends to collect information through five main channels: other federal government departments and agencies, foreign intelligence units, private sector reporting, CBSA reporting and inspections of reporting entities.[351]

The RCMP (including the National Security Operations Branch) and other municipal or provincial police forces, CSIS, the CSE, ITAC, the CBSA, the CRA, DFAIT and SIRC may voluntarily provide information to FINTRAC concerning suspected money laundering and terrorist financing operations.[352] However, FINTRAC cannot request specific information from these agencies. Foreign financial intelligence units also provide information about suspicious transactions.[353] Foreign agencies can provide information voluntarily or in response to a request from FINTRAC.

Most of FINTRAC's information comes from private sector reports. Any business providing financial services, including banks, brokerage houses, real estate brokers, and remittance businesses that send money to foreign countries, must provide reports of the following types of transactions to FINTRAC:

- cash transactions over $10,000, other than withdrawals;
- international electronic currency transfers over $10,000, where the sender or the recipient is outside Canada;
- suspicious transactions; and
- reports from an organization that is holding the property of a terrorist group listed in the *Criminal Code*.[354]

FINTRAC also receives reports from the CBSA about the cross-border movement of $10,000 or more in cash or monetary instruments.[355] The Centre issues guidance to help businesses determine which transactions are suspicious,[356] but

leaves the final decision in the hands of the reporting entity on the basis that these businesses are best positioned to know which transactions are unusual in their area.[357] This reporting is mandatory.[358] FINTRAC also conducts inspections, during which it has the power to examine records and inquire into the business and affairs of a reporting entity to ensure compliance.[359] In addition, FINTRAC has access to commercial databases, limited access to one RCMP database[360] and limited access to the Canadian Police Information Centre.[361] FINTRAC has the authority to enter into agreements to access national security databases,[362] but has not yet done so. It also runs education campaigns to promote compliance.[363]

FINTRAC analyzes data to identify patterns that suggest terrorist financing or money laundering activity. To do this, FINTRAC uses its own databases, public and commercially available databases, and other government databases. Where it has reasonable grounds to suspect that information that it is authorized to disclose would be relevant to an investigation or prosecution of terrorist-financing or money-laundering offences, FINTRAC must share that information with the RCMP or other appropriate police forces.[364] Where it has reasonable grounds to suspect that such information would be relevant to threats to the security of Canada, FINTRAC must disclose information to CSIS.[365] FINTRAC must disclose information that it suspects is relevant to the investigation or prosecution of terrorist-financing or money-laundering offences to the Canada Revenue Agency if it also determines that the information relates to an offence of evading or attempting to evade paying taxes or duties imposed by a statute administered by the Minister of National Revenue (e.g., the *Income Tax Act*).[366] The CRA reviews these disclosures to determine whether to undertake tax enforcement action.

FINTRAC has information-sharing agreements with financial intelligence units (FIUs) in thirty foreign countries and may disclose information to those FIUs.[367]

A typical case disclosure would likely identify six or seven individuals or five businesses, and would involve a considerable number of transactions of various kinds, often reported by two or more reporting entities.[368] Approximately 25 percent of FINTRAC's 2004 workload dealt with suspected terrorist financing activity.[369] FINTRAC is required to record the reasons for making disclosures to CSIS, police forces, the CBSA, the CRA and foreign agencies.[370]

In the absence of a judicial order for disclosure, FINTRAC is permitted to disclose only certain designated information, including:

- information about the transactions;
- where the transactions took place;

- the individuals conducting the transactions; and
- any accounts, businesses or other entities involved.[371]

Information about an individual may include name, address, telephone number, citizenship, date of birth, and passport or similar document number.[372] Information voluntarily provided by law enforcement or CSIS is not included in FINTRAC's onward disclosures.

FINTRAC's complete analysis of suspect transactions, including the reasons for suspecting terrorist financing or money laundering, is available only to police officers or CSIS agents, and only if a judge orders disclosure.[373] The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* also provides stiff penalties for wrongful disclosure: FINTRAC staff members who make unauthorized disclosures can face penalties of up to five years in jail or a $500,000 fine, or both.[374] From the time FINTRAC became operational in 2001 until the end of the first quarter of 2006, it received nine court orders to produce its full case analysis. The Auditor General has criticized the restrictions on the information that FINTRAC is permitted to disclose to law enforcement,[375] and the Department of Finance is studying the possibility of expanding the amount of information that FINTRAC may provide.[376] The federal government has recently announced that it plans to make some changes to the regime.[377] FINTRAC does not put restrictions on domestic agencies' use of information from its disclosures.

The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* puts constraints on information that may be disclosed to foreign financial intelligence units:

1. Only the designated information described above may be disclosed.[378]
2. Information may be disclosed only for intelligence purposes related to investigating money-laundering or terrorist-financing offences, or substantially similar offences.[379]
3. Any onward disclosure by the foreign unit requires FINTRAC's consent.[380]
4. Information may only be shared based on an agreement between FINTRAC and the foreign entity.[381]

To consent to onward disclosure by a foreign unit, FINTRAC requires information about the nature of the foreign investigation. Where the foreign investigation is consistent with the purpose for which FINTRAC collected the information in question (i.e., combating money laundering or terrorist financing), FINTRAC will consent to further disclosure. Consent might be refused if disclosure were requested for an unrelated purpose or if FINTRAC had received the information from another agency, and that agency refused further disclosure.[382]

FINTRAC treats all information received from other Canadian agencies as caveated, and does not further disclose this information without the express written consent of the originating agency. 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.[383] The Minister of Finance must approve all such agreements.[384]

12.
CANADA REVENUE AGENCY

12.1
RELEVANT LEGISLATION

- *Charities Registration (Security Information) Act*, S.C. 2001, c. 41, s. 113 (*CRSIA*)
- *Income Tax Act*, R.S.C. 1985, c. 1 (5th Supp.)

12.2
NATIONAL SECURITY MANDATE

The Canada Revenue Agency's (CRA) national security mandate relates to the registration of charities. The *Charities Registration (Security Information) Act*[385] (*CRSIA*) was part of the 2001 *Anti-terrorism Act*. Under the *CRSIA*, an organization can lose or be denied charitable status if both the Minister of National Revenue and the Minister of Public Safety sign a certificate asserting that there are reasonable grounds to believe that the organization has made, is making or will make any resources directly or indirectly available to a terrorist group.[386]

The *CRSIA* process is similar to that used in security certificate cases under the *Immigration and Refugee Protection Act*, although to date no certificates have been issued under the *CRSIA*.[387] After a certificate has been signed and issued by the two ministers, a Federal Court judge reviews its reasonableness.[388] In making this determination, the judge may review and rely upon information that the judge determines must be kept secret from the charity because its disclosure would harm national security or endanger the safety of any person.[389] The judge must give the charity a summary of the information that reasonably informs the charity of the circumstances giving rise to the certificate, but that does not include any information that in the judge's opinion, would harm national security if disclosed.[390] If the certificate is found to be reasonable, the

organization is denied registration as a charity or stripped of charitable status for seven years.[391] The judge's decision may not be appealed.[392]

The Review and Analysis Section within the Charities Directorate analyzes data, including intelligence assessments, briefs and classified information provided by the RCMP and CSIS, and publicly available information, to identify charities that may be involved with or lend support to terrorist organizations.[393] At present, the CRA does not receive information from foreign counterpart agencies responsible for charities and tax regulatory officials, although it hopes to be able to conclude such arrangements in the future. After completing its analysis, the CRA will make a recommendation to the Minister of National Revenue regarding the issuance of a certificate. In a parallel process, staff at CSIS or the RCMP will do the same for the Minister of Public Safety.

If a registered charity or an organization applying for registration is included on either of the UN terrorist entity lists (the UNSTR and UNAR lists) or on the *Criminal Code* terrorist entity list, the CRA evaluates the organization and begins action under either the *CRSIA* or the *Income Tax Act*.

12.3 INFORMATION SHARING

The CRA is a collector of intelligence to the extent that it collects taxpayer information, some of which may be useful in anti-terrorism investigations.[394] Under the new *CRSIA*, information sharing between the CRA and other government agencies — including the RCMP, CSIS and PSEPC — has also increased.[395] To administer or enforce *CRSIA*, the CRA may disclose information on registered charities to any official employed by the federal government, including RCMP members.[396] Information relevant to issuing a *CRSIA* certificate is also shared with PSEPC. To date, the CRA has provided information to the RCMP's Anti-Terrorist Financing Group in relation to the certificate process on a very few occasions. However, other government agencies, including the RCMP and CSIS, would not be able to use most of this information for their own national security investigations because of the confidentiality provisions in the *Income Tax Act*.[397]

Under current legislation, information about registered charities and other taxpayers can be disclosed outside of the CRA only in limited circumstances. In addition to disclosure for the purposes of *CRSIA*, information may be disclosed after criminal charges have been laid under a federal law[398] or under the authority of a judge's order.[399] On an *ex parte* application by the Attorney General, such an order can be made to further an investigation into a terrorism offence in the *Criminal Code*,[400] and CSIS may also access taxpayer information with a

warrant issued under the *CSIS Act*.[401] Certain information relating to registered charities is also publicly available, and therefore may be disclosed by CRA to personnel from the RCMP, CSIS and other agencies with national security responsibilities.[402] Where legal proceedings have been started under federal or provincial laws relating to the imposition of taxes or duties, the CRA may disclose taxpayer information.[403] Therefore, the CBSA can also access some CRA information while enforcing customs and excise legislation. The CRA may also disclose taxpayer information to appropriate persons where it relates to imminent danger of death or physical injury to any individual.[404] The CRA states that the threshold for exchanging information under this provision is very high and that such disclosures are rare and limited.

A recent government consultation paper suggested amending the *Income Tax Act* and the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, to allow the CRA to disclose files on charities and other taxpayers suspected of involvement with terrorist financing, to among other agencies, FINTRAC, CSIS and the RCMP. Disclosures would be allowed for specific financial tracking, intelligence and national security purposes. FINTRAC would also be allowed to share information with CRA when it had reasonable grounds to suspect that a registered charity was being used to fund terrorism. I am advised that the Department of Finance is currently considering making these legislative amendments.

13.
FOREIGN AFFAIRS AND INTERNATIONAL TRADE CANADA

13.1
RELEVANT LEGISLATION

- *Department of Foreign Affairs and International Trade Act, R.S.C. 1985, c. E-22*
- Order in Council, P.C. 2006-0040, February 6, 2006
- *United Nations Act*, R.S.C. 1985, c. U-2
- *United Nations Suppression of Terrorism Regulations*, S.O.R./2001-360 (UNSTR)

13.2
MANDATE

Foreign Affairs and International Trade Canada (DFAIT) is responsible for the conduct of Canada's international relations.[405] The department manages

Canadian embassies, high commissions and consulates abroad, which provide diplomatic and consular assistance to Canadians in foreign countries. DFAIT is the lead Canadian agency in international treaty negotiations, including the various international treaties on terrorism.[406] The department has many areas of responsibility, including a dedicated International Crime and Terrorism Division.[407] This division has primary responsibility for Canada's participation in and coordination with the anti-terrorism efforts of international organizations such as the United Nations and the North Atlantic Treaty Organization,[408] and plays a role in listing terrorist entities under its purview.

The Department of Foreign Affairs and International Trade has over 9,600 employees, including 1,900 members of the Foreign Service, over 3,000 other staff within Canada and 4,600 locally engaged employees working for Canadian missions abroad.

13.3
NATIONAL SECURITY ACTIVITIES

The Department of Foreign Affairs and International Trade has broad responsibility for Canadian diplomatic initiatives related to combating terrorism in the international arena. As I discussed in my report on the Factual Inquiry, Canadian missions and diplomats play an important role when Canadian citizens are imprisoned or accused of terrorist activity abroad. Another facet of DFAIT's diplomatic role is to obtain assurances from foreign governments that an individual will be treated in accordance with international standards (e.g., not be tortured) if deported to his or her home country. Such assurances are arranged on a case-by-case basis and, generally, through an exchange of diplomatic notes.[409]

Through its Legal Bureau and its International Crime and Terrorism Division, DFAIT plays the lead role in the listing of terrorist entities under the *United Nations Suppression of Terrorism Regulations*[410] (UNSTR) and the *United Nations Afghanistan Regulations* (UNAR).[411] Like the *Criminal Code* list, the UNSTR and the UNAR lists include the names of individuals as well as groups or organizations.[412] The UNAR and the UNSTR are distinct listing processes. The UNAR applies by reference to all individuals and entities designated by the Security Council Committee established under Security Council Resolution 1267 (the 1267 Committee), that is, to members of the Taliban, and to Osama Bin Laden and his associates. The UNSTR applies to two groups: first, the individuals and entities on the 1267 Committee list; and second, individuals and entities listed by the Governor in Council in Schedule 1 to the regulations.

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.[413] The 1267 Committee's listings have force and effect in Canada by virtue of their incorporation by reference into the UNAR and into Schedule 1 of the UNSTR.[414]

The United Nations has not established standards governing when the 1267 Committee may list a person or entity, and different countries use different standards when requesting listings.[415] For example, in November 2001, at the request of the United States the United Nations listed a Canadian citizen based on that person's connections to an international money transfer network suspected of dealings with al-Qaeda, and despite the fact that there was no evidence linking him, as an individual, to terrorist financing.[416] DFAIT is currently creating a process to review the listing of new individuals and entities by the 1267 Committee.

A country may make diplomatic representations to the UN Security Council, in accordance with the 1267 Committee's guidelines, asking that an individual be removed from the UN lists. The Canadian government made such representations to have the above-mentioned Canadian citizen removed from the UN list because there was no reasonable basis for believing that the individual was connected personally to terrorist activities. That individual was delisted after nearly nine months, during which time his personal and business assets remained frozen.[417]

The second group listed under the UNSTR are individuals and entities that DFAIT recommends for listing. The regulations allow DFAIT to list additional individuals where there are reasonable grounds to believe that a listed person is involved in terrorist activity.[418] The DFAIT process usually begins when DFAIT is notified that another country intends to list an entity. DFAIT then calls a meeting with other departments and agencies to discuss the proposed listing, and provides its recommendations to the Governor in Council.[419]

A person listed by DFAIT under the UNSTR may apply to the Minister of Public Safety to be removed from the list.[420] The individual is delisted if the Governor in Council accepts the Minister's recommendation that there are reasonable grounds for the individual's removal.[421]

13.3.1 DFAIT Intelligence

DFAIT's Foreign Intelligence Division (ISI) provides intelligence to protect Canadian citizens and government facilities abroad, and to support operational and policy decision making. It also manages the expulsion of Canadian

diplomats from foreign countries for security reasons and handles terrorist incidents abroad that involve Canadian citizens.[422]

ISI is responsible for liaison with DFAIT's principal intelligence partners, CSIS, the CSE, DND, the RCMP and PCO, and occasionally with other members of the Canadian intelligence community, including the CBSA, CIC and Transport Canada. ISI also liaises with foreign intelligence agencies. In addition, ISI oversees the collection, analysis and dissemination of foreign intelligence within DFAIT. DFAIT maintains full-time, dedicated intelligence officials at the Canadian missions in London, England; Washington, D.C., USA; and Canberra, Australia, as well as other locations.[423]

ISI prepares current intelligence assessments and interview reports based on interviews with individuals who have travelled to countries of intelligence interest to DFAIT and who have information about those countries that is not in the public domain. Current intelligence assessments focus on events of high foreign policy interest and tend to relate to a single issue — Iran's efforts to develop nuclear weapons is an example. In contrast, intelligence assessments by the International Assessment Staff at the Privy Council Office look at broader and longer-term issues — prospects for the remainder of Russian President Vladimir Putin's term, for example; while ITAC reporting focuses on threats to Canada's security, such as assessments of the development of Sunni Muslim extremism. DFAIT also considers itself a major consumer of foreign intelligence. The department advises me that over 400 clients at its Ottawa headquarters, along with staff at 60 missions abroad, receive substantial amounts of foreign intelligence on a daily basis.

DFAIT is also responsible for the security of the department's personnel, physical assets and information systems in Canada and around the world.

13.3.2
RCMP Foreign Liaison Officers and Secondees to DFAIT

The RCMP and DFAIT are parties to a memorandum of understanding reached in 1988.[424] The MOU deals primarily with the relationship between the RCMP and DFAIT. One of the main objects of this MOU is to set out the role of RCMP Foreign Liaison officers posted abroad. These liaison officers maintain relationships with foreign criminal police agencies and related institutions to provide support and assistance to Canadian law enforcement agencies in the prevention and detection of offences under Canadian federal laws. In the national security context, information and intelligence exchanged with a foreign police agency flows through the liaison officer responsible for the area in which the foreign agency is located. This exchange is generally accomplished without

coordination with CSIS. I am informed that if the information is relevant to CSIS' mandate, the RCMP seeks the foreign police agency's permission before sharing it with CSIS. The liaison officer is responsible for ensuring that foreign partners understand the difference in the roles of CSIS and the RCMP, and must report information and intelligence about national security matters to Headquarters.

The MOU provides that the RCMP and DFAIT are to mutually agree upon the creation of liaison officer positions. It also gives DFAIT the right to comment on the liaison officer's performance appraisal. There are a total of 40 liaison officers in 25 locations: Berlin, London, Madrid, Moscow, Paris, Rome, The Hague, Vienna, Bogotá, Caracas, Kingston, Mexico City, Miami, Washington, D.C., Hong Kong, Islamabad, Kuala Lumpur, New Delhi, Beijing, Bangkok, Amman, Brasilia, Rabat, Pretoria and Dubai.

The RCMP/DFAIT MOU also provides for meetings between senior members of each institution. Further, it requires the RCMP to inform DFAIT of proposed RCMP visits abroad for operational purposes, except visits to the United States, unless the meeting might have a bearing on Canada's relations with the United States.

The RCMP also seconds a member to DFAIT. One role of the RCMP secondee is to facilitate the exchange of information between the two organizations. Such information exchanges come within four categories:

1. Investigative, including updates by the RCMP on ongoing criminal investigations that may have foreign policy implications and provision of information relevant to the RCMP by DFAIT.
2. Protective, including exchange of information regarding the environment abroad to ensure the security of official visitors to Canada and to develop security profiles for foreign missions.
3. Consular, including advice during crisis incidents such as hostage takings involving Canadians abroad.
4. General, including information on the smuggling of weapons and nuclear materials.

On occasion, each organization also provides technical security advice and assistance to the other.

14.
PRIVY COUNCIL OFFICE

14.1
MANDATE

The Privy Council Office (PCO) provides non-partisan advice and support for the Prime Minister, departments within the Prime Minister's portfolio, the federal Cabinet and Cabinet committees.[425] As the head of government in Canada, the Prime Minister has ultimate responsibility for national security. The Prime Minister is supported by the National Security Advisor to the Prime Minister, and by the Security and Intelligence Secretariat and the International Assessment Staff, which are all part of the Privy Council Office. In addition to participating in the Interdepartmental Threat Assessment Working Group, PCO Security Operations chairs the Departmental Security Officers' Readiness Committee. As well, PCO and Treasury Board Secretariat co-chair the recently formed Strategic Steering Committee on Security.

PCO's stated role in the determination of intelligence priorities is to promote effective coordination among involved departments and agencies and enable them to jointly present their proposed strategic priorities to ministers.

14.2
NATIONAL SECURITY ADVISOR

The National Security Advisor is the Prime Minister's principal advisor on matters of national security, and provides advice and support for Cabinet discussions on national security matters. The National Security Advisor coordinates activity among members of the Canadian security and intelligence community, and promotes a coordinated and integrated approach to intelligence and threat assessment. The National Security Advisor also maintains relationships with allied governments by acting as a senior Canadian representative on national security issues, visiting allied countries, hosting international visitors in Canada and participating in other exchanges. The National Security Advisor helps to develop national security policy and identify measures to address national security vulnerabilities. At its discretion, the RCMP may brief the National Security Advisor on particular RCMP investigations of terrorism offences. Such a briefing would aim to keep the National Security Advisor generally aware of any significant national security development in the country and enable him or her to brief the Prime Minister, where appropriate. The National Security Advisor does not provide guidance or instructions to the RCMP.

The National Security Advisor is also the Deputy Minister for the Communications Security Establishment, and accountable for the CSE's policy and operations. In addition, the Advisor is accountable for the Integrated Threat Assessment Centre, although the Director of CSIS has administrative responsibility for ITAC. PCO has one person seconded to ITAC.

The National Security Advisor is supported by two PCO secretariats — the Security and Intelligence Secretariat and the International Assessment Staff — which are discussed below.

14.3
SECURITY AND INTELLIGENCE SECRETARIAT

The Security and Intelligence Secretariat (S&I Secretariat) advises Cabinet and the Prime Minister on the management of national security and intelligence issues and activities, and on the coordination of government responses to emergencies. The S&I Secretariat works with federal departments and agencies to coordinate important security measures. In addition, the Secretariat advises and supports ministers on specific national security and intelligence issues. In a national security emergency situation, the S&I Secretariat would be alerted by the Government Operations Centre,[426] the RCMP or CSIS, and would provide direction and guidance to departments and agencies on behalf of the National Security Advisor.

In conjunction with other federal departments and PCO secretariats, the S&I Secretariat works on issues related to managing the Canada-U.S. border. The Secretariat coordinates and monitors the implementation of the security component of the Security and Prosperity Partnership of North America, which includes the exchange of terrorist watch list data and information on high-risk travellers or cargo; the development of compatible mechanisms for screening travellers; compatible export control, visa and lookout policies; joint inspections of certain maritime vessels; the development of interoperable communications systems; and joint planning for critical cross-border infrastructure protection.[427] Other departments and agencies involved in managing the Canada-U.S. border include the CBSA, CIC, the Canadian Coast Guard/DFO, DFAIT, the Public Health Agency of Canada, NRCAN, CSIS, the RCMP, PSEPC and Transport Canada.

In addition, the S&I Secretariat:

- works closely with the RCMP, CSIS and other agencies to coordinate security arrangements for the Prime Minister, the Governor General and Cabinet, and to conduct preappointment background checks for persons appointed to public office;

- administers the security program for PCO and the Prime Minister's Office;
- advises departments and agencies on internal security issues; and
- works with the RCMP, Public Works and Government Services Canada, the National Capital Commission, the Senate and the House of Commons on issues concerning security of the Parliamentary Precinct.

The S&I Secretariat works with the RCMP at three levels: first, on policy issues, largely through discussions in interdepartmental committees and bilateral meetings; second, on individual files involving criminal activity related to Canada's security and on emergencies; and third, on the protection of the Prime Minister, Cabinet or Parliament, and RCMP background checks. For the purposes of advising ministers and coordinating government-wide measures, PCO may receive information about ongoing RCMP investigations where these investigations involve criminal activity that relates directly to Canada's security. PCO's access to RCMP information is on a limited and need-to-know basis, although discussions of national security matters and emergencies could involve the sharing of personal information.

14.4
INTERNATIONAL ASSESSMENT STAFF

The International Assessment Staff (IAS) produces current and strategic assessments of developments and trends in foreign countries that could affect Canadian foreign policy, security or economic interests. Analysts draw from all sources of information — open-source to classified. Through ITAC, the IAS receives terrorism analysis reports from ITAC's partners in the U.K., the U.S., Australia and New Zealand. In addition, the IAS receives intelligence assessments directly from key partners (the U.S., the U.K., Australia, New Zealand, Spain, Germany, Belgium and Singapore). Intelligence other than assessments comes via CSIS and the CSE. Much of this material is available to ITAC via partner agencies, but what the IAS receives from foreign partners is also posted on a secure network to which ITAC has direct access. IAS provides its assessments for the Prime Minister, other senior ministers and senior decision makers in government agencies, including Agriculture and Agri-Food Canada, the Bank of Canada, the CBSA, CFIA, CIC, CIDA, the CSE, CSIS, Environment Canada, EDC, Health Canada, Industry Canada, the Canadian Commercial Corporation, Justice Canada, Natural Resources Canada, PCO, PSEPC, the RCMP, SIRC, Transport Canada, Infrastructure and Communities, DND, DFAIT, Human Resources and Social Development, the National Energy Board, Finance Canada (occasionally) and Treasury Board Secretariat (infrequently).

Other agencies can receive IAS products if their employees have the required clearance, and if the agencies have the facilities and equipment to hold, file or destroy IAS material; the means to receive the material; and a reason to need access to the reports. Assessments focus on strategic and geo-political questions, and contain very little personal information on Canadians. However, the IAS does study foreign leaders and prominent terrorists in their capacity as political actors. Unlike ITAC, the IAS does not track terrorists, but an IAS assessment could include a discussion of the impact of a prominent foreign terrorist. PCO's secondee to ITAC is a member of the IAS.

The IAS also plays a key role in maintaining relationships with allied intelligence assessment organizations and has a mandate to liaise with Canadian academia.

The intelligence assessments that the IAS receives from foreign partners are usually strategic in focus and rarely contain personal information. Although the IAS receives information directly from the intelligence assessment services of some closely allied governments, it obtains most intelligence information through CSIS and the CSE. ITAC receives terrorist threat warnings and related assessments from allied partner agencies and forwards these to others in the Canadian community, including the IAS.

The IAS does have access to some RCMP information, particularly on criminal issues of national and global significance, but there is little interaction on matters related to terrorism. Although the IAS receives RCMP security information that is circulated to those with the appropriate security classification and a need for the information within the government, there is no regular flow of information between the two organizations. Information vital to an ongoing RCMP operation would not be shared with the IAS.

15.
PUBLIC SAFETY AND EMERGENCY PREPAREDNESS CANADA

15.1
RELEVANT LEGISLATION

- *Canada Border Services Agency Act*, S.C. 2005, c. 38 (*CBSA Act*)
- *Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C-23 (*CSIS Act*)
- *Department of Public Safety and Emergency Preparedness Act*, S.C. 2005, c. 10 (*PSEP Act*)
- *Emergency Preparedness Act*, R.S.C. 1985, c. 6

- *Immigration and Refugee Protection Act*, S.C. 2001, c. 27 (*IRPA*)
- *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, S.C. 2000, c. 17 (*PCMLTFA*)
- *RCMP Act*, R.S.C. 1985, c. R-10
- *Security Offences Act*, R.S.C. 1985, c. S-7

15.2
MANDATE

Public Safety and Emergency Preparedness Canada (PSEPC) was created in 2005.[428] However, in December 2003 responsibility for certain agencies and portions of the public service were transferred to the Minister of Public Safety and Emergency Preparedness, who legally continued to be known as the Solicitor General of Canada.[429] As of February 6, 2006, the Minister of Public Safety and Emergency Preparedness adopted the new title of Minister of Public Safety.[430] The Minister of Public Safety replaces the Solicitor General and, subject to other statutes, has authority over all matters relating to public safety and emergency preparedness not specifically assigned to another federal department or agency.

As the lead department on public safety, PSEPC has a lead role in national security policy development.[431] To fulfill this mandate, the Minister may co-operate with foreign states.[432] The Minister may also facilitate the sharing of information, where authorized, to promote public safety objectives.[433] The Minister of Public Safety is responsible for the PSEPC portfolio agencies, which include the RCMP, CSIS, the CBSA and the Correctional Service of Canada,[434] as well as the Commission for Public Complaints Against the RCMP, the Office of the Correctional Investigator and the RCMP External Review Committee.[435] The PSEPC portfolio has over 52,000 employees.[436]

PSEPC is divided into five branches, of which the following three are relevant to national security:

- the Emergency Management and National Security Branch, which is responsible for national security policy; emergency analysis, warning and response, including the Government Operations Centre (GOC) and the Canadian Cyber Incident Response Centre; emergency management policy; and emergency preparedness and recovery, including the Canadian Emergency Management College;
- the Policing, Law Enforcement and Interoperability Branch, which is responsible for policing policy and "law enforcement and border strategies," and for facilitating information sharing and the interoperability of databases and computer systems for security and public safety purposes; and

- the Community Safety and Partnerships Branch, which is responsible for crime prevention and corrections.

15.3
NATIONAL SECURITY ACTIVITIES

PSEPC has a lead role in national security policy development,[437] while PCO provides leadership and acts as the Government's central coordinating body. For example, from a national security perspective, PCO is the lead department on the Security and Prosperity Partnership, which involves several departments and agencies.

PSEPC provides independent advice and support to the Minister of Public Safety on matters specifically related to the Minister's mandate of public safety, national security and emergency management. To do this, PSEPC analysts consult with PSEPC portfolio agencies, other federal departments and agencies, provincial and territorial governments, and the international community. The PSEPC portfolio includes two of Canada's primary collectors of national security information — the RCMP and CSIS — as well as the CBSA.

From a policy perspective, PSEPC provides advice and support to the Minister relating to the direction, control and accountability of CSIS and the national security activities of the RCMP and the CBSA. The department is also involved in developing and reviewing ministerial directives on national security, and is responsible for developing legislation that affects PSEPC portfolio agencies. In addition, PSEPC has created the Cross-Cultural Roundtable on National Security, which is intended to facilitate dialogue between the Canadian government and different cultural communities within Canada.[438]

The Minister of Public Safety and PSEPC portfolio agencies are involved in the issuance of certificates under the *Charities Registration (Security Information) Act*,[439] and the security certificate procedure under the *Immigration and Refugee Protection Act*.[440] Security certificates allow the government to detain (with a view to deporting) non-citizens who are inadmissible to Canada on grounds of security, violating human or international rights, serious criminality or organized criminality.[441]

PSEPC also takes the lead role in the terrorist entity listing process under the *Criminal Code*.[442] Under this listing process, the Minister of Public Safety may recommend to the Governor in Council that certain entities be listed as terrorist entities.[443] The *Criminal Code* sets out a procedure for a listed entity to apply to the Minister to be delisted,[444] and provides for judicial review of the Minister's decision.[445] The Minister must also review the list every two years.[446]

As I discussed in Chapter III, being a listed entity is not a crime in itself. However, listing entails several legal consequences. For example, a listed entity falls within the definition of "terrorist group" in the *Criminal Code*; may have its Canadian assets seized or forfeited;[447] and may not access or dispose of property held by a Canadian institution, such as a bank or brokerage house.[448] A listing supports the application of other provisions in the *Anti-terrorism Act*, including terrorism offences; crimes relating to the financing of terrorism; and requirements to freeze terrorist property, and procedures for the courts to order seizure and forfeiture of that property.[449]

The listing process under the *Criminal Code* is one of three terrorist entity listing processes in Canada. The Department of Foreign Affairs and International Trade is responsible for listing entities under the *United Nations Suppression of Terrorism Regulations*[450] and the *United Nations Afghanistan Regulations*.[451] The *Criminal Code*, UNSTR and UNAR lists are not identical, nor are the consequences of listing.[452] The *Criminal Code* list serves to support criminal prosecutions for terrorism offences in Canada and to freeze or forfeit terrorist assets. The UNSTR and UNAR lists, on the other hand, aim only to halt the flow of terrorist financing. An individual or entity listed as a terrorist by the United Nations may have assets seized or frozen in Canada, and worldwide, in accordance with the legislative scheme for freezing terrorist assets in other countries. I have discussed the UNSTR and UNAR processes in the section of this chapter on DFAIT.

15.4
INTELLIGENCE AND INFORMATION SHARING

PSEPC receives information relating to public safety or emergency preparedness, including national security information, and determines the appropriate response. The department receives classified national security intelligence information from its own portfolio agencies, from other government agencies and through the Integrated Threat Assessment Centre. PSEPC receives information on "national security matters" (within the meaning of the National Security Policy) from the following federal organizations, excluding its portfolio agencies: PCO, DND, the CSE, DFAIT, Transport Canada, Environment Canada, CIC, the CRA, the Canadian Food Inspection Agency, the Public Health Agency of Canada and Health Canada, and the Canadian Nuclear Safety Commission. Information from ITAC comes to PSEPC principally as intelligence threat assessments. PSEPC also has two analysts seconded to ITAC. Occasionally, CSIS, ITAC or RCMP intelligence products may refer to individuals. PSEPC does not normally have access to the operational details of RCMP national security investigations, nor to RCMP databanks. Similarly, it does not have direct access to CSIS databases.

PSEPC shares threat information with provincial and territorial governments and agencies in the context of the Government's National Security Policy. The information transmitted usually does not include personal information. In rare circumstances, at the request of the originating agency, personal information may be shared with specified organizations on a need-to-know basis and in relation to an emerging or occurring event that directly affects the safety of Canadians. General threat information may be shared with the private sector as part of PSEPC's critical infrastructure protection role. The Canadian Cyber Incident Response Centre, which monitors cyberthreats, may also disseminate information to the private sector. When appropriate, sensitive cyber information is shared with the private sector under a non-disclosure agreement.

PSEPC shares classified information with provincial entities that have a need to know and the appropriate security clearance. The department has developed a pilot project to share secret-level classified information within the federal government via an e-mail system, and has a secure communications link with the United States Department of Homeland Security (DHS).[453] The Government Operations Centre shares its own information with the DHS directly, but does not share information from PSEPC portfolio agencies or ITAC with the DHS. PSEPC states that the GOC has not shared personal information about Canadians with the DHS.

The GOC provides strategic-level coordination and direction on behalf of the federal government, in response to actual or potential emergency situations affecting the national interest. Its mandate encompasses a broad range of threats to Canada, from terrorism to natural disasters to serious diseases. The Centre receives classified and unclassified information from federal, provincial, territorial and international partners, including assessed intelligence products and information useful for coordinating and supporting responses to an emergency. It reviews, analyzes and disseminates this information to appropriate response organizations, including provincial and territorial entities and the private sector on a need-to-know basis. The GOC does not have databases to keep or store personal information.

16.
OTHER FEDERAL DEPARTMENTS AND AGENCIES INVOLVED IN NATIONAL SECURITY OPERATIONS

In addition to those that I have described above, a number of other federal departments and agencies play a role in Canada's national security and intelligence community. For example, many of the departments listed below are "virtual partners" in ITAC — they receive ITAC reports and exchange information with

ITAC, but do not have a physical representative at the Centre. The following gives a brief description of the national security activities of these departments.

16.1 HEALTH CANADA AND THE PUBLIC HEALTH AGENCY OF CANADA

Health Canada and the Public Health Agency of Canada (PHAC) analyze health threats to Canada. The Public Health Agency of Canada was created in September 2004 and is part of the federal government's National Security Policy.[454] Health Canada studies subjects like infectious diseases and chemical, biological and radio-nuclear attacks, in relation to their health consequences for Canadians and the repercussions for Canadian social and economic stability.[455] Health Canada and the Public Health Agency of Canada contribute technical expertise on public health issues and input on the health impact for national security threat and risk assessments.

The Centre for Emergency Preparedness and Response (CEPR) is Canada's central coordinating point for public health security issues. Among its many responsibilities, CEPR:

- develops and maintains national emergency response plans for the Public Health Agency of Canada and Health Canada;
- is the health authority in the Government of Canada on bioterrorism, emergency health services and emergency response;
- assesses public health risks during emergencies;
- monitors outbreaks and global disease events;
- manages the Global Public Health Information Network, a secure, Internet-based early warning system that monitors health emergencies, including bio-terrorism and exposure to radio-nuclear threats, around the world.[456]
- contributes to developing Canada's health and emergency policies to ensure they are in line with threats to public health security and general security, in collaboration with other federal and international health and security agencies; and
- administers federal public health rules governing laboratory safety and security, quarantine and similar issues.[457]

Following 9/11, the CEPR created the position of Special Advisor/Medical Threat Intelligence. Since then, Health Canada and the Public Health Agency have established contacts with intelligence colleagues in PCO, CSIS, the CSE and the RCMP. Health Canada and the Public Health Agency provide a medical and public health context to intelligence information when appropriate to PCO and other security and intelligence agencies, and receive relevant intelligence

information, including classified information. Health Canada/PHAC may also receive Passenger Name Record information from the CBSA for travellers arriving in Canada who pose serious public health risks. Finally, Health Canada and the Public Health Agency of Canada are virtual partners in ITAC, and are represented at the RCMP National Operations Centre (NOC) at RCMP Headquarters when the NOC is activated.

16.2
CANADIAN FOOD INSPECTION AGENCY

The Canadian Food Inspection Agency administers all federal laws relating to food inspection, plant protection and animal health programs.

The Agency establishes import policies and standards for plants, animals and food, which the CBSA enforces at points of entry to Canada. It provides advice and support, including veterinary support, to the CBSA in relation to the import of high-risk animals, plants or food. The Agency maintains an emergency response plan and provides support to the provinces in preparing for and responding to emergencies involving food safety, animal or plant protection, or any of its other programs. It is also a partner in *The Chemical, Biological, Radiological and Nuclear Strategy of the Government of Canada*,[458] and participates in research initiatives aimed at detecting and treating biological threats to food, plants and animals. The Agency is currently working to improve laboratory ability to handle potential biohazard emergencies.

The Agency has established the Information Gathering and Analysis Team, an intelligence-gathering unit that collects and analyzes information related to the Agency's mandate. Along with the RCMP, this team is a member of the Canadian delegation to the Science and Technology Intelligence Group. It has access to classified and public information from various sources, including interdepartmental working groups, and information sharing arrangements. The RCMP and the Food Inspection Agency co-operate and share information related to protecting the food industry. The Agency also has the capacity to use the geographic information system (GIS) to locate all Canadian farms, feedlots, food and animal industry and infrastructure in an emergency response scenario. The Agency is a virtual partner in the Integrated Threat Assessment Centre.

16.3
ENVIRONMENT CANADA

The Enforcement Branch of Environment Canada consists of both an Environmental and a Wildlife Enforcement directorate. The Branch is a federal law enforcement body that enforces Canadian environmental legislation. It

provides information, intelligence and expertise to support various national security initiatives, including transportation and border security. These initiatives principally relate to emergency response to incidents, control of the transboundary movements of hazardous waste, toxic and new substances that may pose a threat to the health of Canadians or the environment. The RCMP helps Environment Canada to enforce the *Canadian Environmental Protection Act, 1999*, and shares information regarding the management of toxic substances and the enforcement of pollution prevention laws with the National Office of Pollution Prevention.[459]

Environment Canada also runs intelligence programs, which are linked to the department's law enforcement mandate. These programs gather and analyze information in relation to chemical manufacturing and associated industries, trade in endangered animals, plants and animal parts, and the transboundary movement of hazardous waste. The intelligence programs provide information to managers and enforcement personnel within Environment Canada, and share information with external law enforcement agencies, including the RCMP, the CBSA, the Canadian Food Inspection Agency and provincial ministries of environment, for the purposes of enforcing environmental legislation. The programs also produce tactical, operational and strategic intelligence products on:

- the location, quantities and transboundary movements of toxic and hazardous substances that must be reported to the department;
- the introduction and manufacture of new substances into Canada, including biotechnology, genetically modified organisms and chemicals;
- criminal activity, including activity of organized crime and criminal organizations that violate environmental laws; and
- the importation of invasive, exotic or harmful species, and potential associated diseases such as avian influenza.

The department has just over 20 intelligence officers, who perform both information collection and analysis functions. The intelligence programs collect information from several sources, including the Internet, departmental databases, media, universities, informants, surveillance and covert operations. Enforcement officers, or Intelligence officers designated as Enforcement officers, collect information and have powers similar to those of police officers to enforce various environmental laws. Most intelligence products and information are internal documents used for law enforcement purposes. Within the context of national security, the intelligence programs may obtain information during their activities that is relevant to another agency's mandate, and Environment Canada may

share this information. Information that might be shared would include information regarding the toxicity of certain chemicals or substances, the potential for harm of certain hazardous wastes, and the locations of these substances or wastes. Environment Canada advises me that information about companies or individuals engaged in these activities would be shared only where there are clear indicators of a potential risk to national security. To date, the only information relating to national security that Environment Canada has shared with other government departments and agencies is technical information about chemical and toxic substances. The department is hoping to substantially increase its intelligence programs.

In addition to its enforcement mandate, Environment Canada supports public safety planning, situational awareness and enforcement response within the federal government, by supporting emergency preparedness, planning and response activities through the Environmental Emergencies Directorate and the Meteorological Service. The department is also involved in the Interdepartmental Marine Security Working Group, and is a virtual member of the Integrated Threat Assessment Centre.

16.4
NATURAL RESOURCES CANADA

Natural Resources Canada has a mandate to protect critical energy infrastructure under federal jurisdiction in Canada, including energy facilities in Canada and facilities that cross the Canada-U.S. border. Natural Resources Canada protects infrastructure such as energy transmission lines and oil and gas pipelines. The department is also responsible for explosives licensing and compliance under the *Explosives Act*[460] and the *Explosives Regulations*,[461] and for a substantial part of the government's explosives security research and various government mapping and charting projects.[462]

Agencies within the Natural Resources portfolio, reporting to the Minister of Natural Resources, include the National Energy Board, the Canadian Nuclear Safety Commission and Atomic Energy Canada Limited. These organizations operate with a high degree of autonomy, including in their interactions with elements of the Canadian security and intelligence community.

The department interacts with the RCMP in relation to the protection of Canada's critical energy infrastructure. This includes protection of oil and natural gas pipelines, hydro generation and electrical transmission infrastructure systems, offshore oil and gas exploration, and the development and production of infrastructure systems. To this end, the RCMP and Natural Resources Canada share information and intelligence. Under the *Explosives Act* and the *Explosives*

Regulations, RCMP members are deputy inspectors of explosives. Natural Resources Canada may request RCMP assistance in conducting compliance inspections and investigations in cases of non-compliance with the legal scheme, or where there has been a theft or loss of explosives. The department provides the RCMP with information on explosives licence holders and is working closely with the Force to develop a security check capacity for individuals wishing to acquire and possess explosives. Natural Resources Canada manages the Canadian Section of the International Boundary Commission. In this capacity, the department interacts with the CBSA and jointly monitors unauthorized constructions or activities within 3.05 metres (10 feet) of the border with the United States.

The RCMP and Natural Resources Canada also interact in the context of the Chemical, Biological, Radiological and Nuclear Research and Technology Initiative.[463] Natural Resources Radiation Geophysics Section conducts high-sensitivity aerial mapping of naturally occurring and man-made radioactivity. Although information sharing between the RCMP and Natural Resources would be low under normal, non-threat conditions, Natural Resources could be expected to communicate unusually high levels of radioactivity to the RCMP units that are first-responders to environmental threats.

Natural Resources Canada also interacts from time to time with law enforcement and security intelligence agencies to access or share information relevant to the department's mandate. The department shares information with the RCMP and CSIS, and ITAC may consult it with respect to subject matter within its expertise, or during the preparation of an ITAC threat assessment.

In the context of its critical infrastructure protection role, Natural Resources Canada advises PSEPC and the CBSA. It also works closely with government departments and agencies in the United States and Mexico, sharing information on policy and operational issues.

16.5
CANADIAN NUCLEAR SAFETY COMMISSION

The Canadian Nuclear Safety Commission is both an administrative tribunal and a regulatory agency. It regulates and controls the use of nuclear energy and materials in Canada. The Commission also licenses and inspects the Canadian nuclear industry, which includes large nuclear power plants, uranium mines, nuclear exporters, and industrial and academic users of radioisotopes. The Commission sets physical protection standards at major nuclear facilities. For example, it issued an Emergency Order in October 2001 requiring all such facilities to establish an onsite, armed response force.[464] The Commission shares

information with the RCMP or CSIS about irregularities in any of the activities that it oversees. ITAC may also consult the Commission when preparing a threat assessment.

The Commission also provides technical assistance to develop and implement emergency response plans for a possible radiological attack on Canada.[465] The RCMP's Public Security and Anti-Terrorism/Chemical, Biological, Radiological, Nuclear Training unit and the Commission have participated in joint training exercises.

16.6
DEPARTMENT OF JUSTICE

The Department of Justice (DOJ) provides legal advice on matters relating to national security. The National Security Group of the Federal Prosecution Service in Ottawa is the focal point for the practice of national security law and advice relating to section 38 of the *Canada Evidence Act*, which I have described in detail in Chapter III. Federal prosecutors in Department of Justice regional offices generally conduct criminal prosecutions of designated terrorist offences in the *Criminal Code*.[466] The Criminal Law Policy Section and the Human Rights Law Section are also involved in national security and anti-terrorism work.[467] In addition, the Attorney General of Canada has jurisdiction to prosecute crimes under the *Security of Information Act*,[468] the *Access to Information Act*[469] and the *Privacy Act*.[470] The Attorney General's consent is needed to begin any prosecution under the *Security of Information Act*.[471]

Most government department and agencies, including the RCMP, CSIS and the CSE, have their own legal department (called a legal services unit), made up of DOJ lawyers. The Department of Justice also maintains a Citizenship, Immigration and Public Safety portfolio, which groups together the Legal Services units (LSUs) of the PSEPC, the RCMP, CSIS, the CBSA, CIC, the Correctional Service of Canada, the Canada Firearms Centre, the National Parole Board and the War Crimes and Crimes Against Humanity Program. The DOJ lawyers in Legal Services units for Transport Canada, the CSE, DFAIT, CATSA, DND/CF, FINTRAC, the Canadian Nuclear Safety Commission and others also work on national security matters, as do the LSUs of the other departments and agencies mentioned in this chapter, to the extent that their activities may touch on national security matters. The Legal Services units, as well as specialized groups within DOJ, provide advice on constitutional law, administrative law, the *Charter of Rights and Freedoms*, international law and criminal law in relation to national security and intelligence.

16.7
TREASURY BOARD SECRETARIAT

The Treasury Board Secretariat (TBS) is involved in coordinating, analyzing and evaluating public security and anti-terrorism initiatives from a value-for-money perspective. The Secretariat helps to evaluate departmental spending proposals, identify funding priorities and monitor the performance of public security initiatives. It also evaluates annual departmental reports and recommends changes to reporting requirements for national security programs.

The President of the Treasury Board is responsible for the government-wide administration of the *Privacy Act* and the *Access to Information Act*. As a result, the Treasury Board is responsible for creating government-wide policies on the disclosure and sharing of information by federal government entities.[472] In this capacity, the TBS also oversees the cross-border flow of personal information.[473] Treasury Board policy requires that any data-matching initiative by government departments be reported to the Privacy Commissioner. In addition, a privacy impact assessment that engages the Privacy Commissioner must be conducted for any program that involves the collection, use and disclosure of personal information of employees or individuals. This policy requirement, however, may be overridden by legislation authorizing data sharing.[474] The Treasury Board suspects that not all data matching within the federal government is being reported.[475]

Finally, the Treasury Board creates policies regarding the security of government information, with tactical assistance from the RCMP and the CSE.[476] It also creates policy regarding the disclosure and flow of information under the *Security of Information Act*.[477]

16.8
DEPARTMENT OF FINANCE

The Department of Finance assesses the policy implications of proposed ongoing security initiatives with a view to evaluating the financial costs, efficiency and potential impact on the national economy of specific programs or initiatives. The Minister of Finance is also the minister responsible for the Financial Transactions and Reports Analysis Centre of Canada, or FINTRAC.

16.9
PROVINCIAL AND MUNICIPAL POLICE FORCES

The *Security Offences Act* gives the RCMP primary responsibility for the investigation and prosecution of crimes that represent a threat to the security of

Canada, or crimes that involve internationally protected persons.[478] To fulfill this mandate across Canada, the RCMP enters into formal arrangements to work with provincial and municipal police forces on criminal activity relating to national security,[479] and also co-operates and shares information on a more informal level. The RCMP and the other law enforcement representatives who made submissions to the Commission emphasized the importance of co-operation and integration between the RCMP and local police forces in national security policing. Permanent integrated teams and joint forces operations represent "a strategic response to the complications arising out of jurisdictional issues, the compartmentalization of information, disparate expertise, and the financial burden to be shared in complex investigations."[480] Without such joint operations, "police services would [remain] . . . disorganized in the face of a very organized adversary."[481] While an exhaustive description of the role of provincial, territorial and municipal police forces and governments is beyond the scope of my mandate in this section, I discuss key aspects of the national security activities of provincial, territorial and municipal police forces, particularly in relation to the RCMP's national security activities.[482]

16.9.1 Federally-Led Permanent Integrated Teams and Ad Hoc Joint-Force Operations

Provincial and municipal police officers are seconded to the four RCMP-led INSETs in Vancouver, Toronto, Ottawa and Montreal, which are the primary police units responsible for national security investigations in Canada. However, many municipal police organizations are not represented in INSETs or IBETs. [483] There are no integrated units in the Atlantic provinces that focus on national security, for example. However, representatives from some Atlantic police forces, including the Halifax Regional Police, have representation at the RCMP National Security Intelligence Section for that RCMP Division.

Within the INSET environment, officers are subject to the review and disciplinary procedures of their home jurisdiction.[484] In addition to INSETs and IBETs, national security policing may occur in the context of ad hoc joint-force investigations. The RCMP has informed the Commission that most national security policing activity in Canada is conducted in an integrated environment and includes multiple federal actors and actors under provincial jurisdiction.[485]

Integration also occurs when officers from one police force are seconded to another. For example, although this is not a national security position, the RCMP's Chief Information Officer at the time of writing is seconded from the Ontario Provincial Police (OPP).[486] Similarly, there are a number of RCMP

officers seconded to the Ottawa Police Service. These officers may drive Ottawa Police vehicles but wear RCMP uniforms.[487] While seconded RCMP officers are not assigned specifically to national security investigations,[488] like any police officer, they could be involved in investigations or operations that take on a national security dimension (for example, a car stopped for speeding contains a bomb).

Co-operation between the Ottawa Police Service and the RCMP provides a good example of the ways that local law enforcement agencies contribute to national security policing, and the difficulties inherent in defining where local jurisdiction ends and RCMP jurisdiction begins in the national security context. Criminal activity threatening ministers of the Crown or diplomatic personnel fall within RCMP jurisdiction, while the OPS has general responsibility for maintaining the peace in the city. However, government and diplomatic offices and personnel intermingle with private businesses and citizens. The previous chapter describes the hypothetical example provided by Chief Vince Bevan, in which the OPS receives a 911 call regarding an individual with a gun in a building that has offices for private businesses and for a federal minister. The OPS would respond to such a call and would not initially even inform the RCMP. Only if the investigation brought to light national security concerns, such as a threat to the minister, would the RCMP be notified, and this might not happen until the OPS investigation was well underway.[489]

Even in criminal situations where the RCMP has assumed primary jurisdiction, local police forces still have responsibilities and legal obligations to fulfill.[490] While the national security aspect of an investigation, which falls within RCMP jurisdiction, may have priority, local police forces still have responsibility for non-national security aspects of an investigation that fall within their statutory responsibilities.[491] For example, if an individual engages in commercial break-and-enter activities to finance terrorist activities, the local police force can investigate the break-ins, including executing any warrants, laying charges, assisting victims of crime, and participating in the prosecutions, while the RCMP focuses on the national security aspects of the case and anything coming out of that investigation. This type of co-operation could happen concurrently and seamlessly within the context of an INSET team.

In addition to working on joint-forces operations with the RCMP, provincial and municipal police services may work jointly on an ad hoc basis with other federal actors. The OPP, for example, works on joint operations, including intelligence operations, with CBSA customs officers. A number of provincial and municipal police forces also worked on joint-forces operations in relation to security at the 2002 G8 Summit in Kananaskis, Alberta. This security related

not only to the orderly conduct of the Summit and the protection of public and private property, but also to the protection of dignitaries and delegates, which falls under RCMP jurisdiction in the *Security Offences Act*.[492] Security planning for the Summit involved over 6,000 Canadian police officers and 5,000 Canadian Forces members.[493]

16.9.2
Provincially-Led Integrated Anti-terrorism Teams

There are also a wide variety of provincially-based integrated teams with a national security component. Examples include the Ontario Provincial Police's Anti-Terrorism Section; the Surêté du Québec's Anti-Terrorism Section; and the Manitoba Threat Advisory Group.[494]

The Manitoba Threat Advisory Group is intended to coordinate responses to emergencies and national security threats in Manitoba. The Group comprises first-responder and emergency management agencies including PSEPC, CSIS, the RCMP "D" Division, the Manitoba Emergency Measures Organization, the Winnipeg Police Service, and other Manitoba law enforcement, critical infrastructure and emergency management agencies.[495] Alberta does not have a provincial anti-terrorism police squad, but does have the Provincial Security and Information Management Unit. This unit gathers and disseminates information about possible threats to the province's security, but has no enforcement mandate.

In British Columbia, the Vancouver Police Department has established a Counter-Terrorism Unit, located organizationally within its Criminal Intelligence Section. The Unit collects, analyzes and operationalizes information about terrorist activities in Vancouver. Intelligence and operational plans are generally shared with the Vancouver INSET, and there is also a close working relationship with the local CSIS office. The Unit aims to complement the work of the RCMP and CSIS, and would advise both of these organizations of investigative or enforcement activities. The South Fraser Integrated Probe Team in British Columbia may also do some national security-related activity. This team is an RCMP-based intelligence team that works out of the Abbotsford Police Department. The team collects intelligence on all levels in the Fraser Valley area, including cross-border drug smuggling, and includes representatives from both the federal RCMP and municipal officers in Abbotsford, Langley, Mission and Chilliwack.

In the province of Quebec, the RCMP have the primary role in national security activities. However, the Sûreté du Québec (SQ) and the Montreal Police Department also have an anti-terrorism mandate.[496] The RCMP, the SQ and the Montreal Police have formed a partnership and work together under the

Anti-Terrorism Police Management Structure. The SQ also has representation at the Montreal and Ottawa INSETs, as part of the Marine Security Enforcement Team and the Great Lakes–St. Lawrence Seaway MSOC.

In 2002, the Government of Ontario established a multi-jurisdictional joint forces operation known as the Provincial Anti-Terrorism Section (PATS). PATS collects criminal intelligence in Ontario relating to public security threats, including terrorism offences under the *Criminal Code*. However, PATS does not enter into or lead national security criminal investigations, unless requested to do so under RCMP leadership.

PATS is led by the Ontario Provincial Police and includes members from ten different police services, including the RCMP. PATS headquarters are co-located with the RCMP INSET in the Greater Toronto Area, but PATS teams are deployed throughout Ontario. PATS co-operates closely with the RCMP. For example, PATS and the Ontario INSET jointly establish intelligence requirements and operational directions, and discuss initiatives to avoid duplication. Furthermore, the RCMP is the primary client of PATS intelligence.

PATS focuses on collecting and analyzing information related to terrorist criminal activity, and disseminates finished criminal intelligence products to inform law enforcement decision making. PATS collects information for the purpose of criminal prosecution. Information collection is subject to the same standards that apply to evidence collection. National security intelligence information received during a PATS operation is provided to the INSET or to CSIS, as appropriate. Files that do not disclose a public security threat will be turned back to the police service with jurisdiction for ordinary criminal investigation.

16.9.3
Day-to-Day Interaction

Although most provincial or municipal national security policing is conducted within the context of permanent or ad hoc integrated teams, considerable interaction can take place between municipal or provincial forces, CSIS and the RCMP on a day-to-day basis, depending on the police force in question, the location of events, and the type of event or investigation. Providing information is one of the principal ways that municipal and provincial police forces contribute to the national security. This type of information sharing also takes place outside the context of formal anti-terrorism teams. Municipal and provincial police services regularly pass national security information to, and receive relevant information from, the RCMP and CSIS.

16.9.3.1 Examples of Interaction with the RCMP

In British Columbia, where the RCMP provide provincial policing services and contract policing services to many municipalities, the province has created an integrated information system that allows the RCMP and municipal police forces to share information. Under the B.C. *Police Act*,[497] all police agencies, including the RCMP, are required to employ the system. The system, known as the Police Records Information Management Environment (PRIME), is an integrated police records management system that allows real-time sharing of information across municipal boundaries. For example, information from a traffic stop in rural British Columbia can be accessed by Vancouver Police officers investigating the movements of individuals suspected of involvement in organized crime.[498] Intelligence gleaned from such routine police activities may assist with anti-terrorism investigations by revealing important information such as the movement of suspects or their associations with other persons of interest.

Similarly, police agencies across Canada have recently agreed on a framework, called the Police Information Portal (PIP), an initiative that grew out of PRIME. PIP will be used to share information collected in the course of law enforcement activities.[499] It allows member law enforcement and public safety agencies to electronically share operational information that is needed to respond to interjurisdictional crime, and to track individuals who may be committing criminal offences in multiple jurisdictions. Police agencies operating on different databases are able to populate the PIP with their information, which allows all connected agencies to access that information. Currently, one third of all Canadian police officers, including all officers in British Columbia, have access to the PIP, and more law enforcement and public safety agencies are expected to become members.[500] The RCMP has signed the PIP Memorandum of Understanding, but has not yet implemented it.

In Ontario, OPP Intelligence proactively gathers information related to terrorism. Regular OPP officers are also encouraged to look out for and record information that may relate to terrorism or other national security threats. The OPP provides all information that it believes may relate to terrorist criminal activity to the RCMP INSET. Similarly, the Toronto Police Service maintains an intelligence group, which may collect information relating to national security. In addition, if the Toronto police receive information on certain behaviours that they recognize as possible precursors for terrorist activity, they share this information with the RCMP, the Ontario INSET and PATS.

The OPP and the Toronto Police Service advise that they receive threat assessments and imminent threat information from the RCMP and CSIS. A very small number of OPP members also have access to RCMP databases, including the Secure Criminal Information System and the Automated Criminal Intelligence Information System (ACIIS), which is the national criminal intelligence database. The Toronto Police Service states that most of the national security information that it receives is unclassified and can be shared broadly. However, the Service does not share the classified information that it receives.

16.9.3.2

Examples of Interaction with CSIS

Police services are increasingly aware of the importance of security intelligence information (as opposed to criminal intelligence information). The OPP and the Toronto Police Service, for example, feed security intelligence information to CSIS as it comes into their possession.[501] This information sharing might be done through the O-INSET or PATS, or the OPP might provide information directly to a CSIS regional office. The SQ also shares information with CSIS. The OPP advises me that it considers criminal intelligence to relate to any *Criminal Code* offence; beyond that, the distinction between criminal and security intelligence is a matter of professional judgment. The Toronto Police Service advises that it is in direct, regular contact with CSIS. Further, the Toronto Police may work closely with CSIS either within the context of the Ontario INSET or on an ad hoc basis. However, police services receive limited amounts of specific information from CSIS, partly because of the requirement that the police disclose all relevant information to an accused during a criminal prosecution.[502] On occasion, the Toronto Police may receive uncaveated information from CSIS to help with a criminal investigation, and this information can be used as evidence. Nonetheless, the Attorney General of Canada may still object to its disclosure during a criminal prosecution by issuing a certificate under section 38 of the *Canada Evidence Act*.

The Toronto Police Service advises that it is more likely to use CSIS linguistic and cultural resources to assist with certain types of policing as, for example, policing a demonstration by a particular cultural community. CSIS may also provide background information on criminal extremist groups, or new groups attempting to establish themselves in the Toronto area. The TPS also receives information from CSIS regarding individuals held under security certificates who have been linked to terrorism. If the Toronto Police come across information about an occurrence involving one of these people, they will report back to CSIS.

Notes

1 On February 6, 2006, Prime Minister Harper announced the reintegration of the Department of Foreign Affairs and the Department of International Trade into the Department of Foreign Affairs and International Trade. However, there are still two ministers — the Minister of Foreign Affairs and the Minister of International Trade.

2 With the exception of Canadian Heritage.

3 Except where otherwise noted, the information in this chapter is based upon meetings and communications between Policy Review legal counsel and the federal government departments and agencies described in this chapter.

4 *Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C-23, s. 6(1) [*CSIS Act*].

5 Ibid., s. 12.

6 Ibid., s. 2.

7 Ibid., s. 2.

8 Ibid., s. 21ff.

9 CSIS website on Intelligence Collection and Analysis.

10 *CSIS Act*, s. 21.

11 CSIS website.

12 *CSIS Act*, s. 16 (1)(*a*).

13 Ibid., s. 16(1)(*b*).

14 CSIS website.

15 Ibid.

16 *CSIS Act*, s. 13(1).

17 Ibid., s. 13(2)(*a*).

18 Ibid., s. 13(2)(*b*).

19 CSIS website.

20 *CSIS Act*, s. 13(3).

21 S.C. 2001, c. 27 (*IRPA*].

22 Testimony of Jim Judd, Director of CSIS, June 19, 2006, Standing Senate Committee on National Security and Defence [Testimony of Jim Judd, Director of CSIS].

23 *IRPA*, ss. 76ff.

24 See *IRPA*, ss. 34, 35, 37.

25 CSIS Backgrounder No. 14, Certificates Under the *Immigration and Refugee Protection Act (IRPA)*, revised February 2005, accessed online at htpp://www.csis-scrs.gc.ca/en/newsroom/backgrounders/backgrounder14.asp. [CSIS Backgrounder No. 14.]

26 *IRPA,* s. 82(2).

27 Ibid., s. 82(1).

28 Ibid., s. 78(*g*).

29 CSIS Backgrounder No. 14.

30 *IRPA*, s. 80(3).

31 Canada, Senate, *Proceedings of the Senate Standing Committee on the Anti-terrorism Act*, 38th Leg., (March 21, 2005), p. 6:13, testimony of Paul Kennedy, Senior Assistant Deputy Minister, PSEPC, online, Parliament of Canada, http://www.parl.gc.ca/38/1/parlbus/commbus/senate/Com-e/anti-e/pdf/06issue.pdf (accessed January 27, 2006).

32 CSIS Backgrounder No. 14.

33 *CSIS Act*, s. 17(1)(*a*)(ii).

34 Ibid., s. 17(1)(*b*).

35 Ibid., s. 17(2).

36 Ibid., s. 19(2).

37 Ibid., s. 19(2)(*a*).

38 Ibid., s. 19(2)(*b*), (*c*).

39 Ibid., s. 19(2)(*d*).

40 Ibid., s. 19(3).

41 As discussed in Chapter II, the RCMP/CSIS MOU dated September 2006 (2006 MOU) sets out a number of principles to guide the relationship between the RCMP and CSIS. It specifically addresses information and intelligence exchange and operational support and assistance.

42 Integrated National Security Enforcement Teams (see Chapter IV, s. 3.5).

43 *Criminal Code*, R.S.C. 1985, c. C-46, s. 83.05.

44 Testimony of Jim Judd, Director of CSIS.

45 Privy Council Office, *Securing an Open Society: Canada's National Security Policy* (Ottawa: Privy Council Office, 2004), online, http://www.pco-bcp.gc.ca/docs/Publications/NatSecurnat/natsecurnat_e.pdf (accessed January 4, 2006) [*Securing an Open Society: Canada's National Security Policy*].

46 Canada, Security Intelligence Review Committee, *SIRC Annual Report 2004–2005*: *An Operational Review of the Canadian Security Intelligence Service* (Ottawa: Public Works and Government Services Canada, 2005), p. 51 [*SIRC Annual Report 2004–2005*]. SIRC's annual reports are available online at http://www.sirc-csars.gc.ca/reports_e.html (accessed February 21, 2006).

47 *SIRC Annual Report 2004–2005*, p. 48.

48 For example, the Centre has studied the potential for terrorists to use the avian flu virus as a biological weapon.

49 Assessment sharing may be expanded to include Germany, the Netherlands and Spain.

50 "Welcome to the Communications Security Establishment," March 20, 2003, online, CSE, http://www.cse-cst.gc.ca/index-e.html (accessed March 22, 2006).

51 P.C. 1975-95, C. Gaz. 1975 II. 233.

52 Proceedings of the Special Committee of the Senate on the Canadian Security Intelligence Service, Hansard, September 22, 1983, pp. 18–19, 27, 31–33.

53 *National Defence Act*, R.S.C. 1985, c. N-5, s. 273.62(2).

54 Ibid., s. 273.62(3).

55 Ibid., s. 273.64.

56 Ibid., s. 273.64(2)(*a*).

57 The term "private communication" is legally defined in s. 183 of the *Criminal Code* to mean "any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it." There is a considerable body of jurisprudence interpreting this section of the *Criminal Code*. For example, pager communications do not fall within the definition of private communications (*R. v. Lubovac* (1989), 52 C.C.C. (3d) 551 (Alta. C.A.)), and a digital number recorder installed by a telephone company that discloses the outgoing telephone numbers dialled does not intercept private communications (*R. v. Fegan* (1993), 21 C.R. (4th) 65 (Ont. C.A.)). Other leading cases include *R. v. Monachan*, [1985] 1 S.C.R. 176; *Goldman v. R.* (1979), 13 C.R. (3d) 228 (S.C.C.); and *R. v. Davie* (1980), 17 C.R. (3d) 72 (B.C.C.A.).

58 *National Defence Act*, ss. 273.65(1), 273.69. The CSE's intelligence activities under the (a) mandate are subject to several legislative restrictions: they may not be directed at Canadians or any

person in Canada, and shall be subject to measures to protect the privacy of Canadians: s. 273.64(2). In addition, the Minister can authorize the interception of private communications only where the interception is directed at foreign entities located outside Canada; where the information could not reasonably be obtained by other means; where the expected foreign intelligence value of the information justifies the interception; and where measures are in place to protect the privacy of Canadians, and to ensure that private communications will be used or retained only if they are essential to international affairs, defence or security: s. 273.65(2)(*a*)–(*d*).

59 *Anti-terrorism Act*, S.C. 2001, c. 41.

60 *National Defence Act*, s. 273.65(2)(*d*).

61 Testimony of Keith Coulter, CSE Chief, before the Senate Special Committee on the Anti-terrorism Act, April 11, 2005, at 7:44 [Testimony of Keith Coulter, CSE Chief].

62 Testimony of Keith Coulter, CSE Chief at 7:54.

63 *National Defence Act*, ss. 273.65(3)–(5).

64 Ibid., s. 273.65(6).

65 Canada, Auditor General, *Auditor General's Report, November 2003* (Ottawa: Public Works and Government Services Canada, 2003), para. 10.134.

66 Testimony of Keith Coulter, CSE Chief at 7:39.

67 Testimony of Keith Coulter, CSE Chief at 7:51.

68 Canada, Privy Council Office, *Securing an Open Society: One Year Later* (Ottawa: Public Works and Government Services Canada, 2005), p. 14, online, www.pco-bcp.gc.ca/docs/ministers/deputypm/secure_e.pdf (accessed July 24, 2006) [*Securing an Open Society: One Year Later*]

69 Testimony of Keith Coulter, CSE Chief at 7:37.

70 Testimony of Keith Coulter, CSE Chief at 7:39. I describe the Canadian Forces Information Operations Group later in this chapter.

71 *Securing an Open Society: One Year Later*, p. 14.

72 Testimony of John Ossowski, Director General, Policy and Communications, CSE, before the Senate Special Committee on the Anti-terrorism Act, April 11, 2005, at 7:48.

73 Testimony of Keith Coulter, CSE Chief at 7:50.

74 *Securing an Open Society: One Year Later*, p. 14. References to "alliance" and "allied agencies" refer to the alliance of Canada, the United Kingdom, the United States, Australia and New Zealand.

75 *Securing an Open Society: One Year Later*, p. 14.

76 Department of National Defence, "The National Defence Family," Sept. 12, 2005, online, Department of National Defence, http://www.forces.gc.ca/site/about/family_e.asp For more information on the Canadian Rangers, see Department of National Defence, Backgrounder, "The Canadian Rangers," February 18, 2000, online Department of National Defence, http://www.forces.gc.ca/site/newsroom/view_news_e.asp?id=49 (accessed February 20, 2006).

77 Ibid.

78 Communication Security Establishment, "Place in Government," http://www.cse-cst.gc.ca/about-cse/place-in-gov-e.html (accessed March 14, 2006).

79 Department of National Defence, "About DND/CF," March 9, 2006, online. http://www.forces.gc.ca/site/about/partner_e.asp; Communication to Policy Review legal counsel, May 3, 2006. In relation to counter-proliferation, DND would provide assistance to both the CBSA and the RCMP.

80 Department of National Defence, *Canada's International Policy Statement: A Role of Pride and Influence in the World — Defence* (Ottawa: Her Majesty the Queen in Right of Canada, 2005).

81 This burden may include personnel, equipment or assets, and/or time. Examples include coalition operations in Afghanistan and during the 1990–1991 Persian Gulf War.

82 Established by Ministerial Order 98023 (11 May 1998), Unclas DGPS 9985 021550Z Sep 99.

83 *Criminal Code*, s. 183. See the discussion of private communications in the previous section of this chapter.

84 *National Defence Act*, ss. 274–285.

85 Gen. R.J. Hillier, Chief of Defence Staff, "CISS Seminar: Implementing Canada's Defence Policy Statement" (Seminar, Royal Canadian Military Institute, July 2005), online, Department of National Defence, http://www.forces.gc.ca (accessed February 10, 2005); Canada, Department of National Defence, CDS Action Team Reports, "Executive Summary of CAT 2 Report," online, Department of National Defence, http://www.cds.forces.gc.ca/cft-tfc/pubs/cat_e.asp (accessed February 15, 2006).

86 The exchange of intelligence products between these various agencies is based on individual stated requirements and the "need to know" policy.

87 Department of National Defence, Directive DAOD 8002-1, *National Counter-Intelligence Program*, March 28, 2003, online, DND Finance and Corporate Services, http://www.admfincs.forces.gc.ca/admfincs/subjects/DAOD/8002/1_e.asp (accessed March 21, 2006). [*National Counter Intelligence Program, DAOD 8002-1*]

88 "INSETs" is the acronym for "Integrated National Security Enforcement Teams"; "IBETs" is the acronym for "Integrated Border Enforcement Teams." See Chapter IV, s.3.5.

89 See Department of National Defence, Directive DAOD 8002-3, *Security Intelligence Liaison Program*, March 28, 2003, online, DND Finance & Corporate Services, http://www.admfincs.forces.gc.ca/admfincs/subjects/daod/8002/3_e.asp (accessed March 21, 2006). [*Security Intelligence Liaison Program, DAOD 8002-3*]

90 *Security Intelligence Liaison Program, DAOD 8002-3*. Threats to the security of DND/CF are outlined and discussed in Department of National Defence, Directive DAOD 8002-0, *Counter-Intelligence*, March 28, 2003, online, DND Finance & Corporate Services, http://www.admfincs.forces.gc.ca/admfincs/subjects/daod/8002/0_e.asp (accessed March 21, 2006).

91 *National Counter Intelligence Program, DAOD 8002-1*.

92 These directions are sometimes referred to by the acronym "CFAAD."

93 For more information on JTF 2, see Department of National Defence, "Joint Task Force Two," online, http://www.ops.forces.gc.ca/units/jtf2/pages/about_e.asp (accessed February 9, 2006).

94 I describe the Government Operations Centre in the section of this chapter on Public Safety and Emergency Preparedness Canada. See also Canada, Department of National Defence, Backgrounder, "Special Operations Group," Sept. 13, 2005, online, Department of National Defence, http://www.forces.gc.ca (accessed February 12, 2006).

95 *Order Designating the Canada Border Services Agency as a Department and the President as Deputy Head*, S.I./2003-218, C. Gaz. II, 31/12/03, made pursuant to the *Public Service Employment Act*, R.S.C. 1985, c. P-33. The Minister of Public Safety and Emergency Preparedness became the minister responsible for the CBSA by virtue of a second order in council, *Order Transferring from the Minister of Citizenship and Immigration to the Deputy Prime Minister and Minister of Public Safety and Emergency Preparedness the Control and Supervision of the Canada Border Services Agency*, S.I./2003-214, C. Gaz. II, 31/12/03.

96 *Order Transferring Certain Portions from the Department of Citizenship and Immigration to the Canada Border Services Agency*, S.I./2003-215, C. Gaz. II, 31/12/03; *Order Transferring to the Canada Border Services Agency the Control and Supervision of Certain Portions in the Department of Citizenship and Immigration*, S.I./2004-136, C. Gaz. II, 20/10/04; *Order Transferring to the Department of Citizenship and Immigration the Control and Supervision of Certain Portions within the Canada Border Services Agency and Transferring from the Deputy*

Minister and Minister of Public Safety and Emergency Preparedness to the Minister of Citizenship and Immigration Certain Powers, Duties and Functions, S.I./2004-135, C. Gaz. II, 20/10/04.

97 *Order Transferring Certain Portions of the Canada Customs and Revenue Agency to the Canada Border Services Agency*, S.I./2003-216, C. Gaz. II, 31/12/03.

98 *Order Transferring Certain Portions of the Operations Branch of the Canadian Food Inspection Agency to the Canada Border Services Agency*, S.I./2003-217, C. Gaz. II, 31/12/03. The key statute in relation to food inspection is the *Canadian Food Inspection Agency Act*, S.C. 1997, c. 6, transferred from the Canadian Food Inspection Agency.

99 *An Act to establish the Canada Border Services Agency*, S.C. 2005, c. 38, s. 5(1) [*CBSA Act*]. The Border Agency's mandate also requires it to "facilitate the free flow of persons and goods" that meet all legal requirements.

100 *CBSA Act,* s. 2.

101 Ibid., s. 13. There are some restrictions on this power. The CBSA requires the approval of the Governor in Council, given on the recommendation of the Minister of Public Safety and the Minister of Foreign Affairs. Any agreement may only be made subject to s. 38 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, S.C. 2000, c. 17, which allows an individual or organization to avoid reporting the import or export of currency by choosing not to transfer the currency.

102 "Canada Border Services Agency National Statistics," online, CBSA, http://www.cbsa-asfc.gc.ca/newsroom/release-communique/2005/0615ottawa-e.html (accessed January 4, 2006).

103 *Securing an Open Society: Canada's National Security Policy*.

104 More precisely, immigration laws refer to "the laws and regulations that relate to the admission, temporary entry, removal, naturalization, denaturalization or loss of nationality by persons": API/PNR MOU, sbs. 1(d).

105 *IRPA*, s. 34.

106 Ibid., s. 35.

107 Ibid., s. 36.

108 Ibid., s. 37.

109 Ibid., ss. 38–42.

110 Ibid., ss. 34(2), 37(2). The Minister of Citizenship and Immigration may not make an exception for individuals who are reasonably believed to have committed war crimes or crimes against humanity: *IRPA*, ss. 35(1)(*a*), 35(2). The Minister also has some discretion with respect to people convicted of serious crimes who, after a certain period of time, satisfy the Minister that they have been rehabilitated: *IRPA*, s. 36(3)(*c*).

111 "Serious criminality" is defined in s. 36(1) of the *Immigration and Refugee Protection Act*. Specifically, serious criminality includes:

> (a) having been convicted in Canada of an offence under an Act of Parliament punishable by a maximum term of imprisonment of at least 10 years, or of an offence under an Act of Parliament for which a term of imprisonment of more than six months has been imposed;
>
> (b) having been convicted of an offence outside Canada that, if committed in Canada, would constitute an offence under an Act of Parliament punishable by a maximum term of imprisonment of at least 10 years; or
>
> (c) committing an act outside Canada that is an offence in the place where it was committed and that, if committed in Canada, would constitute an offence under an Act of Parliament punishable by a maximum term of imprisonment of at least 10 years.

112 "Organized criminality" is defined in s. 37(1) of the *Immigration and Refugee Protection Act*. Specifically, organized criminality includes:

> (a) being a member of an organization that is believed on reasonable grounds to be or to have been engaged in activity that is part of a pattern of criminal activity planned and organized by a number of persons acting in concert in furtherance of the commission of an offence punishable under an Act of Parliament by way of indictment, or in furtherance of the commission of an offence outside Canada that, if committed in Canada, would constitute such an offence, or engaging in activity that is part of such a pattern; or
>
> (b) engaging, in the context of transnational crime, in activities such as people smuggling, trafficking in persons or money laundering.

113 For example, at points of entry into Canada, CBSA officers will perform the functions of both agencies. Inside Canada, on the other hand, CIC officers perform the functions of both organizations in relation to refugee claimants.

114 The CBSA's mandate with respect to migration is regulated by the *Immigration and Refugee Protection Act*.

115 For more information on CBSA's detention powers and policies, see Canada, Citizenship and Immigration, "ENF 20, Detention" (Ottawa: CIC, 2005), online, CIC, http://www.cic.gc.ca/manuals-guides/english/enf/enf20e.pdf (accessed March 8, 2006). See also *Sahin v. Canada (Minister of Citizenship and Immigration)* (1994), 85 F.T.R. 99 (F.C.) and *Canada (Minister of Citizenship and Immigration) v. Thanabalasingham*, [2004] 3 F.C.R. 572 (F.C.A.).

116 For more information on CBSA removals powers and policies, see Canada, Citizenship and Immigration, "ENF 10, Removals," online, CIC, http://www.cic.gc.ca/manuals-guides/english/enf/enf10e.pdf (accessed March 8, 2006).

117 Customs laws can be more precisely defined as "the laws and regulations relating to the importation, exportation and transportation of goods across national boundaries and all other laws and regulations enforced and administered" by CBSA Customs: API/PNR MOU, *infra*, para. 1(c). The principal customs statute is the *Customs Act*, R.S.C. 1985, c. 1 (2nd Supp.), transferred from the Canada Customs and Revenue Agency. See also the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, S.C. 2000, c. 17, s. 12(1) [*PCMLTFA*].

118 *PCMLTFA*, s. 12; *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations*, S.O.R./2002-184, s. 12(1). The regulations currently require all transactions over $10,000 to be reported.

119 *PCMLTFA*, ss. 15–17.

120 Ibid., s. 18.

121 Ibid., s. 19.1.

122 Under the *IRPA*, officers may be authorized by the Minister of Public Safety to exercise police powers: *IRPA*, ss. 4(2), 6(1), 138(1).

123 *Customs Act*, s. 163.5(1); *Excise Act*, R.S.C. 1985, c. E-14, s. 75; *Export and Import Permits Act*, R.S.C. 1985, c. E-19, s. 25; *IRPA*, s. 55.

124 *Customs Act*, ss. 163.5(3), 153.1, 160.1; *Excise Act*, ss. 97, 157(1); *Export and Import Permits Act*, s. 25; *R. v. Simmons*, [1988] 2 S.C.R. 495; *IRPA*, s. 55; *Dehghani v. Canada (Minister of Employment and Immigration)*, [1993] 1 S.C.R. 1053; *Sahin v. Canada (Minister of Citizenship and Immigration)*, [1995] 1 F.C. 214 (F.C.T.D.).

125 *Customs Act*, ss. 98, 99, 99.2, 153.1, 160.1; *Excise Act*; ss. 72–74, 157; *Excise Act 2001*, S.C. 2002, c. 22, ss. 258(1), 260; *Export and Import Permits Act*, s. 25.

126 *Customs Act*, ss. 110–116; *Excise Act*, s. 70; *Excise Act 2001*, ss. 258(1), 260(2)(*f*), 293; *Export and Import Permits Act*, s. 25.

127 *Customs Act*, s. 163.5(2); *Export and Import Permits Act*, s. 25.

128 *IRPA*, ss. 6(1), 15, 16, 55, 138(1).

129 Ibid., s. 55(1). Officers may also issue warrants if they believe a permanent resident or foreigner will not appear at an immigration proceeding.

130 *IRPA*, s. 55(2)(*a*). Para. (*b*) also allows a foreign national to be arrested and detained without a warrant if an immigration officer is not satisfied of the person's identity during a procedure under the *IRPA*.

131 *IRPA*, s. 55(3). Detention is also possible if the officer suspects the person is inadmissible on the basis of human or international rights violations. Under s. 34 of the *IRPA*, a person is inadmissible on grounds of "security" for engaging in terrorism or acts of violence likely to endanger the lives or safety of persons in Canada; being a member of an organization that it is believed engages, has engaged or will engage in such activity; being a danger to the security of Canada; or engaging in espionage or subversion.

132 Canada, Department of Finance, *Budget Plan 2006* (Ottawa: Her Majesty the Queen in Right of Canada, 2006), p. 131.

133 *Memorandum of Understanding between the Department of Citizenship and Immigration Canada and the Royal Canadian Mounted Police, Investigations and Referrals for Prosecution*, being Annex IV to the *Memorandum of Understanding Concerning Partnership, Communication, Cooperation and Information Sharing between Citizenship and Immigration Canada and the Royal Canadian Mounted Police*, Ottawa, December 23, 2002. [Investigations and Referrals for Prosecution MOU] *Memorandum of Understanding Concerning Partnership, Communication, Cooperation and Information Sharing between Citizenship and Immigration Canada and the Royal Canadian Mounted Police*, Ottawa, December 23, 2002, s. 16 [CIC-RCMP Cooperation MOU]. Note that CIC, the RCMP and the CBSA are renegotiating bilateral arrangements to replace this MOU.

134 *Customs Act*, s. 2(1).

135 *Excise Act*, s. 66(1)*; Excise Act 2001,* s. 2.

136 Canada, Department of National Revenue, Customs Prosecution Policy for Offences Under the Customs Act, in force September 6, 1983, s. 1; Customs/RCMP Division of Investigative and Enforcement Responsibilities (revision of 1983 policy), February 1991, s. 1(a); R.S.C. 1985, c. I-5, s. 18(1). Note that some bands have established their own police forces to provide policing services on reserves.

137 I have discussed the *RCMP Act*, R.S.C. 1985, c. R-10, and RCMP policies in more detail in chapters II and IV.

138 "Fact Sheet, Immigration Intelligence — Overview," online, CBSA, http://www.cbsa-asfc.gc.ca/newsroom/factsheets/2004/0128overview-e.html (accessed January 5, 2006) [Immigration Intelligence Fact Sheet].

139 *Memorandum of Understanding between the Department of Justice and the Department of Citizenship and Immigration and the Royal Canadian Mounted Police*. [CBSA-DOJ-RCMP War Crimes MOU].

140 Immigration Intelligence Fact Sheet.

141 Ibid.

142 Ibid.

143 This reporting is governed by the Intelligence and Fraudulent Documents MOU.

144 *Memorandum of Understanding for the Exchange of Customs Related Intelligence Information between the Royal Canadian Mounted Police and the Department of National Revenue, Customs and Excise, of Canada and the Department of the Treasury of the United States of America, United States Customs Service*, Ottawa, December 8, 1982 [Customs-RCMP-USA MOU]; *Memorandum of Understanding between the Royal Canadian Mounted Police and Revenue Canada Customs*, Ottawa, January 11, 1995; Ministerial Policy: Division of Investigative and Enforcement Responsibilities, s. 10.

145 Customs-RCMP-USA MOU.

146 The CBSA is in the process of building a separate, long-term detention facility connected to Millhaven maximum security prison in Kingston, Ontario, to house security certificate detainees. The facility will belong to the CBSA, but the Correctional Service of Canada will be the service provider.

147 Office of the Privacy Commissioner of Canada, *Audit of the Personal Information Management Practices of the Canada Border Services Agency*, Final Report, June 2006, para. 3.58, online, http://www.privcom.gc.ca/information/pub/ar-vr/cbsa_060620_e.asp (accessed July 10, 2006) [CBSA Audit].

148 I also discuss the lookout screening process and the various grounds for inadmissibility in the section on Citizenship and Immigration Canada.

149 For more information on lookout flags, see Canada, Citizenship and Immigration, "ENF 4, Port of Entry Examinations" (Ottawa: CIC, 2006), s. 26, online, CIC, http://www.cic.gc.ca/manuals-guides/english/enf/enf04e.pdf (accessed March 8, 2006) [Memorandum ENF 4].

150 The Terrorist Screening Center is administered by the FBI and includes staff from the Department of Homeland Security and the State Department. U.S. Customs and Border Protection administers the National Targeting Center. The two agencies work closely together to identify and apprehend persons on the U.S. National Terrorist Watch List, and both work closely with the U.S. National Counterterrorism Center to identify potential terrorist suspects: U.S., Department of Homeland Security, Fact Sheet: "U.S. Customs and Border Protection's National Targeting Center," Sept. 2004, online, http://www.dhs.gov/dhspublic/display?content=3989 (accessed March 6, 2006); U.S., Department of Homeland Security, Fact Sheet: "The Terrorist Screening Center," Sept. 16, 2003, online: http://www.dhs.gov/dhspublic/display?content=1598; U.S., Department of Justice, Fact Sheet: Terrorist Screening Center, September 2003, online, http://www.fbi.gov/ressrel/pressrel03/tscfactsheet091603.htm (accessed March 7, 2006). For more information on these initiatives, see the Federation of American Scientists Intelligence website at http://www.fas.org/main/content.jsp?formAction=325&projectId=6.

151 For more information on the review and removal of lookout flags, see Memorandum ENF 4.

152 *Customs Act*, s. 107.1(1); *Passenger Information (Customs) Regulations*, S.O.R./2003-219.

153 See for example *Memorandum of Understanding for the Automated Exchange of Lookouts and the Exchange of Advance Passenger Information (API) between The Canada Border Services Agency and United States Customs and Border Protection*, Alexandria, Virginia, USA, March 9, 2005, s. 1(g). [API/PNR MOU].

154 Even details such as the type of airline meal requested and Passenger Type Codes could indirectly reveal information about an individual's religious beliefs. See the discussion in European Union Article 29 Data Protection Working Party, *Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP)*, adopted January 29, 2004, pp. 7–8, online, Europa, Article 29 Data Protection Working Party, http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/index_en.htm (accessed March 30, 2006).

155 *Customs Act*, s. 107(4)(*b*); *Privacy Act*, s. 8(2); Memorandum D1-16-3, s. 64. See also Canada, CBSA, *Privacy Impact Assessment: Advanced Passenger Information/Passenger Name Record Program,* online, CBSA, http://www.cbsa-asfc.gc.ca/general/pia-efvp/api_ipv_20051003-e.html (accessed March 7, 2006) [API/PNR Privacy Impact Assessment].

156 Memorandum D1-16-3, s. 65.

157 Ibid., ss. 23, 35.

158 Ibid, s. 23.

159 Ibid, s. 54.

160 *Customs Act*, ss. 107(5)(*b*), 107(5)(*c*), 107(5)(*k*).

161 Memorandum D1-16-3, s. 56.

162 Ibid, s. 60.

163 These agreements or arrangements must comply with s. 8(2) of the *Privacy Act* or s. 107(8) of the *Customs Act*.

164 Memorandum D1-16-3, s. 34.

165 *Aeronautics Act*, R.S.C. 1985, c. A-2, s. 4.82. I discuss this program in more detail later in this chapter in relation to Transport Canada.
Note that s. 4.82 is not yet in force. The text of this section is available on the Library of Parliament website, Legisinfo, at http://www.parl.gc.ca/PDF/37/3/parlbus/chambus/house/bills/government/C-7_4.pdf (accessed March 22, 2006).

166 "Fact Sheet, National Risk Assessment Centre," online, CBSA, http://www.cbsa-asfc.gc.ca/newsroom/factsheets/2005/0125risk-e.html (accessed January 5, 2006) [NRAC Fact Sheet].

167 *Passenger Information (Customs) Regulations*, SOR/2003-219, s. 3(g). The regulation is deemed to have come into force on October 4, 2002: s. 5. S. 269 of the *Immigration and Refugee Protection Regulations*, S.O.R./2002-227, contains a similar requirement. An agreement between Canada and the European Union identifies a list of 25 pieces of PNR information that will be provided by European air carriers to the CBSA. There is no limitation on the types of PNR information that may be provided by carriers from other countries: *Agreement between the European Community and the Government of Canada on the Processing of Advance Passenger Information (API)/Passenger Name Record (PNR) Data* online, European Union, http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2005/com2005_0200en01.pdf (accessed January 4, 2006) [Canada-EU Agreement]. The PNR information that European airlines are to provide to the CBSA includes date of reservation; payment information; billing address; names of other travellers on the same record; contact telephone numbers; travel itinerary; some frequent flyer information; travel agency and agent; seat number; no-show history; baggage tag numbers; whether the ticket is one-way or return; whether the ticket was purchased on stand-by; and the order in which a person checked in for the flight. However, the 2005 Canada-U.S. API/PNR MOU mentioned above expressly refers to commitments and undertaking given to the European Union by Canada and the United States, respectively, during negotiations relating to the transfer of API/PNR data from European air carriers: API/PNR MOU, s. 4, note 1. The Canadian commitments are discussed in European Union Article 29 Data Protection Working Party, *Opinion 1/2005 on the level of protection ensured in Canada for the transmission of Passenger Name Record and Advance Passenger Information from airlines*, Adopted January 19, 2005, online European Union, Article 29 Working Party, http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/index_en.htm (accessed March 30, 2006). The American undertakings are discussed in European Union Article 29 Data Protection Working Party, *Opinion 2.2004 on the Adequate protection of Personal Data Contained in the PNR of Air Passengers to be Transferred to the United States' Bureau of Customs and Border protection (US CBP)*, Adopted January 29, 2004, online, European Union, Article 29 Working Party, http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/index_en.htm (accessed March 30, 2006).

168 "Privacy Impact Assessments," online, CBSA, http://www.cbsa-asfc.gc.ca/general/pia-efvp/hrti_ivre_20051003-e.html.

169 Canada, CBSA, "Departmental Performance Report 2004–2005, Section II – Analysis of Performance by Strategic Outcome, Program Activity: Enforcement (Security)," online, Treasury Board Secretariat of Canada, http://www.tbs-sct.gc.ca/rma/dpr1/04-05/BSA-ASF/BSA-ASFd4502_e.asp (accessed January 4, 2006) [CBSA DPR 2004-2005].

170 API/PNR MOU. [This information-sharing program has been reviewed by the Privacy Commissioner: http://www.cbsa-asfc.gc.ca/general/pia-efvp/api_ipv_20051003-e.html.]

171 API/PNR MOU, ss. 1(g), 7–10.

172 *Concept of Operations US-Canada Terrorist Watch List Program (CONOPS)*, signed May 23, 1997 [TUSCAN/TIPOFF Aide-Memoire].

173 Ibid.

174 Ibid., s. A(2).

175 Ibid., s. C(1)(a).

176 Ibid., s. C(1)(c).

177 Ibid., s. C(1)(c)(5) and Appendix C.

178 Canada–United States *Container Security Initiative Partnership Arrangement*, Washington, D.C., Oct. 20, 2005; "Marine Trade Security," online, Canadian Border Services Agency, http://www.cbsa-asfc.gc.ca/general/enforcement/mts_smc-e.html (accessed January 4, 2006); "Advance Commercial Information," online, CBSA, http://www.cbsa-asfc.gc.ca/import/advance/menu-e.html (accessed January 4, 2006); Canada, CBSA "Departmental Performance Report 2004–2005, Section II – Analysis of Performance by Strategic Outcome, Program Activity: Enforcement (Security)," online, Treasury Board Secretariat of Canada, http://www.tbs-sct.gc.ca/rma/dpr1/04-05/BSA-ASF/BSA-ASFd4502_e.asp (accessed January 4, 2006) [CBSA DPR 2004-2005]. See also a description of joint EU-US initiatives, "Customs and Security," online, European Union, http://europa.eu.int/comm/taxation_customs/customs/policy_issues/customs_security/index_en.htm (accessed January 4, 2006).

179 Detailed information about the type of information the CBSA requires is available on the CBSA website, "Advance Commercial Information," http://www.cbsa-asfc.gc.ca/import/advance/cap_pac-e.html (accessed January 31, 2006).

180 "Marine Trade Security," online, CBSA, http://www.cbsa-asfc.gc.ca/general/enforcement/mts_smc-e.html (accessed January 4, 2006).

181 For more information on the Container Security Initiative program, see the U.S. Customs and Border Patrol website at http://www.cbp.gov/xp/cgov/border_security/international_activities/csi/ (accessed March 9, 2006).

182 Canada-United States *Container Security Initiative Partnership Arrangement*, Washington, D.C., Oct. 20, 2005. For more information on Canada's participation in the Container Security Initiative and related container security programs, see generally CBSA, "Marine Trade Security," online, CBSA, http://www.cbsa-asfc.gc.ca/general/enforcement/mts_smc-e.html (accessed January 4, 2006).

183 CBSA DPR 2004-2005.

184 Ibid.

185 These goods are listed in the Export Control List, S.O.R./89-202.

186 Any goods exported to countries listed on the Area Control List, S.O.R./81-543, require an export permit. Currently, Myanmar (Burma) is the only country on this list.

187 *Export and Import Permits Act*, s. 25.

188 Investigation and Referrals for Prosecution MOU, ss. 1–14.

189 Ibid., s. 14.

190 Ibid, s. 15.

191 Canada, RCMP, "Waterfront Joint Forces Operation," online, RCMP, http://www.rcmp-grc.gc.ca/bc/crops/caw/coastal/wjfo/home_e.htm (accessed March 6, 2007); Canada, RCMP, "National and Border Security," online, RCMP, http://www.rcmp-grc.gc.ca/qc/pro_ser/sec_nat_front_e.htm≠ENEP (accessed March 8, 2006).

192 Section 241 of the *Income Tax Act*, R.S.C. 1985, c. 1 (5th Supp.), prevents CRA representatives from disclosing taxpayer information unless a judicial order for disclosure has been made or criminal charges have been laid: *Income Tax Act*, ss. 241(3), 241(3.2), 241(4)(*e*)(v). I have discussed these restrictions in more detail in the section of this chapter dealing with the CRA.

193 Canada, RCMP, "Integrated Proceeds of Crime (IPOC)," online, RCMP, http://www.rcmp-grc.gc.ca/on/prog_serv/fed_serv/ipoc_e.htm (accessed March 6, 2006).

194 Canada, RCMP, "Combined Forces Special Enforcement Unit," online, RCMP, http://www.cfseu.org/site.htm (accessed March 6, 2006). The CBSA has a mandate to screen immigrants and travellers to Canada for links with organized crime under s. 37 of the *IRPA*.

195 Canada, RCMP, "Integrated Market Enforcement Teams," online, RCMP, http://www.rcmp-grc.gc.ca/fio/imets_e.htm (accessed March 6, 2006).

196 Intelligence and Fraudulent Documents MOU, ss. 2(a)–(b). Topics on which information may be shared include public security concerns, terrorism, espionage and subversion, war crimes and other criminal activity.

197 Intelligence and Fraudulent Documents MOU, s. 2(d).

198 CIC-CSIS MOU.

199 Investigation and Referrals for Prosecution MOU, s. 10.

200 Ibid, s. 11.

201 Ibid, s. 9.

202 *Criminal Code*, ss. 7(7), 477.2. Offences under the *Security of Information Act*, R.S.C. 1985, c. O-5, also require such consent.

203 *IRPA*, s. 117.

204 Investigation and Referrals for Prosecution MOU, s. 8.

205 Ibid, s. 16.

206 *Memorandum of Understanding between The Department of National Revenue Responsible for the Enforcement of the Customs Act, Excise Act, Excise Tax Act, and Income Tax Act and the Canadian Police Information Centre, a National Police Service of the Royal Canadian Mounted Police*, Ottawa, July 17, 1995; *Memorandum of Understanding between Citizenship and Immigration Canada Enforcement Branch, National Service Sector and the Canadian Police Information Centre, a National Police Service of the Royal Canadian Mounted Police*, Ottawa, October 1995; *Memorandum of Understanding between the Royal Canadian Mounted Police and Revenue Canada Customs*, Ottawa, January 11, 1995 (this MOU relates to access to the Police Information Retrieval System).

207 RCMP assistance would be requested in relation to specific, legislatively defined grounds for inadmissibility to Canada, set out at ss. 34, 35 and 37 of the *IRPA*.

208 *Memorandum of Understanding between the Royal Canadian Mounted Police and Revenue Canada Customs*, Ottawa, January 11, 1995.

209 Investigation and Referrals for Prosecution MOU, s. 17. This list is not exhaustive.

210 Ibid, s. 20.

211 Ibid, s. 21.

212 CBSA-DOJ-RCMP War Crimes MOU.

213 *CSIS Act*, s. 14.

214 CIC-CSIS MOU. This agreement allows the parties to share information under s. 8(2)(*e*) of the *Privacy Act*, R.S.C. 1985, c. P-21.

215 *CBSA Act*, s. 119(1), amending ss. 150.1(1)(*a*) and (*b*) of the *IRPA*. The conditions under which information may be shared or used can be set by government regulation: *CBSA Act*, s. 119(2).

216 Three principle policy documents help CBSA employees interpret s. 107: *Memorandum D1-16-1, Explanation of Section 107 of the Customs Act* (Ottawa: Canada Customs and Revenue Agency, 2003) [Memorandum D1-16-1]; *Interim Memorandum D1-16-2, Interim Administrative Guidelines for the Provision to others, Allowing access to others, and Use of Customs Information* (Ottawa: Canada Customs and Revenue Agency, 2003) [Memorandum D1-16-2]; and *Interim Memorandum D1-16-3, Interim Administration Guidelines for the Provision to others, Allowing access to others and Use of Passenger Name Record (PNR) Information*. Memorandums D1-16-1

and D1-16-2 are available on the CBSA website at http://www.cbsa.gc.ca/formspubs/menu-e.html (accessed March 8, 2006).

217 *Customs Act*, s. 107(4)(*b*).

218 Ibid., s. 107. See especially ss. 107(4)(*d*) and 107(5)(*a*) and (*c*). The individuals authorized to make disclosures for law enforcement purposes are listed in Appendix B to Memo D1-16-2, at 13-21.

219 *Customs Act,* ss. 107(5)(*a*), 107(5)(*c*)(ii); Memorandum D-16-2, para. 30.

220 *Customs Act*, s. 107(5)(*j*).

221 *IRPA*, s. 150.1(*b*); Memorandum IN 1 at 7.

222 The investigatory bodies with whom information may be shared under s. 8(2)(*e*) of the *Privacy Act* are listed in Schedule II of the *Privacy Regulations*, S.O.R./ 83-508.

223 *Privacy Act*, s. 8(2)(*e*).

224 Ibid., s. 8(2)(*f*).

225 Memorandum IN 1 at 7. A partial list of Immigration information sharing agreements and arrangements is provided in Appendix A to memorandum IN 1.

226 Memorandum IN 1, Appendix 1.

227 I discuss FINTRAC's national security role later in this chapter.

228 *PCMLTFA*, s. 12; *Cross-border Currency and Monetary Instruments Reporting Regulations*, S.O.R./2002-412.

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

230 Ibid., s. 36(2).

231 Ibid., s. 36(3.1).

232 Canada, CBSA, *Memorandum D19-14-1, Cross-Border Currency and Monetary Instruments Reporting* (Ottawa: CBSA, 2004), para. 50, online, CBSA, http://www.cbsa.gc.ca/formspubs/menu-e.html (accessed March 8, 2006).

233 *PCMLTFA*, s. 55(3)(*d*).

234 Ibid.

235 *Agreement Between the Government of Canada and the Government of the United States of America Regarding Mutual Assistance and Co-operation Between their Customs Administrations*, Quebec, June 20, 1984, C.T.S. 1985/23, Arts. 11 (i) and (ii). This treaty is available online at DFAIT, Canada Treaty Information Section, http://www.treaty-accord.gc.ca/ViewTreaty.asp?Treaty_ID=100821 (accessed February 21, 2006) [1984 Canada-US Customs Mutual Assistance Treaty].

236 Customs-RCMP-USA MOU.

237 CBSA Audit, Recommendation #1.

238 The Customs branch of the CBSA has Customs Mutual Assistance agreements, which are formal treaty instruments, in place with France; Germany; the Republic of Korea; Mexico; the United States; and the European Community, including Austria, Belgium, Denmark, Finland, Germany, Greece, Ireland, Italy, Luxemburg, the Netherlands, Portugal, Spain, Sweden and the United Kingdom.

239 Signed 7 July 1999, implemented October 2004.

240 Signed 29 March 2001, implemented on the same day.

241 Signed 22 November 2000, not implemented.

242 Signed 4 June 1999, not implemented.

243 Signed 1996, not implemented.

244 The agreements with the U.K., New Zealand and Hong Kong are not operational because individuals have not been designated by their respective governments to receive requests and provide information under the agreement, and identified to the other party. The designations for the MOUs with Australia and the Netherlands are very limited, so only a small number of people are authorized to share information.

245 For example, at points of entry into Canada, CBSA officers will perform the functions of both organizations. Inside Canada, on the other hand, CIC officers perform the functions of both organizations in relation to refugee claimants.

246 Under the *IRPA*, s. 36.

247 Security concerns are defined in the *IRPA*, ss. 34, 35, 37.

248 See for example Canada, Citizenship and Immigration, IP 10, *Refusal of National Security Cases/Processing of National Interest Requests* (Ottawa: Citizenship and Immigration Canada, 2005). This policy document describes CIC-CBSA co-operation on national security screening for applications for permanent residence.

249 CIC does not create or add information to lookouts; this responsibility lies with the CBSA. Lookout flags are discussed in more detail in the next section of this chapter, which deals with the CBSA's national security role.

250 CIC-RCMP co-operation in this regard is governed by a *Memorandum of Understanding between the Department of Citizenship and Immigration Canada and the Royal Canadian Mounted Police*, *Fingerprinting and Screening*, being Annex II of *Memorandum of Understanding Concerning Partnership, Communication, Cooperation and Information Sharing between Citizenship and Immigration Canada and the Royal Canadian Mounted Police*, Ottawa, December 23, 2002 [Fingerprinting and Screening MOU].

251 The CBSA also has specialized units dedicated to preventing the entry of organized criminals and war criminals.

252 *Memorandum of Understanding* between CIC and CSIS, February 4, 2002 [CIC-CSIS MOU].

253 Co-operation between CIC and the RCMP in this regard is governed by the Fingerprinting and Screening MOU.

254 RCMP assistance would be requested in relation to specific, legislatively defined grounds for inadmissibility to Canada, set out at ss. 34, 35 and 37 of the *IRPA*. In relation to CSIS presence, see Canada, Security Intelligence Review Committee, *SIRC Annual Report 2003–2004*: *An Operational Review of the Canadian Security Intelligence Service* (Ottawa: Public Works and Government Services Canada, 2004), p. 6.

255 The *IRPA*, s. 55(1), allows a refugee claimant to be detained if an officer suspects that the individual will not appear at future immigration proceedings. S. 55(3) allows a CBSA officer to detain a refugee claimant at the border for further questioning or where the officer suspects that the individual poses a risk to national security.

256 SMU Annex.

257 *IRPA*, ss. 112–114 in relation to immigration and visa applicants, and s. 115(1) in relation to refugee claimants. A separate process under s. 115(2) of the *IRPA*, called the danger opinion process, is used for refugee claimants; however, it not used for refugee claimants found to be inadmissible for reasons broadly relating to national security. Therefore, I have not discussed it further in this section.

258 *IRPA*, ss. 112(1), 115(1), 115(2).

259 The factors that must be considered are set out in detail at s. 97 of the *IRPA*. The standard of "serious risk of torture" is the internationally accepted interpretation of Art. 3 of the *United Nations Convention Against Torture and Other Inhuman, Cruel or Degrading Treatment or Punishment*, New York, December 10, 1984, C.T.S. 1987/36, 1465 U.N.T.S. 85.

260 *IRPA*, ss. 79, 81(c).

261 Ibid., s. 113(*d*). If the assessment recommends that the person be allowed to remain in Canada, the deportation order will be stayed: *IRPA*, s. 114(1)(*b*). The Supreme Court of Canada has held that balancing process does not violate Canada's Constitution: *Suresh v. Canada (Minister of Citizenship and Immigration)*, [2002] 1 S.C.R. 3. However, in the recent case of *Dadar v. Canada*, December 5, 2005, U.N. Doc. CAT/C/35/D/258/2004 (decision of the Committee Against Torture), the United Nations Committee Against Torture held that the balancing test

violates Canada's absolute obligation not to deport individuals where they face a real risk of torture under the *Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*, 10 December 1984, 1465 U.N.T.S. 85, Can T.S. 1987/36 (in force June 26, 1987), Art. 3, online, Office of the High Commissioner for Human Rights, http://www.ohchr.org/english/law/cat.htm (accessed January 20, 2006).

262 Statement of Mr. Daniel Therrien, Senior General Counsel, Department of Justice, to the Senate Special Committee on the *Anti-terrorism Act*, March 21, 2005 at 6:42 [Statement of Mr. Daniel Therrien].

263 The rules on the admissibility of hearsay evidence are complex and beyond the scope of this chapter. At the time of writing, the leading case on hearsay from the Supreme Court is *R. v. Starr*, [2000] 2 S.C.R. 144, 2000 SCC 40.

264 Statement of Mr. Daniel Therrien at 6:42.

265 This official will be a member of the Case Management Branch: Canada, CIC, "Policy PP 3 – Pre-removal Risk Assessment (PPRA)," December 14, 2005, para. 14.2.

266 Statement of Mr. Daniel Therrien at 6:42.

267 Canada, CIC, "Policy PP 3 – Pre-removal Risk Assessment (PRRA)," December 14, 2005, para. 14.2.

268 Statement of Mr. Daniel Therrien at 6:42. This official is the Director, Case Management Branch: CIC Policy PP 3 – Pre-removal Risk Assessment, December 14, 2005, para. 14.2.

269 *IRPA*, s. 80.

270 Canada, CIC, "PP 3 – Pre-removal Risk Assessment (PPRA)," December 14, 2005, s. 15.

271 Canada, Citizenship and Information, "IN 1, Overview of Information Sharing," (Ottawa: CIC, 2005) at 7 [Memorandum IN 1].

272 CIC-RCMP Cooperation MOU; Memorandum *of Understanding* between CIC and CSIS, February 4, 2002 [CIC-CSIS MOU]. CSIS is legally mandated to provide advice to the Minister of Citizenship and Immigration regarding criminal or security matters relating to immigration: *CSIS Act*, s. 14. Since the CIC-RCMP MOU was negotiated before the government reorganization that created the CBSA, CIC, the CBSA and the RCMP are negotiating bilateral MOUs.

273 CIC-RCMP Cooperation MOU, s. 12.

274 *Statement of Mutual Understanding on Information Sharing,* Department of Citizenship and Immigration Canada, the U.S. Immigration and Naturalization Service and the U.S. Department of State, 2003, arts. 4c. and d., online, http://www.cic.gc.ca/english/policy/smu/smu-ins-dos.html (accessed January 18, 2006) [SMU]; Memorandum IN 1, p. 13. Guidance on the interpretation of the agreement can be found in Canada, *Directives for Sharing Information pursuant to the 2003 Canada-U.S. SMU on Information Sharing*, Policy Statement updated May 12, 2005, online, Citizenship and Immigration, http://www.cic.gc.ca/manuals-guides/english/in/in02e.pdf (accessed January 18, 2006) [*Information Sharing Directive*]. The *Canada-US Information Sharing Understanding* provides that its terms shall be reviewed after five years: art. 13.

275 SMU, arts. 2, 3.

276 Ibid., art. 4.

277 Ibid., art. 4f.

278 I have discussed the restrictions on information sharing in the *Privacy Act* earlier in this chapter. Readers should note that s. 8 of the *Privacy Act* generally allows information to be shared for national security purposes.

279 SMU, art. 5.

280 Ibid., art. 6(c)(ii).

281 Ibid., art. 6(c)(ii).

282 Ibid., art. 6(c)(ii).

283 Ibid., art. 10. Canadian officials are required to notify any U.S. entities that have been given information of any corrections, changes or deletions: *Information Sharing Directive*, p. 7.

284 *Annex Regarding the Sharing of Information on Asylum and Refugee Status Claims to the Statement of Mutual Understanding on Information Sharing*, 2003, online, Citizenship and Immigration, http://www.cic.gc.ca/english/policy/smu/smu-ins-annex1.html (accessed August 10, 2006) [SMU Annex].

285 SMU Annex, arts. 5, 6.

286 Ibid., art. 7(c).

287 Ibid., art. 3.

288 Ibid., art. 7(d).

289 *Concept of Operations US-Canada Terrorist Watch List Program (CONOPS)*, signed May 23, 1997 [TUSCAN/TIPOFF Aide-Memoire]. This agreement is summarized in Memorandum IN 1, p. 13.

290 *Agreement Between the Government of Canada and the Government of the United States of America for Cooperation in the Examination of Refugee Status Claims From Nationals of Third Countries*, December 5, 2002 (entered into force December 29, 2004).

291 *Information Sharing Directive*, p. 4.

292 Ibid., pp. 3–4.

293 Ibid., pp. 6–7.

294 For general information on Transport Canada and its mandate, see "What We Do," online, Transport Canada, http://www.tc.gc.ca/aboutus/whatwedo.htm (accessed December 13, 2005) [Transport Canada website].

295 Transport Canada website.

296 These security clearances are governed by the *Aeronautics Act*, s. 4.8.

297 The other members of the Working Group are CSIS, the RCMP, the CBSA, DND, the Coast Guard/DFO, DFAIT, PCO, PSEPC, the Department of Justice, Environment Canada, Defence Research and Development Canada, the Department of Finance, the Treasury Board, the Canadian Space Agency and the Canadian Food Inspection Agency. Other departments and agencies (e.g., CIC) participate in the Working Group when their mandates involve them in marine security matters.

See also Transport Canada, Backgrounder, "Highlights of New Marine Security Initiatives" (Nov. 16, 2004), online, Transport Canada, http://www.tc.gc.ca/mediaroom/backgrounders/b03-M001.htm (accessed January 25, 2006).

298 More information on the Interdepartmental Marine Security Working Group and the Marine Security Operation Centres can be found in the section of this chapter on the Canadian Coast Guard.

299 See Transport Canada, News Release, GC No. 001/05, "Government of Canada Announces New Marine Security Initiatives" (April 22, 2005), online, Transport Canada, http://search2.tc.gc.ca/mediaroom/releases/releases.asp?region=-1&selModes=0&Year=&Show=1000 (accessed January 26, 2006) [Marine Security Initiatives News Release].

300 Maritime domain awareness refers to Canada's ability to understand what is happening over, under, in and near its waters.

301 The list of other departments and agencies that will receive intelligence and/or information from MSOCs, and the precise relationship between MSOCs on the one hand and IBETs or INSETs on the other is still being developed at the time of writing.

See also Canadian Coast Guard, Marine Communications and Traffic Services; Canada, Department of Fisheries and Oceans, *Marine Programs' National Performance Report for 2003–2004, Marine Communications and Traffic Services* (Ottawa: Public Works and

Government Services Canada Canada, 2003), online, Canadian Coast Guard, http://www.ccg-gcc.gc.ca/mp-pm/docs/03-04/pr/pdf_e.htm (accessed January 26, 2006).

302 *Securing an Open Society: One Year Later*, p. 34.

303 The interim Great Lakes–St. Lawrence Seaway MSOC is expected to operate until mid-2008. In the meantime, planning will take place to create a fully functional MSOC that also includes representatives from the CBSA, Transport Canada and the Coast Guard.

304 *Securing an Open Society: One Year Later*, p. 34.

305 The RCMP is currently studying the project to determine what RCMP information, if any, can be stored in MIMDEX.

306 Interdepartmental Marine Security Working Group, "Canada's Marine Transportation System," online, Canadian Navy, Jan. 12, 2004 http://www.marine.gc.ca/cms_strat/strat-issues_e.asp?id=301 (accessed November 2, 2006).

307 *Aeronautics Act*, s. 4.8.

308 Transport Canada is also developing a mechanism to hear complaints from employees who are denied security clearance to work in restricted or sensitive areas in airports on the basis of adverse security information.

309 Canada, Senate, *Proceedings of the Special Senate Committee on the Anti-terrorism Act*, 38th Parl. (14 November 2005) (testimony of the Honourable Jean Lapierre, Minister of Transport) at 19:33, online, Parliament of Canada, http://www.parl.gc.ca/38/1/parlbus/commbus/senate/Com-e/anti-e/pdf/19issue.pdf (accessed December 13, 2005) [Testimony of Minister of Transport]. In relation to security clearances for port workers, see also Transport Canada, "Information Package on the Proposed Marine Transportation Security Clearance Program (MTSCP)," online, Transport Canada, http://www.tc.gc.ca/MarineSecurity/Regulatory/Initiatives/Info_package.pdf (accessed April 12, 2006).

310 See Transport Canada and the Ministry of Public Safety and Emergency Preparedness, "Press Release: Government of Canada Moving Forward on Air Passenger Assessment," Aug. 5, 2005, online, Transport Canada, http://www.tc.gc.ca/mediaroom/releases/nat/2005/05-gc009e.htm (accessed December 13, 2005).

311 *Aeronautics Act*, s. 4.76.

312 Testimony of Minister of Transport at 19:30 and 19:44. See also http://www.tc.gc.ca/mediaroom/releases/nat/2006/06-gc014e.htm (accessed Oct. 30, 2006).

313 I have described API/PNR information in detail in the section of this chapter on the CBSA.

314 *Aeronautics Act*, s. 4.81. The CBSA automatically receives Advance Passenger Information (including name, passport and citizenship information) for all flights into Canada; Transport Canada, however, must request information.

315 *Aeronautics Act*, s. 4.81.

316 See testimony of Ward Elcock, Director of CSIS, before the House of Commons Committee on Bill C-17, the *Public Safety Act*, December 5, 2002 and February 13, 2003, and testimony of Commissioner Giuliano Zaccardelli, Royal Canadian Mounted Police, before the House of Commons Committee on Bill C-17, the *Public Safety Act*, December 5, 2002, and February 13, 2003, online, www.parl.gc.ca (accessed May 6, 2006). On February 13, 2003, Mr. Elcock indicated that CSIS would be creating a separate, computerized watch list against which to match this data.

317 *Aeronautics Act*, ss. 4.82(2)–(3).

318 Ibid., s. 4.82.

319 Testimony of Ward Elcock, Director of CSIS, before the House of Commons Committee on Bill C-17, the *Public Safety Act*, February 13, 2003.

320 Ibid.

321 *Aeronautics Act*, s. 4.82(4)–(5).

322 Testimony of Wayne Easter, Solicitor General of Canada, before the House of Commons Committee on Bill C-17, the *Public Safety Act*, December 5, 2002; Testimony of Commissioner Giuliano Zaccardelli, Royal Canadian Mounted Police, before the House of Commons Committee on Bill C-17, the *Public Safety Act*, December 5, 2002 and February 13, 2003.

323 *Aeronautics Act*, s. 4.82(1)(*a*).

324 Ibid., ss. 4.82(1)(*b*) and (*c*), respectively.

325 Testimony of Wayne Easter, Solicitor General of Canada, Mr. Ward Elcock, Director of CSIS, Commissioner Giuliano Zaccardelli, Royal Canadian Mounted Police, before the House of Commons Committee on Bill C-17, the *Public Safety Act*, February 13, 2002, online, www.parl.gc.ca (accessed May 6, 2006); Library of Parliament – Parliamentary Information and Research Services, *Bill C-7: The Public Safety Act, 2002*, February 12, 2004 (LS-463E), para. K, online, Library of Parliament, http://www.parl.gc.ca/common/bills_ls.asp?Parl=37&Ses=3&ls=c7#bministerialtxt (accessed December 13, 2005).

326 S.C. 2004, c. 15.

327 *Canadian Air Transport Security Authority Act*, S.C. 2002, c. 9, s. 4 [*CATSA Act*]. The Act requires the Minister to complete a five-year review of CATSA by 2007 and present the report to Parliament.

328 CATSA's general mandate is found at s. 6 of the *CATSA Act*.

329 CATSA does not screen for explosives at every airport in Canada; however, the 89 designated airports cover 99 percent of air travellers in Canada: Canada, Canadian Air Transport Security Authority, *The Canadian Air Transport Security Authority: An Overview*, online, "Mandate," Canadian Air Transport Security Authority, http://www.catsa-acsta.gc.ca/english/about_propos/mandat.pdf (accessed December 14, 2005); Canada, Senate, *Proceedings of the Special Senate Committee on the Anti-terrorism Act*, 38th Parl. (14 November 2005) (testimony of Jacques Duchesneau, CEO, Canadian Air Transport Security Authority) at 19:47, online, Parliament of Canada, http://www.parl.gc.ca/38/1/parlbus/commbus/senate/Com-e/anti-e/pdf/19issue.pdf (accessed December 13, 2005) [Testimony of Jacques Duchesneau, CEO of CATSA]

330 Ibid.

331 *CATSA Act*, s. 8.

332 The authority to hire contractors to provide screening services is found in the *CATSA Act*, s. 7.

333 For example, CATSA does not screen for forged passports or other fraudulent identity documents: Testimony of Jacques Duchesneau, CEO of CATSA at 19:47.

334 *Aeronautics Act*, s. 4.81. If s. 4.82 of the *Aeronautics Act* is brought into force, it will allow designated RCMP and CSIS officers to share information about individual passengers with CATSA if they reasonably believe that the information is relevant to transportation security.

335 *CATSA Act*, s. 9.

336 *Criminal Code*, as amended at s. 494.

337 Ibid., s. 494(3).

338 *Aeronautics Act*, s. 4.81.

339 See Transport Canada, Backgrounder, "Transfer of Canadian Coast Guard Responsibilities from the Department of Fisheries and Oceans to Transport Canada" (February 2005), online, Transport Canada, http://www.tc.gc.ca/mediaroom/includes/printable_backgrounder.asp?lang=eng (accessed January 25, 2006) [Transfer of Coast Guard Responsibilities Backgrounder].

340 Canada, *Government Response to the First Report of the Standing Committee on Fisheries and Oceans on the Canadian Coast Guard, entitled "Safe, Secure, Sovereign: Reinventing the Canadian Coast Guard,"* recommendations 17 and 18, online, Parliament of Canada, http://www.parl.gc.ca/committee/CommitteeList.aspx?Lang=1&PARLSES=381&JNT=0&SELID=

e8_&COM=0 (accessed January 26, 2006). Both the House of Commons Standing Committee on Fisheries and Oceans and the Standing Senate Committee on National Security and Defence have studied the activities and responsibilities of the Coast Guard in recent years. See: House Committee Report on MCTS; Canada, House of Commons, *Safe, Secure, Sovereign: Reinventing the Canadian Coast Guard, Report of the Standing Committee on Fisheries and Oceans* (March 2004), online, Parliament of Canada, http://www.parl.gc.ca/committee/CommitteeList.aspx?Lang=1&PARLSES=381&JNT=0&SELID=e8_&COM=0#TOC (accessed January 26, 2006); Canada, Senate, Standing Committee on National Security and Defence, *Canada's Coastlines: The Longest Under-Defended Borders in the World* (October 2003), online, Parliament of Canada, http://www.parl.gc.ca/common/Committee_SenRep.asp?Language=E&Parl=38&Ses=1&comm_id=76 (accessed January 26, 2006).

341 *Securing an Open Society: Canada's National Security Policy*, p. 38.

342 Fisheries and Oceans Canada, Backgrounder, "RCMP and Canadian Coast Guard Launch Joint Partnership on the Great Lakes and St. Lawrence River" (July 2005), online, Department of Fisheries and Oceans, http://www.dfo-mpo.gc.ca/media/backgrou/2005/hq-ac66a_e.htm?template=print (accessed January 25, 2006) [DFO Backgrounder].

343 See RCMP, News Release, "RCMP-Canadian Coast Guard Begin Joint Marine Security patrols on Great Lakes and St. Lawrence Seaway" (July 11, 2005), online, Royal Canadian Mounted Police, http://www.rcmp-grc.gc.ca/news/adv_0509_e.htm (accessed January 26, 2006) [RCMP-CG Joint Patrols News Release]; Fisheries and Oceans Canada, News Release, "RCMP and Canadian Coast Guard Begin Joint Marine Security Patrols Along Great Lakes and St. Lawrence Seaway" (July 13, 2005), online, Department of Fisheries and Oceans, http://www.dfo-mp.gc.ca/media/newsrel/2005/hq-ac66_e.htm?template=print (accessed January 25, 2006).

344 RCMP, "National and Border Security," online, Royal Canadian Mounted Police, http://www.rcmp-grc.gc.ca/qc/pro_ser/sec_nat_front_e.htm (accessed January 25, 2006); DFO Backgrounder.

345 These vessels are identified in the *Vessel Traffic Services Zones Regulations*, S.O.R./89-98, passed under the *Canada Shipping Act*, R.S.C. 1985, c. S-9.

346 See Canada, House of Commons, *Canadian Coast Guard Marine Communications and Traffic Services, Report of the Standing Committee on Fisheries and Oceans* (February 2003), online, Parliament of Canada, http://www.parl.gc.ca/committee/CommitteeList.aspx?Lang=1&PARLSES=381&JNT=0&SELID=e8_&COM=0#TOC (accessed January 26, 2006) [Commons Committee Report on MCTS]; Canadian Coast Guard, "Marine Communications and Traffic Services, General Information," online, http://www.ccg-gcc.gc.ca/mcts-sctm/docs/misc/general_e.htm (accessed January 25, 2006) [Canadian Coast Guard, Marine Communications and Traffic Services]; Transfer of Coast Guard Responsibilities Backgrounder; Marine Security Initiatives News Release; Capt. Peter Avis, "Surveillance and Canadian Maritime Domestic Security, online, Canadian Navy, http://www.navy.forces.gc.ca/mspa_news/news_issues_e.asp?category=4&title=14 (accessed January 26, 2006); Larry Murray, Deputy Minister, Department of Fisheries and Oceans, "Canada's Oceans: Maximizing Opportunities for Canadians from a Sovereignty and Security Perspective" (Presentation to the Centre for Foreign Policy Studies Conference, "What Canadian Military and Security Forces in the Future World? A Maritime Perspective," June 10–12, 2005), online, Canadian Naval Review, http://naval.review.cfps.dal.ca/pdf/canadasoceansmurray.pdf (accessed January 26, 2006).

347 S.C. 2001, c. 41.

348 *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, S.C. 2000, c. 17, s. 2 [*PCMLTFA*].

349 Ibid., s. 40(*a*).

350 Ibid., s. 40(*c*).

351 Ibid., s. 54.

352 Ibid., s. 54(*a*).

353 Canada, Senate, *Proceedings of the Senate Special Committee on the Anti-terrorism Act*, 38th Leg., (Apr. 18, 2005), Testimony of Horst Intscher, Director, FINTRAC at 8:8-8:9, online, Parliament of Canada, http://www.parl.gc.ca/38/1/parlbus/commbus/senate/Com-e/anti-e/pdf/08issue.pdf (accessed January 23, 2006) [Testimony of Horst Intscher].

354 For a description of the terrorist entity listing process under s. 83.1 of the *Criminal Code*, see the section of this chapter on the Department of Public Safety and Emergency Preparedness.

355 *PCMLTFA*, s. 12; *Cross-border Currency and Monetary Instruments Reporting Regulations*. I have discussed the CBSA's role under the *PCMLTFA* in more detail in the section of this chapter on the CBSA.

356 "Guideline 2: Suspicious Transactions," online, FINTRAC, http://www.fintrac.gc.ca/publications/guide/guide_e.asp (accessed January 23, 2006).

357 Testimony of Horst Intscher at 8:13.

358 *PCMLTFA*, s. 9.

359 Ibid., s. 62.

360 The Police Information Retrieval System, or PIRS.

361 See testimony of Horst Intscher at 8:9; *PCMLTFA*, s. 54(*b*).

362 *PCMLTFA*, s. 54(*b*).

363 Ibid., s. 58.

364 Ibid., s. 36(2).

365 Ibid., s. 55.1.

366 *PCMLTFA*, s. 55(3)(*b*); *Income Tax Act*.

367 *PCMLTFA*, ss. 56, 56.1. These countries include the U.S.A., the U.K., Belgium, Australia, Mexico, Italy, Barbados, the Netherlands, Portugal, the Republic of Korea, El Salvador, Panama, France, Finland, Bulgaria, Denmark, Monaco, Latvia, Cyprus and Guernsey: Canada, Senate, *Proceedings of the Senate Special Committee on the Anti-terrorism Act*, 38th Leg., (Apr. 18, 2005), Testimony of Josée Desjardins, Senior Counsel, FINTRAC at 8:27, online, Parliament of Canada, http://www.parl.gc.ca/38/1/parlbus/commbus/senate/Com-e/anti-e/pdf/08issue.pdf (accessed January 23, 2006). See also Canada, FINTRAC, *FINTRAC Annual Report 2005* (Ottawa: Financial Transactions and Reports Analysis Centre of Canada, 2005), p. 20, online, FINTRAC, http://www.fintrac.gc.ca/publications/annualreport/2005/AR_E.pdf (accessed January 23, 2006) [FINTRAC 2005 Annual Report].

368 Testimony of Horst Intscher at 8:10.

369 *November 2004 Report of the Auditor General of Canada to the House of Commons* (Ottawa: Public Works and Government Services Canada Canada, 2004), para. 2.21 [Auditor General's Report]; Testimony of Horst Intscher at 8:19.

370 *PCMLTFA*, ss. 55.1(2), 55(5.1) and 56.1(4), respectively.

371 See *PCMLTFA*, ss. 55(7), 55.1(3), 56.1(5); and the *Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transactions Reporting Regulations*, S.O.R./2001-317, s. 13.

372 *Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transactions Reporting Regulations*, s. 13.

373 *PCMLTFA*, s. 60. In keeping with the Centre's arm's-length role, disclosure of FINTRAC's case analysis requires the police to establish that there are reasonable grounds to believe that the person about whom disclosure is sought is involved in, or has benefited from, a terrorist-financing or money-laundering offence: *PCMLTFA*, s. 60(3)(*d*). In a parallel process, CSIS can also get judicial authority to access FINTRAC's case analysis: *PCMLTFA*, s. 60.1.

374 *PCMLTFA*, s. 74.

375 Auditor General's Report, paras. 2.2, 2.39.

376 Canada, Department of Finance, *Enhancing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime, Consultation Paper, June 2005* (Ottawa: Department of Finance, 2005), Proposal 4.1 and Proposal 2.2, online, Department of Finance Canada, http://www.fin.gc.ca/toce/2005/enhancing_e.html (accessed January 24, 2006).

377 Canada, Department of Finance, "Budget Plan 2006," Chapter 3, online, Department of Finance, http://www.fin.gc.ca/budget06/bp/bpc3de.htm (accessed May 3, 2006).

378 See *PCMLTFA*, s. 56.1(1) and *Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transactions Reporting Regulations*, S.O.R./2001-317, s. 13.

379 *PCMLTFA*, ss. 56.1(1)(*a*), 56.1(2)(*a*).

380 Ibid., ss. 56(3)(*a*)–(*b*).

381 Ibid., ss. 56, 56.1(1)(*b*), 56.1(2)(*b*).

382 Testimony of Horst Intscher at 8:21; Communication to Policy Review legal counsel, Arar Commission, March 14, 2006.

383 Testimony of Horst Intscher at 8:21.

384 *PCMLTFA*, s. 56.2.

385 S.C. 2001, c. 41, s. 113 [*CRSIA*].

386 *CRSIA*, s. 4.

387 *Subcommittee on Public Safety and National Security of the Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness*, 38th Parl. (May 19, 2005), p. 3 (Statement by Mr. Michel Dorais, Commissioner, Canada Customs and Revenue Agency).

388 *CRSIA*, ss. 6–7.

389 Ibid., ss. 6(*b*), (*e*), (*g*).

390 Ibid., s. 6(*b*).

391 Ibid., ss. 8, 13.

392 Ibid., s. 8(2). If an organization believes that the circumstances that led to a certificate being issued have changed, it may request that the ministers review the certificate and reinstate charitable status (s. 10). The Federal Court can review the reasonableness of the ministers' decision (s. 11).

393 The CRA has bilateral memoranda of understanding with the RCMP and CSIS concerning the transmission of such information.

394 Registered charities and organizations seeking registration are technically taxpayers under the *Income Tax Act*.

395 *Subcommittee on Public Safety and National Security of the Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness*, 38th Parl. (May 19, 2005), p. 3 (Statement by Ms. Elizabeth Tromp, Director General, Charities Directorate, Policy and Planning Branch, Canada Customs and Revenue Agency) [Statement of Ms. Elizabeth Tromp].

396 *Income Tax Act*, s. 241(4)(*f.1*).

397 Ibid., s. 241. See also *R. v. Ling*, [2002] 3 S.C.R. 814 [*Ling*]; *R. v. Jarvis*, [2002] 3 S.C.R. 757 [*Jarvis*]; Canada, Department of Finance, *Enhancing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime*, Consultation Paper, June 2005, p. 24, online, Department of Finance Canada, http://www.fin.gc.ca/toce/2005/enhancing_e.html (accessed January 19, 2006) [Consultation Paper].

The confidentiality provisions of the *Income Tax Act* also apply to the CRA's participation in RCMP-led Integrated Proceeds of Crime units, which I have discussed earlier in this chapter in relation to the CBSA.

398 *Income Tax Act*, s. 241(3)(*a*). The RCMP cannot execute a search warrant on the CRA prior to the laying of charges: See *Ministry of Natural Resources v. Fawcett (Justice of the Peace)*, [1988]

2 C.T.C. 62 (B.C.S.C.); Communication from the CRA to Policy Review legal counsel, May 3, 2006.

399 *Income Tax Act*, s. 241(4)(*e*)(v). The judge's order must be made under s. 462.48(3) of the *Criminal Code*.

400 *Criminal Code*, s. 462.48 (1.1)(*d*).

401 *Income Tax Act*, s. 241(*e*)(iv); *CSIS Act*, s. 21(3).

402 *Income Tax Act,* s. 241(3.2). This section sets out the publicly available information about registered charities.

403 Ibid., s. 241(3)(*b*).

404 Ibid., s. 241(3.1).

405 Department of Foreign Affairs and International Trade Act, R.S.C. 1985, c. E-22, as amended, s. 10.

406 There are many international treaties relating to acts of terrorism. Some of the principal treaties to which Canada is a party are the following:

- *International Convention for the Suppression of Acts of Nuclear Terrorism, 14 September 2005, A/RES/59/290, online, http://untreaty.un.org/English/Terrorism/English_18_15.pdf (accessed July 11, 2006);*
- *Inter-American Convention Against Terrorism, June 3, 2002, Bridgetown;*
- *International Convention for the Suppression of the Financing of Terrorism, 9 December 1999, C.T.S. 2002/9, online, http://untreaty.un.org/English/Terrorism/Conv12.pdf (accessed July 11, 2006);*
- *International Convention for the Suppression of Terrorist Bombings, 15 December 1997, A/RES/52/164, online, http://untreaty.un.org/English/Terrorism/Conv11.pdf (accessed July 11, 2006);*
- *Convention on the Marking of Plastic Explosives for the Purpose of Detection, 1 March 1991, 1678 U.N.T.S. 304, online, http://www.unodc.org/unodc/en/terrorism_convention_plastic_explosives.html (accessed July 11, 2006);*
- *Protocol to the Convention for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf, 10 March 1988, 1678 U.N.T.S. 201, online, http://untreaty.un.org/English/Terrorism/Conv8.pdf (accessed July 11, 2006);*
- *Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, 10 March 1988, 1678 U.N.T.S. 201, online, http://untreaty.un.org/English/Terrorism/Conv8.pdf (accessed July 11, 2006);*
- *Protocol tor 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, 24 February 1988, 1589 U.N.T.S. 474, online, http://untreaty.un.org/English/Terrorism/Conv7.pdf (accessed July 11, 2006);*
- *Convention on the Physical Protection of Nuclear Material (with annexes), 3 March 1980, 1456 U.N.T.S. 101, online, http://untreaty.un.org/English/Terrorism/Conv6.pdf (accessed July 11, 2006);*
- *International Convention Against the Taking of Hostages, 17 December 1979, 1316 U.N.T.S. 205, online, http://untreaty.un.org/English/Terrorism/Conv5.pdf (accessed July 11, 2006);*
- *Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents, 14 December 1973, 1035 U.N.T.S. 167, online, http://untreaty.un.org/English/Terrorism/Conv4.pdf (accessed July 11, 2006);*
- *Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, 23 September 1971, 974 U.N.T.S. 177, online, http://untreaty.un.org/English/Terrorism/Conv3.pdf (accessed July 11, 2006);*

- *Convention for the Suppression of Unlawful Seizure of Aircraft, 16 December 1970, 860 U.N.T.S. 105,online, http://untreaty.un.org/English/Terrorism/Conv2.pdf (accessed July 11, 2006); and*
- *Convention on Offences and Certain Other Acts Committed on Board Aircraft, 14 September 1963, 704 U.N.T.S. 219, online, http://untreaty.un.org/English/Terrorism/Conv1.pdf (accessed July 11, 2006).*

407 For more information about the Division and its work, see "International Crime and Terrorism," online, Foreign Affairs Canada, http://www.dfait-maeci.gc.ca/internationalcrime/menu-en.asp (accessed January 13, 2006).

408 See "Terrorism," online, Foreign Affairs Canada, http://www.dfait-maeci.gc.ca/internationalcrime/terrorism-en.asp (accessed January 13, 2006).

409 Testimony of Keith Morrill, Director, Criminal, Security and Treaty Law Division, FAC, in Canada, Senate, Proceedings of the Senate Special Committee on the Anti-terrorism Act, 38th Parl. (Mar. 21, 2005) at 6:61.

410 SOR/2001-360 [UNSTR], passed pursuant to the *United Nations Act*, R.S.C. 1985, c. U-2. An entity is listed on the UN list by the UN Security Council 1267 Committee. The UN list is maintained pursuant to several resolutions of the UN Security Council:

- *Security Council Resolution 1267: Resolution 1267 (1999), 15 October 1999, S/Res/1267 (1999), online, United Nations Security Council Resolutions 1999, http://daccessdds.un.org/doc/UNDOC/GEN/N99/300/44/PDF/N9930044.pdf?OpenElement (accessed January 13, 2006);*
- *Security Council Resolution 1333: Resolution 1333 (2000), 19 December 2000, S/Res/1333 (2000), S/Res/1333 (2000), online, UN Security Council Resolutions 2000, http://daccessdds.un.org/doc/UNDOC/GEN/N00/806/62/PDF/N0080662.pdf?OpenElement (accessed January 13, 2006);*
- *Security Council Resolution 1373: Resolution 1373 (2001), 28 September 2001, S/Res/1373 (2001), online, United Nations Office on Drugs and Crime, http://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf (accessed January 12, 2006). Note that this resolution does not create a different list — it requires UN member states to freeze terrorist assets without delay; and*
- *Security Council Resolution 1390: Resolution 1390 (2002), 28 January 2002, S/Res/1390 (2002), online, Security Council Resolutions 2002,* http://daccessdds.un.org/doc/UNDOC/GEN/N02/216/02/PDF/N0221602.pdf?OpenElement (accessed January 13, 2006).

There are two other terrorist entity listing processes in Canada, one under the Criminal Code, which I review in the section of this chapter on the Department of Public Safety and Emergency Preparedness, and a separate process under the Charities Registration (Security Information) Act, which I discuss in relation to the Canada Revenue Agency.

411 *United Nations Afghanistan Regulations*, S.O.R./99-444 [UNAR].

412 *Resolution 1373 (2001)*, S/Res/1373 (2001), online, United Nations Office on Drugs and Crime, http://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf (accessed July 31, 2006).

413 For more information on the UN listing process, see E. Alexandra Dosman, "For the Record: Designating 'Listed Entities' for the Purposes of Terrorist Financing Offences at Canadian Law" (2004) 62(1) U.T. Fac. L. Rev. 1 (QL), paras. 18–32 [Dosman, "For the Record"].

414 UNSTR, s. 1*(a)*.

415 See for example the discussion of the standards used in 2001 by American authorities in the UN listing process in John Roth, Douglas Greenburg & Sarah Wille, *Monograph on Terrorist Financing, Staff Report to the Commission*, National Commission on Terrorist Attacks upon the United States, 2003–2004, pp. 84-85, online, National Commission on Terrorist

Attacks upon the United States, Staff Statements, http://govinfo.library.unt.edu/911/staff_statements/index.htm (accessed January 13, 2006) [*9/11 Commission Staff Monograph*].

416 For a narrative of the events, see *9/11 Commission Staff Monograph*, pp. 84–85. In relation to evidence of the individual's personal involvement in terrorist activities, see *United States of America v. Hussein*, [2001] O.J. No. 5812 at para. 1. The case relates to an American extradition request. Canada subsequently decided not to proceed with the extradition. For the U.S. request to the UN, see U.S. Executive Order 13,224, List 4, "Al Barakaat Entities," November 7, 2001, online, United States Department of the Treasury, http://www.ustreas.gov/rewards/terrorismlist.shtml (accessed March 23, 2006); U.S., The White House, "Terrorist Financial Network Fact Sheet," November 7, 2001, online, White House, http://www.whitehouse.gov/news/releases/2001/11/20011107-6.html (accessed March 23, 2006).

417 S.O.R./2002-210; United Nations, UN News Service, "Canadian Citizen no longer subject to sanctions against Al-Qaida, Security Council Panel Says," July 11, 2002, online, UN News Centre, http://www.un.org/apps/news/printnewsAr.asp?nid=4159 (accessed January 10, 2006).

418 UNSTR, s. 2.

419 *SIRC Annual Report 2004–2005*, p. 5.

420 UNSTR, s. 2(2).

421 Ibid., s. 2(3).

422 Canada, Privy Council Office, *The Canadian Security and Intelligence Community* (Ottawa: Her Majesty the Queen in Right of Canada, 2001), online, Privy Council Office, http://www.pco-bcp.gc.ca/default.asp?Language=E&Page=publications&doc=si/si_text_e.htm#Roles%20and%20Responsibilities (accessed January 13, 2006).

423 Ibid.

424 Exhibit P-12, Tab 50, Arar Commission Factual Inquiry.

425 The Prime Minister's Office, on the other hand, provides partisan, political support to the Prime Minister.

426 I discuss the national security role and functions of the Government Operations Centre in the part of this chapter dealing with the Department of Public Safety and Emergency Preparedness.

427 For more information on the Security and Prosperity Partnership of North America, see http://www.fac-aec.gc.ca/spp/spp-menu-en.asp (accessed March 23, 2006).

428 *Department of Public Safety and Emergency Preparedness Act*, S.C. 2005, c. 10 [*PSEP Act*].

429 *Order Transferring from the Department of National Defence to the Department of the Solicitor General the Control and Supervision of the Office of Critical Infrastructure Protection and Emergency Preparedness*, S.I./2003-229, C. Gaz. II, 31/12/03. See also *Order Designating the Deputy Prime Minister and Minister of Public Safety and Emergency Preparedness as Minister for Purposes of the Act*, S.I./2004-106, C. Gaz. II, 11/8/04.

430 The *PSEP Act* does not yet reflect the new name. However, for the sake of clarity, I will refer to the Minister of Public Safety and Emergency Preparedness by the new title, Minister of Public Safety.

431 *PSEP Act*, ss. 4–5. See also "Who we are," on the PSEPC website, online, http://www.psepc-sppcc.gc.ca/wwa/index-en.asp (accessed January 9, 2006) [PSEPC website, "Who we are"].

432 *PSEP Act*, s. 6(*b*).

433 Ibid., s. 6(*d*).

434 Ibid., s. 5. The Minister is also responsible for the Canadian Firearms Centre and the National Parole Board.

435 PSEPC website, "Who we are."

436 Ibid.

437 "About the National Security Directorate," online, PSEPC, http://ww2.psepc-sppcc.gc.ca/national_security/counter-terrorism/antiterrorism_e.asp (accessed January 9, 2006) [PSEPC

website, "About the National Security Directorate"]; *Securing an Open Society*: *Canada's National Security Policy*; *Securing an Open Society: One Year Later*.

438 Representatives of the Round Table and PSEPC appeared before the Senate Special Committee on the *Anti-terrorism Act* on October 24, 2005. Readers who would like more detail on the role of the Round Table and some of the criticisms levelled against it can refer to the transcripts of the Senate hearings, available online at http://www.parl.gc.ca/38/1/parlbus/commbus/senate/Com-e/anti-e/pdf/17issue.pdf, at pp. 17:34ff.

439 I discuss the charities certificate procedure in relation to the Canada Revenue Agency in the section of this chapter dealing with the CRA.

440 *IRPA*, ss. 77ff. I describe the security certificate process in the section of this chapter dealing with the CBSA.

441 The security certificate process exists under ss. 76–85 of the *Immigration and Refugee Protection Act*. A detailed description of the process can be found on the CBSA website, "Security Certificates under the *Immigration and Refugee Protection Act*," online, http://www.cbsa-asfc.gc.ca/newsroom/factsheets/2005/certificat-e.html (accessed January 4, 2006).

442 The list of terrorist entities and a description of the various groups is available at http://www.psepc-sppcc.gc.ca/prg/ns/le/cle-en.asp (accessed January 9, 2006). For a description of the *Criminal Code* listing process, focusing on CSIS' involvement in the process, see SIRC's 2004–2005 annual report, pp. 4–10.

443 *Criminal Code*, ss. 83.05(1) and (1.1). The names of these entities are listed in the *Regulations Establishing a List of Entities,* S.O.R./2002-284, as amended.

444 *Criminal Code*, s. 83.05(2).

445 Ibid., ss. 83.05(5) and (6).

446 Ibid., ss. 83.05(9) and (10).

447 Ibid., s. 83.14.

448 Ibid., s. 83.08.

449 Ibid., Part II.1, "Terrorism," ss. 83.01–83.27.

450 S.O.R./2001-360, passed under the *United Nations Act*. An entity is listed on the UN list by the UN Security Council Committee created by UNSCR 1267.

451 S.O.R./99-444, passed under the *United Nations Act*.

452 For a critical comparison of the listing processes under the *Criminal Code* and the UNSTR, see Dosman, "For the Record."

453 Department of Foreign Affairs and International Trade, "Smart Border Action Plan Status Report, December 17, 2004," #25, online, Department of Foreign Affairs and International Trade, http://www.dfait-maeci.gc.ca/can-am/main/border/smart_border_12_17_04-en.asp (accessed January 27, 2006).

454 *Securing an Open Society: One Year Later*, p. 28. The regulations creating the Public Health Agency are *Order Designating the Public Health Agency of Canada as a Department and the Chief Public Health Officer of Canada as Deputy Head*, S.I./2004-124 and *Order Transferring from the Department of Health to the Public Health Agency of Canada the Control and Supervision of the Population and Public Health Branch and Ordering the Minister of Health to Preside Over the Agency*, S.I./2004-123.

455 For more information on the national security role of the Public Health Agency of Canada, see the Agency's website at http://www.phac-aspc.gc.ca/ep-mu/bioem_e.html (accessed February 3, 2006).

456 For more information on this system, see Public Health Agency of Canada, News Release, "Global Public Health Intelligence Network" (November 2004), online, Public Health Agency of Canada, http://www.phac-aspc.gc.ca/media/nr-rp/2004/2004_gphin-rmispbk_e.html (accessed February 3, 2006).

457 For more information on the Centre for Emergency Preparedness and Response, see the Centre's website at http://www.phac-aspc.gc.ca/cepr-cmiu/index.html (accessed February 3, 2006). For more information on the public health component of Canada's National Security Policy, see *Securing an Open Society: Canada's National Security Policy*, pp. 29–34, and *Securing an Open Society: One Year Later*, pp. 27–32.

458 Public Safety and Emergency Preparedness Canada, *The Chemical, Biological, Radiological and Nuclear Strategy of the Government of Canada* (Ottawa: Public Works and Government Services Canada, 2005) [CBRN Strategy].

459 S.C. 1999, c. 33.

460 R.S.C. 1985, c. E-17.

461 C.R.C., c. 599.

462 Privy Council Office Background Document. For more information about Natural Resources Canada, see the department's website at http://www.nrcan.gc.ca (accessed February 5, 2006). More information on the department's mapping and charting role is available at http://www.geoconnections.org/CGDI.cfm/fuseaction/cgdiServices.welcome/gcs.cfm (accessed February 5, 2006).

463 More information about this initiative is available online at Canadian Research and Technology Initiative, http://www.crti.drdc-rddc.gc.ca/en/default.asp (accessed April 6, 2006).

464 More information about the Nuclear Safety Commission's security activities is available online at http://www.nuclearsafety.gc.ca (accessed February 5, 2006).

465 CBRN Strategy, p. 8.

466 However, jurisdiction over these offences is shared with the provincial attorneys general.

467 Communication to Policy Review legal counsel from the Department of Justice, March 22, 2006.

468 R.S.C. 1985, c. O-5.

469 Ibid., c. A-1.

470 Ibid., c. P-21.

471 *Security of Information Act*, s. 24.

472 Treasury Board of Canada Secretariat, "Government Security Policy — Operational Standard for the Security of Information Act" (March 2003), online, http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/sia-lpi1_e.asp#effe (accessed July 31, 2006) [Government Security Policy].

473 Canada, Senate, *Proceedings of the Senate Special Committee on the Anti-terrorism Act*, 38th Leg., (May 30, 2005); Testimony of the Hon. Reg Alcock, President of the Treasury Board of Canada at 12:70. At the Senate hearings, The Hon. Reg Alcock discussed the risk that Canadians' personal information would be disclosed or disclosable to American authorities as a result of the provisions of the *U.S.A. Patriot Act*: *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*, Pub. L. No. 107-56, 115 Stat. 272. For more information on the potential effects of the *USA Patriot Act* on the disclosure of Canadians' personal information, see British Columbia, Office of the Information and Privacy Commissioner, *Privacy and the USA Patriot Act, Implications for British Columbia Public Sector Outsourcing* (Victoria: Office of the Information and Privacy Commissioner, 2004), online, Office of the Information and Privacy Commissioner for British Columbia, http://www.oipcbc.org/sector_public/usa_patriot_act/pdfs/report/privacy-final.pdf (accessed February 6, 2006).

474 Canada, Senate, *Proceedings of the Senate Special Committee on the Anti-terrorism Act*, 38th Leg., (May 30, 2005), Testimony of Donald Lemieux, Senior Director, Treasury Board of Canada at 12:88.

475 Ibid., Testimony of Helen McDonald, Chief Information Office, Treasury Board of Canada at 12:91-92.

476 Government Security Policy.

477 Ibid.

478 *Security Offences Act*, R.S.C. 1985, c. S-7, s. 6.

479 For example, the RCMP and the Ontario Provincial Police (OPP) have concluded a memorandum of understanding stipulating the roles and responsibilities of the OPP and municipal police forces in relation to offences that fall under RCMP jurisdiction: Oral submissions of Commissioner Gwen Boniface, Ontario Provincial Police, Transcript of Arar Commission Policy Review Public Hearing (November 18, 2005), p. 640 [Boniface, Transcript].

480 Boniface, Transcript, pp. 637–38.

481 Ibid., p. 638.

482 Except where otherwise noted, information in this section is based upon on meetings and communications between Policy Review Legal Counsel and the OPP, the Toronto Police Service, the CACP and the Ottawa Police service regarding the national security activities of provincial and municipal police forces.

483 INSETs (Integrated National Security Enforcement Teams) and IBETs (Integrated Border Enforcement Teams).

484 Boniface, Transcript, p. 678.

485 Oral submissions of Commissioner Giuliano Zaccardelli, RCMP, Transcript of Arar Commission Policy Review Public Hearing (November 18, 2005), p. 706 [Zaccardelli, Transcript].

486 Zaccardelli, Transcript, p. 709.

487 Oral submissions of Chief Vince Bevan, Ottawa Police Service, Transcript of Arar Commission Policy Review Public Hearing (November 18, 2005), p. 707 [Bevan,Transcript].

488 Bevan, Transcript, p. 708.

489 See Chapter IV, Section 6.2.2.

490 Bevan, Transcript, p. 656.

491 See, for example, *Ontario Police Services Act*, R.S.O. 1990, c. P.15, ss. 1 and 42. Local police forces will also be subject to provincial ministerial directives, policies and agreements. They may also be party to provincial response, support and mutual aid agreements carrying a host of obligations.

492 *Security Offences* Act, s. 2(*b*).

493 Police participants included members from the RCMP, the Edmonton Police Service, Camrose Police Service, Lacombe Police Service, Medicine Hat Police Service, Lethbridge Regional Police Service, Moose Jaw Police Service, Estevan Police Service, OPP, Toronto Police Service, Peel Regional Police and Waterloo Regional Police Service.

494 "Submission of the Canadian Association of Chiefs of Police" (Written submission, Arar Commission Policy Review Public Submissions), March 11, 2005, pp. 6, 7 [CACP written submission]. Integrated organized crime teams also exist in several provinces. Given the fine line between ordinary criminal activity and criminal activity relating to national security, it is possible that a national security investigation could grow out of the organized crime mandates of these teams.

495 CACP written submission, p. 7.

496 *Police Act*, R.S.Q. c. P-13.1, Schedule G; Communication from CACP.

497 R.S.B.C. 1996, c. 367.

498 CACP written submission, pp. 8, 9.

499 Bevan, Transcript, p. 650.

500 For example, the Province of Quebec is currently preparing to enter into an arrangement to allow Quebec police services to access the Portal.

501 The TPS advises that it logs all the information it provides to CSIS.

502 In relation to disclosure requirements, see *R. v. Stinchcombe*, [1991] 3 S.C.R. 326.

VI
Review of National Security Activities: The Canadian Experience

1. INTRODUCTION

In this chapter, I outline the Canadian experience with review of national security activities. I begin by describing review mechanisms for a number of law enforcement agencies in Canada. This is of obvious relevance to the review of RCMP law enforcement activities related to national security. Next, I examine the Canadian experience with review of the activities of security intelligence agencies. This is pertinent for two reasons. To begin with, it is instructive to examine review bodies focused on national security. In addition, given the increased integration of RCMP national security policing with agencies such as CSIS and the Communications Security Establishment (CSE), such an examination is helpful for understanding how a review mechanism for the RCMP's national security activities should interact with other review mechanisms. In the last part of the chapter, I examine other existing federal accountability mechanisms: the Auditor General of Canada, Privacy Commissioner of Canada, Information Commissioner of Canada and Canadian Human Rights Commission. These mechanisms do not focus on any particular institution or activity, but review activities across the federal government, and their mandates include or touch on the national security activities of the RCMP and other Canadian national security actors.

2. LAW ENFORCEMENT REVIEW BODIES

2.1 POLICE COMPLAINTS BODIES

In the 1980s, bodies independent of the police were established across Canada to review how the police handled complaints from the public. A background paper produced by the Commission[1] provides an overview of experience with review of police complaints in all provinces and territories. Here, I focus on the existing complaints body for the RCMP, the Military Police Complaints Commission of Canada and certain provincial bodies (in Ontario, Quebec and British Columbia) that provide some of the more significant policy alternatives to the present federal models.

2.1.1 Commission for Public Complaints Against the RCMP (CPC)

Before 1988, there was no civilian oversight of investigations into public complaints against the RCMP, or of any discipline applied by the Force. The first RCMP directive on public complaints, issued in 1964, stated that "[a] complaint against the Force or a member shall be investigated immediately."[2] This led to the promulgation of RCMP standing orders relating to public complaints. At the time, there were also provisions for external investigations, such as that conducted by the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, known as the McDonald Commission, as well as for criminal charges or civil actions against RCMP officers.

The Commission for Public Complaints Against the RCMP (CPC) was established in 1988 primarily to review the Force's handling of complaints, although it was given the power to initiate complaints in exceptional cases.[3] As will be seen, this model departed from recommendations made by the McDonald Commission for a more robust review body for the RCMP — one that would not be limited to reviewing the Force's handling of public complaints.

2.1.1.1 Marin and McDonald Commission Reports

Two important federal studies led to the creation of the CPC in 1988. The first was by the Commission of Inquiry Relating to Public Complaints, Internal Discipline and Grievance Procedure within the Royal Canadian Mounted Police, chaired by Judge René J. Marin (Marin Commission), which reported in 1976.[4]

The second was by the McDonald Commission, mentioned above, which reported in 1981.[5]

The Marin Commission report focused on public complaints against the RCMP. Judge Marin recommended that the RCMP generally investigate and adjudicate complaints against the Force. This emphasis on internal investigation and adjudication departed from certain other reform proposals of the day, but was motivated by the idea that "management must retain initial responsibility for action in this and all other aspects of public complaint procedures."[6] Judge Marin did propose a new outside review authority, the Federal Police Ombudsman, who would become involved only after the RCMP had completed its internal investigation and discipline process. Appeals by dissatisfied complainants or members of the Force who had a grievance or were disciplined by the Force would be heard by the Ombudsman, who would be appointed for a fixed term by Parliament and be responsible to it.[7]

Judge Marin envisioned that the Ombudsman would have general powers of oversight of the public complaints process. The Ombudsman would not only provide a "review of any particular complaint" and "appoint tribunals to hold hearings convened for the purpose of determining the merits of a complaint,"[8] but would also have responsibility for "ascertaining that all complaints [were] investigated in an appropriate matter."[9] Further, the Ombudsman would have responsibility for "recommending such remedial action as he believe[d] necessary at both the individual and organizational level."[10] He or she would be given all of the authority vested in a commissioner appointed pursuant to the *Inquiries Act*. According to Judge Marin, "[w]ithout full powers of inquiry, the ombudsman would be unable to fulfill his role as a watchman on behalf of Parliament."[11]

The Ombudsman proposed by Judge Marin would not have the power to impose discipline. That would remain with the RCMP. However, in Judge Marin's view, the Ombudsman's annual and other reports and the publicity generated by the publication of findings would help ensure that the process was fair to complainants and individual officers.

In 1978, the federal government introduced legislation to establish a federal ombudsman to handle complaints arising in all federal departments and agencies, including the RCMP,[12] something Judge Marin had recommended against:

> [T]he Federal Police Ombudsman should not be subsumed by an Ombudsman with a more general mandate. The size and geographic distribution of the Force, the multiplicity of its duties as federal, provincial and municipal police, as well as the nature and visibility of its contact with the public, indicate the need for the services of a specialized ombudsman.[13]

In any event, the bill respecting the federal ombudsman died on the order paper[14] and legislation in this respect was never enacted. One result of the Marin Report was that, at the end of 1978, the RCMP established a unit called the Complaints Section within its Internal Affairs Branch at Headquarters to receive complaints and forward them to the appropriate regions.[15]

The McDonald Commission agreed that there should be a specialized external review body, but went further than the Marin recommendations. It wrote:

> [W]e believe the institution of the Ombudsman would not go far enough in meeting the needs we have identified. Our view is that the work of an external review body should go beyond the traditional role of the Ombudsman of responding to individual complaints and should involve a continuing review of the adequacy of the R.C.M.P.'s practices. Such matters, we feel, should be within the mandate of an external body charged not only with reviewing the R.C.M.P.'s disposition of complaints, but also with identifying problems within the R.C.M.P. which may have contributed to the incidents in question.[16]

In other words, the McDonald Commission concluded that effective review of the RCMP's national security activities would require more than monitoring of the Force's handling of individual complaints.

The Commission recommended the establishment of the Office of Inspector of Police Practices, modeled on the Office of Professional Responsibility that had recently been created in the Attorney General's Department in the United States to oversee the FBI's activities.[17] The Office would be within the Department of the Solicitor General and the Inspector would be appointed by Cabinet for a renewable five-year term.[18] The RCMP would retain initial responsibility for handling complaints,[19] but the Inspector would have the power to investigate complaints for the purpose of carrying out his or her mandate.[20] As will be seen, this is similar to the power of the Chair of the CPC to conduct "public interest" investigations.

The McDonald Commission envisioned a further role for the Office:

> In addition to its investigatory role, the Office of the Inspector of Police Practices should have a second function — that of monitoring the R.C.M.P.'s investigations of complaints and evaluating the R.C.M.P.'s complaints handling procedures. To perform this role effectively, the Inspector should receive copies of all written complaints of R.C.M.P. misconduct and reports from the R.C.M.P. of the results of its investigations of these complaints.[21]

The Commission's report quoted Albert Reiss, a noted expert on the police, who had written that "[a]cquisition of the input and output information (relating

to a complaint) is one of the most powerful monitoring devices available over an organization. Whoever has that information has the potentiality to assess where the problems of the organization lie."[22]

The McDonald Commission did not limit the Inspector's jurisdiction to complaints, however, noting that often no complaint is made, for a variety of reasons, including fear of reprisals from the police, lack of awareness of possible police misconduct and lack of confidence in police impartiality.[23] It envisioned a general audit function for the Inspector:

> [A]s part of his reviewing and evaluating role, the Inspector of Police Practices [should] inquire into and review at his own discretion or at the request of the Solicitor General any aspect of R.C.M.P. operations and administration insofar as such matters may have contributed to questionable behaviour on the part of R.C.M.P. members.[24]

These recommendations were consistent with the McDonald Commission's recommendations for an independent monitoring body (the Security Intelligence Review Committee, or SIRC) for the new national security organization (the Canadian Security Intelligence Agency, or CSIS), empowered to conduct self-initiated reviews.

2.1.1.2
Creation of CPC

Pressure on the government to set up a system for complaints against the RCMP increased after the release of the McDonald Commission report exposing wrongdoing by the RCMP. Further pressure arose following a 1981 decision by the Supreme Court of Canada that only a federally established body could deal with complaints against the Force, which resulted in provincial attempts to discipline RCMP officers being struck down.[25] The 1986 amendments to the *Royal Canadian Mounted Police Act* (*RCMP Act*) that established the CPC borrowed more heavily from the Marin Commission than the McDonald Commission report.[26] The CPC is primarily the overseer of the RCMP complaints process. Initial investigation of most complaints is done by the RCMP. As a rule, the CPC becomes involved only if a complainant is not satisfied with the RCMP's disposition of the complaint, whereupon the CPC may prepare a report to the Minister commenting upon the complaint, request that the RCMP investigate further, conduct further investigation on its own or institute a hearing to inquire into the complaint.[27] It also has the power to initiate its own complaint. Its power to institute a hearing is not dependent on an initial investigation or report by the RCMP. The CPC does not have the power to impose penalties or sanctions,

however. Its power is a power of persuasion, in that it may issue reports to the Minister and make those reports public.

The CPC's jurisdiction is limited to complaints "concerning the conduct, in the performance of any duty or function under this Act . . . of any member or other person appointed or employed under the authority of this Act."[28] As the Federal Court of Appeal stated in 1994, "Parliament did not retain the suggestion contained in the *Marin Report* that the complaint process should apply to complaints alleging the failure of the Force itself to meet public expectations."[29] This means that complaints are heard with respect to alleged individual, not systemic, misconduct.

2.1.1.3
Statutory Framework for CPC

The legislation establishing the CPC was enacted in 1986[30] and came into force in 1988.[31] Originally called the RCMP Public Complaints Commission, the body was renamed in 2001 under the Federal Identity Program Policy to reflect the fact that it is an independent entity and not part of the RCMP organization.[32] The Act provides that the CPC may have up to 29 members, appointed by the federal Cabinet for renewable five-year terms.[33] Despite the CPC's potential for broad representation from across Canada,[34] at present it has only two members, the Chair and the Vice-Chair, both of whom hold full-time appointments. It has a staff of 44 and a budget of $5.1 million.[35]

Part VI of the *RCMP Act* sets out procedures for the CPC to deal with public complaints against members of the RCMP.

There is a broad right for members of the public to bring complaints against members of the RCMP or other persons employed under the Act in relation to the performance of their duties. The Act provides that any member of the public, "whether or not that member of the public is affected by the subject-matter of the complaint" may make a complaint.[36] The complaint may be made to the CPC, the RCMP or a relevant provincial authority. In 2004-2005, the Commission received 825 complaints that were referred to the RCMP for investigation, and in 2005–2006 it received 738 complaints.[37]

The Chair of the CPC may also initiate a complaint where he or she is satisfied that there are reasonable grounds to investigate the conduct of any member. Such a complaint is investigated by the RCMP.[38] This power was recently used with respect to an RCMP shooting of an Aboriginal man in Norway House, Manitoba.[39]

Although every complaint must be acknowledged in writing and the Commissioner of the RCMP must be notified of every complaint,[40] there is no

statutory obligation to inform the CPC of all complaints received by the RCMP.[41] The RCMP Commissioner is required to "establish and maintain a record of all complaints received by the Force under this Part; and . . . on request, make available to the Commission any information contained in the record."[42] However, the CPC does not generally request information under this section. Consequently, citizens' complaints made directly to the police come to its attention only if the matter is referred to it by a complainant who is not satisfied with the RCMP's handling of the complaint.

The *RCMP Act* provides for a procedure for attempting to informally dispose of a complaint, where the complainant and the RCMP member who is the subject of the complaint consent.[43] In 2004–2005, alternative dispute resolution was used for 502 cases, 471 of which were resolved without a formal complaint proceeding, and in 2005-2006 the Commission facilitated the informal resolution of 339 complaints.[44]

Where complaints are not disposed of informally, the RCMP generally conducts an investigation of the complaint and provides a report to the complainant. However, the Commissioner of the RCMP may direct that no investigation be conducted or that an investigation be terminated if, in the Commissioner's opinion, the complaint could more appropriately be dealt with, initially or completely, according to a procedure provided under any other act of Parliament; the complaint is trivial, frivolous or vexatious, or was made in bad faith; or, having regard to all the circumstances, investigation or further investigation is not necessary or reasonably practicable. The complainant must be informed of any decision not to investigate and of his or her right to refer the complaint to the CPC if not satisfied with that decision.[45]

Indeed, if a complainant is not satisfied with the RCMP's disposition of the complaint or a decision not to investigate, he or she may ask the CPC to conduct a review.[46] If, upon reviewing the complaint, the Chair of the CPC is satisfied with the RCMP's disposition of the complaint, he or she sends a written report to that effect to the Minister, the Commissioner, the subject of the complaint and the complainant. If dissatisfied, the Chair may prepare and send to the Minister and the Commissioner a written report setting out findings and recommendations with respect to the complaint; ask the Commissioner to conduct a further investigation; or investigate the complaint further or institute a hearing to inquire into the complaint.[47]

In 2005-2006, the CPC received 159 requests for review, and completed 260 review reports. In 82 percent of the reviews, the Commission was satisfied with the conduct of RCMP members. In the remaining 18 percent of cases, the

Commission made adverse findings resulting in 67 recommendations for remedial action, most of which the RCMP Commissioner agreed to implement.[48]

Although the Chair of the CPC does not technically sit in appeal of the RCMP's investigation, he or she does have several options when a complainant is dissatisfied with the Force's disposition of the complaint. Regardless of whether or not the complaint has been investigated, reported on, or otherwise dealt with by the RCMP, the Chair may investigate or institute a public hearing into a complaint concerning the conduct of a member where he or she deems it in the public interest.[49] In such a case, the RCMP is not required to investigate or deal with the complaint until the CPC provides it with a report.[50] The CPC makes use of this "public interest" procedure once or twice each year.[51] For example, it did so in the well-known case relating to RCMP conduct at the 1997 APEC conference in Vancouver, where pepper spray was used against protesters.[52] That case, which started in early 1998,[53] involved an aborted hearing, a number of court proceedings, and a further hearing by former Justice Ted Hughes. In the Arar case, a complaint was instituted by the Chair of the CPC[54] and an investigation was started, but was subsequently suspended pending the outcome of this Inquiry.

Other public investigations have related to police conduct at a 1997 demonstration concerning the closing of French-language schools in New Brunswick[55] and, more recently, police handling of an arrested person who was suffering from mental illness.[56] In late May 2004, a public interest investigation was launched into RCMP investigations into alleged sexual abuse at the Kingsclear Youth Training Centre in New Brunswick.[57] In July of the same year, another public interest investigation was begun into an allegation of sexual assault by an RCMP officer.[58]

Where the Chair of the CPC is dissatisfied with the disposition of a complaint by the RCMP either after a review or a hearing, including a public interest hearing, the Chair sends an interim report to the RCMP Commissioner and the Minister, setting out his or her findings and recommendations. The Commissioner of the RCMP is required to inform the Chair and the Minister, in writing, of any action to be taken in response to the Chair's interim findings and recommendations[59] and provide reasons for rejecting any findings or recommendations. The Chair then prepares a final report that includes the Commissioner's response and the Chair's final findings and recommendations and sends it to the complainant, the RCMP member(s) involved, the Commissioner and the Minister. The Chair does not have the power to impose a recommendation on the Commissioner.

The CPC's powers to access information are not specified in the Act. Unlike SIRC, which has broad authority to review the activities of the Canadian Security Intelligence Service (CSIS)[60] and receives reports on what CSIS does,[61] as well as ministerial directions to CSIS,[62] the CPC generally only becomes involved when persons complain directly to it or when complainants dissatisfied with how the RCMP handled their complaints refer the complaints to the CPC. Under the *RCMP Act*, where a complainant is not satisfied with the disposition of a complaint and refers the complaint to the CPC for review, the Commissioner of the RCMP "shall furnish" the Chair of the CPC with the RCMP's report of the results of its investigation and any action taken and "such other materials under the control of the Force as are relevant to the complaint."[63]

In its 2004–2005 Annual Report, the CPC commented:

> The CPC has 16 years' experience in working with the public complaint process established by Part VII of the *RCMP Act* . In those 16 years, the biggest challenge the CPC has faced, and continues to face, is access to information in the control of the RCMP. The RCMP Act states in clear and unequivocal words that, when a complainant requests a review of a complaint by the CPC, the RCMP must provide the CPC with all the materials relating to that complaint. These materials may include, for example, RCMP investigative and operational files, witness statements, RCMP policies and protocols, police notes, search warrants and reports to Crown. The CPC's access to these materials is vital to its ability to piece together the evidence with a view to making impartial findings of fact and determining whether or not a complaint is substantiated.[64]

In the same report, the CPC raised its concerns about obtaining access to relevant material from the RCMP. The Commission cited delays in obtaining materials, or refusals to produce relevant materials on grounds including "national security," as causing concerns regarding accountability. The CPC stressed the distinction between disclosing information to it and disclosing information to the complainant or the public.[65]

Another means for the CPC to gain access to information is to hold a public hearing. When holding such a hearing, the CPC has the powers conferred on a board of inquiry by the *RCMP Act* (such as the power to summon a person and receive evidence on oath) in relation to the matter before it.[66] The Act moreover allows the CPC to order that a hearing or part of a hearing be held in private if information is likely to be disclosed that could reasonably be expected to be injurious to the defence of Canada or any state allied or associated with Canada or to the detection, prevention or suppression of subversive or hostile activities; could reasonably be expected to be injurious to law enforcement; or

is information respecting a person's financial or personal affairs where that person's interest or security outweighs the public's interest in the information.[67]

This procedure is used in the case of a public interest investigation and a public hearing, but not in routine cases. Indeed, no public hearing has been held since the APEC case mentioned above.

In a speech to the Canadian Institute for the Administration of Justice six months after the events of September 11, 2001, then CPC chair Shirley Heafey complained publicly about the CPC's lack of powers.[68] "The RCMP," she said, "may have greater powers, but the agency with oversight responsibility does not." She went on to state:

> When Parliament framed the *CSIS Act* and established the Security Intelligence Review Committee (SIRC), it recognized that, where matters of national security are concerned, there is always a great deal of secrecy surrounding operations. Accordingly, to ensure adequate oversight, SIRC was equipped with a large arsenal of oversight tools. For example: it has audit powers so it can look at any situation that it decides warrants review. As well, by law, certain activities of CSIS must be reported to the Security Intelligence Review Committee. And, most notably, SIRC has access to judicial warrants and the affidavits upon which they were obtained. The CPC does not have similar powers.

Ms. Heafey pointed out that, under the *RCMP Act*, the "process is complaint driven":

> [P]roblems are generally drawn to my attention by a complainant. But what happens when a potential complainant doesn't know of the CPC's existence or, worse, is afraid to complain about the actions of the police? . . . Without a complaint and without the power to randomly review files, it is difficult to investigate and to assess RCMP use of the new powers. . . . A search is authorized by warrant issued by a judicial official who has read an affidavit in support of the request for the warrant. If I don't have access to those documents, how can I, in good conscience, assure the Minister of Justice and the Solicitor General that I am overseeing the RCMP's use of these new powers?

"The CPC," she concluded, "requires additional powers and additional resources to restore balance — to balance the new powers and resources given to the RCMP for the purpose of combating terrorism."[69]

The CPC submits annual reports of its activities to Parliament.[70] It has also produced some studies not directly linked to a specific complaint, such as one in 1999 on police pursuits.[71]

2.1.2
Military Police Complaints Commission

A somewhat different approach to review of police activity is taken for the military police.[72] There are some 1,300 military police members in Canada and overseas in places such as Afghanistan and the Golan Heights. Military police members have jurisdiction over all persons subject to the *Code of Service Discipline* throughout Canada and abroad and have peace officer status for the purpose of enforcing the Code.[73] In addition, they have peace officer status in respect of all persons when engaged in certain prescribed policing and security duties on or in Department of National Defence (DND) property.[74] Thus, they have jurisdiction over members of the general public who commit offences on or in relation to DND property.

Most military police officers are assigned to active military units, where they carry out policing functions, but also serve as members of the Canadian Forces (CF). Approximately 110 members of the military police are assigned to the CF National Investigation Service (NIS), a special unit that reports to the Provost Marshal and is independent of the operational chain of command (applicable to the army, navy and air forces). Members of the NIS investigate the more serious criminal or military offences and conduct "sensitive" investigations involving senior officers or equivalent civilian employees of DND, sensitive material or instances that could bring discredit to DND.

About 40 members of the military police are assigned to the National Counter-Intelligence Unit (NCIU), under the command of the Deputy Chief of Defence Staff, within J2 (Intelligence). Some of the members serving in the NCIU may participate in joint operations with the RCMP or other agencies through Integrated National Security Enforcement Teams (INSETs) or Integrated Border Enforcement Teams (IBETs) where there is a military nexus.

Generally speaking, the RCMP takes the lead on national security investigations, although the military police could be involved, likely through the NIS, depending on the facts. The military may acquire top secret and other national security information through formal channels. If it acquires this type of intelligence by other means, the practice is to pass it on to the RCMP.

The Military Police Complaints Commission (MPCC) is a civilian review body that operates independently of DND and the Canadian Forces (CF). It is staffed entirely by civilians and reports to Parliament through the Minister.[75] The MPCC was created to make the handling of complaints involving the military police more transparent and accessible, discourage interference with military police investigations, and ensure that both complainants and members of

the military police are dealt with impartially and fairly.[76] It was established in 1999 as part of an overhaul of the *National Defence Act*,[77] in response to recommendations by various working groups that had looked at the military justice system.[78]

The MPCC reviews the investigation of certain complaints undertaken by the CF Provost Marshal.[79] It has jurisdiction over both conduct and interference complaints, although such jurisdiction is limited to conduct complaints that relate to the performance of policing duties and functions and interference complaints that pertain to an investigation.[80]

The *National Defence Act* makes the following provision with respect to conduct complaints:

> Any person, including any officer or non-commissioned member, may make a complaint under this Division about the conduct of a member of the military police in the performance of any of the policing duties or functions that are prescribed for the purposes of this section in regulations . . . .[81]

The relevant regulations provide:

> 2(1) For purposes of subsection 250.18(1) of the Act, any of the following, if performed by a member of the military police, are policing duties or functions:
>
> (a) the conduct of an investigation;
> (b) the rendering of assistance to the public;
> (c) the execution of a warrant or another judicial process;
> (d) the handling of evidence;
> (e) the laying of a charge;
> (f) attendance at a judicial proceeding;
> (g) the enforcement of laws;
> (h) responding to a complaint; and
> (i) the arrest or custody of a person.
>
> (2) For greater certainty, a duty or function performed by a member of the military police that relates to administration, training, or military operations that result from established military custom or practice, is not a policing duty or function.[82]

The Provost Marshal[83] has initial responsibility for dealing with conduct complaints, although such complaints may be made to the Chairperson of the MPCC, Judge Advocate General, Provost Marshal or any member of the military police.[84] The Provost Marshal classifies complaints as relating to policing duties or functions, or as internal matters. The distinction is an important one, as the MPCC has jurisdiction only with respect to the former, and the Provost Marshal

has no obligation to notify the MPCC of complaints involving matters classified as internal.[85] There have been some differences of interpretation between the MPCC and the Provost Marshal's office as to whether a matter falls within the definition of "policing duty or function" and thus engages the jurisdiction of the MPCC. Following an independent review of the legislation, the Right Honourable Antonio Lamer, former Supreme Court of Canada Chief Justice, recommended that this particular definition be clarified.[86] I note that Bill C-7, which, if passed, would have a significant impact on the operation of the MPCC, proceeded to First Reading in the House of Commons on April 27, 2006.[87]

2.1.2.1
Procedural Powers

A conduct complaint made orally or in writing must be acknowledged and the subject of the complaint must be advised of the allegation unless this could adversely affect or hinder an investigation.[88] Both the complainant and the subject of the complaint must be advised of the progress of the matter periodically until it is resolved.[89]

Subject to any attempts at informal resolution, the Provost Marshal is responsible for investigating conduct complaints. However, he or she may direct that no investigation be started or that an investigation be ended if the complaint is frivolous or vexatious, or was made in bad faith; could more appropriately be dealt with according to a procedure under another part of the *National Defence Act* or under any other act of Parliament; or, having regard to all the circumstances, investigation is not necessary or reasonably practicable.[90] Thus, the Provost Marshal exercises a filtering function with respect to conduct complaints.

Upon completion of an investigation into a conduct complaint, the Provost Marshal is required to send the complainant, the subject of the complaint and the Chairperson of the MPCC a report setting out a summary of the complaint, the findings of the investigation, a summary of action that has or will be taken, and the right of the complainant to refer the complaint to the MPCC for review if not satisfied with the disposition.[91]

A complainant dissatisfied with the direction by the Provost Marshal refusing or ending informal resolution or an investigation or with the disposition of the conduct complaint may request that the MPCC review the matter.[92] In such a case, the Provost Marshal must provide the Chairperson with all information and materials relevant to the complaint.[93] The MPCC does not possess other significant powers to compel witnesses and evidence when reviewing conduct complaints. However, if the Chairperson considers it advisable "in the public

interest," he or she may at any time cause the MPCC to conduct an investigation and, if circumstances warrant, hold a public hearing into a complaint. This applies to both conduct and interference complaints.[94]

When reviewing the file, the Chairperson may investigate any matter relating to the complaint. Upon completion of the review, the Chairperson sends the Minister, Chief of the Defence Staff and Provost Marshal a report setting out his or her findings and recommendations regarding the complaint.[95] After reviewing the Chairperson's report, the Provost Marshal prepares and sends the Chairperson a notice of action indicating the intended response to the complaint and reasons for any decision not to act on any findings or recommendations.[96] After considering the Provost Marshal's notice of action, the Chairperson prepares a final report on the complaint, which is sent to the same officials as the initial report, as well as the complainant and the subject of the complaint.[97]

As for interference complaints, the Chairperson of the MPCC is responsible for dealing with such complaints in the first instance. However, if appropriate, the Chairperson may ask the Provost Marshal to conduct the investigation.[98] Procedures are similar to those for conduct complaints. The MPCC has the power to compel the attendance of witnesses or production of documents only if a public interest hearing is convened.[99]

Hearings are held in public, although the MPCC may order a private hearing (in whole or in part) if it is of the opinion that information is likely to be disclosed that could be injurious to the defence of Canada or any state allied or associated with Canada or to the detection, prevention or suppression of subversive or hostile activities, or that could be injurious to the administration of justice, including law enforcement. A private hearing may also be ordered to avoid disclosure of information affecting a person's privacy or security interest, if that interest outweighs the public's interest in the information.[100]

The *National Defence Act* guarantees more or less full procedural rights to interested persons in a public hearing, including the right to be represented by counsel, present evidence, cross-examine witnesses, and make representations.[101] Witnesses must answer questions, although what they say cannot be used against them in other proceedings in respect of an allegation that the witness made a false statement.[102]

2.1.3
Provincial Police Review Bodies

2.1.3.1
Ontario

Two review bodies in Ontario provide interesting variations on the federal models: the Ontario Civilian Commission on Police Services (OCCPS) and the Special Investigations Unit (SIU).

The province's mechanisms for civilian review can be traced back to a series of reports starting in 1975 that recommended increased civilian review of complaints against the police. In 1975, Arthur Maloney completed a review of citizen-police complaint procedures for the Metropolitan Toronto Police Board.[103] At the time, complaints were handled by the police force's internal complaints bureau. Mr. Maloney recommended that complaints continue to be investigated by the police, but that a commissioner (a lawyer or retired judge) review the complaints process and have the right to call an adjudicative hearing.[104] Where the Commissioner found the complaint to be valid, the case would be returned to the chief of police to impose punishment.[105]

The Royal Commission into Metropolitan Toronto Police Practices, chaired by Justice Donald Morand, arrived at similar conclusions in 1976,[106] as did the Task Force on Human Relations, chaired by Walter Pitman, in 1977[107] and Roman Catholic Cardinal Emmett Carter in 1979.[108] Both of the latter looked into race relations. In 1979, then Attorney General of Ontario Roy McMurtry asked Sidney Linden to study this same issue.[109] Professor Linden's report recommended that the police have the authority to conduct the initial investigation of a complaint, but that it allow an independent civilian review agency to do so in exceptional circumstances. The Linden report also recommended that the review agency have the power to impose penalties.

In 1981, the Ontario government enacted legislation permitting a three-year pilot project for Metropolitan Toronto.[110] Under that legislation, the Toronto Chief of Police was required to establish a Public Complaints Investigation Bureau to receive, record and investigate public complaints. The Public Complaints Commissioner was to monitor and review the Bureau's investigations and could investigate a complaint after receiving an interim report from police investigators or prior to receipt of such report in the event of undue delay by the police or other exceptional circumstances.[111] Independent hearings could be ordered by the Commissioner if the complainant was not satisfied with disciplinary action taken by the police in response to a finding of wrongdoing.[112]

The Toronto Chief of Police could also refer a matter to a hearing, to be conducted *de novo*.[113] The tribunal at such a hearing was empowered to impose penalties, including dismissal from the force.[114] After the pilot project was concluded, permanent legislation was enacted in 1984.[115]

In 1990, the Ontario government made the Toronto complaints mechanism applicable to all police forces in Ontario, including the Ontario Provincial Police (OPP).[116] The process remained much the same as the Metropolitan Toronto complaints process. However, the 1990 Act gave the Attorney General the power to direct the Commissioner of the complaints body to initiate a complaint and gave the Commissioner the right to review a decision by a chief of police concerning a complaint.[117] In order to emphasize the complaint body's independence from the police, the Commissioner was made responsible to the Attorney General rather than the Solicitor General, who had responsibility for the police.[118] Tribunals were to be chaired by independent lawyers,[119] who could make findings on "clear and convincing evidence"[120] rather than on "proof beyond a reasonable doubt," as set out in the earlier legislation respecting Metropolitan Toronto.[121] Penalties could be imposed directly by the tribunal.[122]

There continued to be opposition to this process by some police associations and, in 1995, the Ontario government commissioned a study on the issue.[123] Following release of the study report, the *Ontario Police Act* was amended in 1997 to create the current public complaints regime, under which only a person "directly affected" can make a complaint.[124] However, a complaint can relate to "the policies of or services provided by a police force," in addition to the conduct of a police officer.[125] A complaint may be made to either the Ontario Civilian Commission on Police Services (OCCPS) or the relevant police service.

Complaints are to be initially investigated, findings made and discipline imposed by the relevant police agency (usually by the chief of police). Thus, while the OCCPS has the power to conduct, on its own motion, investigations, inquiries and reviews into various matters,[126] its role is largely limited to appeals from decisions of chiefs of police.[127] The Chair of the OCCPS has written that "the primary responsibility for dealing with public complaints rests with the chief of police under the general direction and guidelines of the local board."[128] Chiefs of police have the power to refuse to deal with a complaint because it is frivolous or vexatious, was made in bad faith or was made more than six months after the event complained of.[129] In such an event, a complainant has the right to ask the OCCPS to review the decision.[130]

If the complaint relates to policies or services, as opposed to the conduct of an officer, the chief of the service investigates and submits a report, along with

his or her disposition of the complaint to the relevant police services board.[131] The complainant receives a copy of the report and is entitled to ask the police services board to review it.[132]

A conduct complaint is processed differently. The chief of police is responsible for ordering the investigation of such complaints, but the actual investigation may be undertaken by the professional standards branch or, where the service has no such branch, by an officer in the service. Less serious complaints may be investigated by unit commanders.[133] A chief may ask another police service to carry out the investigation.[134]

If it is determined that a complaint cannot be substantiated, the complainant and the subject of the complaint are notified of the decision and the complainant's right to have the OCCPS review the decision.[135] The OCCPS has the power to require a hearing of the complaint. If the investigation reveals misconduct or unsatisfactory work performance, but the matter is not of a serious nature, the *Police Services Act* provides for informal resolution. If this fails, the chief of police may impose certain penalties without a hearing.[136]

A hearing is held for more serious matters or where the affected officer requests one. Such hearings are presided over by the chief, who appoints a prosecutor, who may be a police officer, lawyer or agent. A broad range of penalties up to and including dismissal are available if misconduct or unsatisfactory performance is found "on clear and convincing evidence."[137]

Both police officers and complainants may appeal decisions in discipline hearings to the OCCPS, and OCCPS decisions in such matters may in turn be appealed in Divisional Court.[138] The right to appeal to Divisional Court does not apply to other OCCPS decisions, such as refusals to proceed because a complaint is frivolous or vexatious, or determinations after investigation that a complaint cannot be made out.

The OCCPS is made up of two full-time and 11 part-time members[139] and has a budget of about $1.6 million.[140] In 2004, there were 3110 complaints reported in the province of Ontario; 562 were reviewed by the Commission at the request of the complainant and 38 hearings were ordered.[141] The OCCPS is under the jurisdiction of the Ministry of Community Safety and Correctional Services[142] rather than the Ministry of the Attorney General, as was the case with the former Metropolitan Toronto Commission.

In his recent review of the Ontario complaints structure, the Honourable Patrick LeSage commented that, when Ontario introduced its 1997 reforms, there was a 70 percent decrease in the total budget assigned to the handling of police complaints and oversight. Justice LeSage proposed the creation of a new independent body that could not only review, but also investigate police

complaints. Moreover, he proposed that third-party complaints be allowed and that steps be taken to make the complaint system in Ontario more accessible to and connected with the community. He also recommended that regular audits be done of the way police forces handle complaints and indicated that "[t]he new body should have a power of inquiry available to it to identify systemic problems that may underlie complaints and make recommendations to prevent their recurrence."[143]

The Special Investigations Unit (SIU) is a body that is unique in Canada in terms of its powers and jurisdiction.[144] The Director of the SIU has the discretion to "cause investigations to be conducted into the circumstances of serious injuries and deaths that may have resulted from criminal offences committed by police officers."[145] The civilian investigators, who must not be active police officers,[146] automatically initiate an investigation without the necessity of the existence of a complaint.

The SIU was established in 1990[147] following the release of a report by the Task Force on Race Relations and Policing, chaired by Clare Lewis,[148] which was set up after several controversial shootings of black men by police in Ontario.[149] The unit reports to the Attorney General[150] and has a budget of over $5 million. It was not affected by the changes to the complaints process in 1997. In the year ending March 31, 2005, it conducted investigations into 137 incidents, resulting in three charges being laid.[151]

As described in chapters IV and V, Ontario police are involved in national security investigations. There are no special mechanisms for handling complaints or reviewing activities of these units other than those discussed above.

2.1.3.2 Quebec

Legislation dealing with the independent review of public complaints against Quebec's provincial police force, the *Sûreté du Québec*, as well as all municipal and Aboriginal police forces in Quebec was first enacted in 1988.[152] Before then, discipline was handled by the police forces themselves. The legislation has been amended several times since, but the thrust of the latest version of the Quebec *Police Act*[153] does not differ significantly from that of the 1988 legislation.

In contrast to the current Ontario and RCMP mechanisms, where a complaint is generally initially investigated by members of the police force to which the subject of the complaint belongs, complaints in Quebec are handled by an independent authority, the Police Ethics Commissioner. Under the original 1988 legislation, the Commissioner could allow the police force whose member was the subject of the complaint to investigate the matter, but amendments made in

1997 provide that "[a]n investigator may not be assigned to a file involving the police force to which he belongs or has belonged."[154]

In almost all cases, the Ethics Commissioner has his or her own staff conduct investigations or uses private investigators, many of whom are retired police officers. The Commissioner's budget is about double that of the Ontario Commission.[155] The Commissioner has powers of entry to police premises and power to require the production of documents.[156]

After the initial investigation, the Commissioner may dismiss the complaint, send it forward for a criminal investigation, or try to reconcile the parties involved in the complaint. Conciliation by the Commissioner's independent conciliator is required for all non-serious cases, but is not used for complaints involving death or serious bodily harm, criminal offences or other serious misconduct.[157] A complainant may not object to conciliation without giving a valid reason.[158] There is a strong incentive for an officer in Quebec to attempt to obtain an agreement because, if conciliation succeeds, no record of the complaint or settlement is placed in the member's personnel file.[159] However, the office of the Commissioner does keep such a record.

The Commissioner may also summon the police officer to appear before a separate independent body, the Police Ethics Committee,[160] which holds hearings to determine if a police officer has committed a breach of the *Code of ethics of Québec police officers*.[161]

The Commission receives about 1,300 complaints a year and the Committee conducts about 60 hearings.[162] It also hears appeals by complainants from dismissals of complaints by the Commissioner after investigation.[163] It may impose a number of penalties, ranging from a warning or rebuke, to suspension without pay for up to 60 days and dismissal.[164] Appeals from decisions of the Committee may be brought before the Court of Quebec.

The Police Ethics Commissioner and full-time members of the Police Ethics Committee must have been members of the bar for at least ten years.[165] Appointments are for five years and may be renewed.[166] The original 1988 legislation in Quebec required police representation on the hearing panels[167] and tripartite tribunals were therefore necessary. Amendments made in 1997 eliminated the requirement for police representation, making it possible to have single-member panels.[168]

The Ethics Commissioner is notified within five days of all complaints received by the police.[169] Complaints in Quebec may be lodged by "any person."[170] Although the Commissioner has not specifically been given the power to initiate a complaint, as the CPC has, the Minister may request an investigation.[171] Moreover, there is an obligation on the part of police officers under the *Police*

Act "to inform the director of police of the conduct of another police officer likely to constitute a breach of discipline or professional ethics."[172] In turn, the chief must inform the Ethics Commissioner of any "presumed commission of an act derogatory" to the *Code of ethics of Québec police officers*.[173] Where appropriate, the Commissioner then contacts the citizen to see if he or she wishes to make a formal complaint.[174] Thus, in theory, the Commissioner receives notification of all complaints received by the police, as well as of potential complaints reported to the chief through other police officers.

Complaints are based on the Code.[175] The following are some of the duties and standards of conduct set out therein: a police officer must "produce official identification when any person asks him to do so;" must not "use greater force than is necessary to accomplish what is required or permitted;" must not "illegally dispose of property belonging to any person;" and must not "show, handle or point a weapon without justification."[176]

2.1.3.3
British Columbia's Variation

For the purposes of this examination, Ontario's system of monitoring police handling of complaints and hearing some appeals and Quebec's system of having a complaints body investigate complaints convey a sense of the major policy choices in this area. In addition, Ontario's SIU demonstrates how, in a monitoring system, certain issues can be subject to separate independent investigation. Other provincial and territorial systems with variations on the Ontario and Quebec models have been outlined in a background paper produced by this Commission.[177] Although I do not describe them all again here, I do touch on certain features of British Columbia's police complaints system below, as it includes some interesting variations.

British Columbia established the Office of the Police Complaint Commissioner in July 1998,[178] following publication of a report by Justice Wallace Oppal.[179] Many of the recommendations of the Oppal report were incorporated into the 1998 amendments, including that of having the Office of the Police Complaint Commissioner replace the B.C. Police Commission, established in 1974.[180] In 2005–2006, the Complaint Commissioner had an annual budget of just over a million dollars and a full time staff of eight persons.[181] In 2005, it received 426 complaints, and held one public hearing.[182]

The process for appointing B.C.'s Police Complaint Commissioner, designed to increase the Commissioner's independence, is unique in Canada. The Commissioner is an officer of the legislature, appointed by the Lieutenant Governor in Council on the recommendation of a special committee of the

legislature.[183] The term of office is six years and is non-renewable. The Office of the Commissioner does not itself conduct investigations.[184] As in almost all other jurisdictions, these are conducted by the police, but there are requirements for ongoing reporting to the Commissioner during an investigation,[185] and the Commissioner may appoint an employee to oversee the conduct of an investigation if "necessary in the public interest."[186] The Commissioner receives a full transcript of all proceedings, reviews all complaint dispositions, and may ask for further reasons for the disposition of the complaint.[187] After the case is concluded by the police authority, the complainant or the officer may request that the Commissioner arrange a public hearing, to be chaired by a Provincial Court judge.[188] The Commissioner may arrange a hearing without such a request if he or she determines that it is "necessary in the public interest."[189] No provision is made for appeal from a decision of the Commissioner.[190] However, there is provision for appeal of a decision by the hearing adjudicator to the court of appeal, with leave, on questions of law.[191]

2.2
JUDICIAL REVIEW OF POLICE ACTIONS

Any examination of the review of the national security activities of the police would be incomplete without an examination of the role of the courts in reviewing police conduct, a corollary of Canada's commitment to the rule of law. The rule of law requires that police actions be authorized by a valid law and that police conduct be subject to judicial review and, if illegal, the award of an appropriate remedy. When police officers act without legal authority, they can be the subject of an action for damages in private or civil law. Cases such as *Roncarelli v. Duplessis*[192] establish that no state official, whether the Premier or the police, is immune from the law; that the action of each official must be authorized by the law and that the police may be held accountable for illegal activities. In recent years, new potential civil causes of actions have been recognized with respect to matters such as malicious prosecution[193] and misuse of public office.[194] Although civil lawsuits against the police are expensive and lengthy and therefore relatively rare, they do serve an important accountability function.

In 1981, the McDonald Commission recommended that courts be given discretion to exclude evidence obtained through police improprieties, in part because of a concern that some within the RCMP interpreted "the absence of critical comment by the judiciary as tacit approval of forms of conduct that might be unlawful."[195] Subsequently, the 1982 enactment of the *Canadian Charter of*

Rights and Freedoms fundamentally changed the criminal trial and provided much greater scope for the review of police conduct.

Police misconduct may become a relevant matter in a criminal trial, frequently through *Criminal Code* or Charter challenges concerning the admissibility of evidence. For example, police use of electronic surveillance may be carefully examined in criminal trials when the accused raise objections to the admissibility of evidence under either the Code or Charter. The accused have broad rights of disclosure of all material relevant to the case, including the material used to justify the warrant.

Evidence obtained in a manner that involves other methods of search and seizure may also be challenged on the basis that the police did not respect Charter standards and so the evidence should be excluded. In addition, police practices with respect to interrogation and investigative steps are subject to Charter review in a criminal trial, to ensure that they comply with a variety of legal rights protected under the Charter.

Section 24(2) of the Charter mandates that unconstitutionally obtained evidence be excluded when its admission would bring the administration of justice into disrepute, and judges have not hesitated to exclude evidence obtained through serious violations of the Charter. This represents a fundamental change from the pre-Charter environment examined by the McDonald Commission.

The McDonald Commission also recommended that a defence of entrapment be added to the *Criminal Code* as an external judicial control on undercover operations and the use of agent provocateurs. In 1988, the Supreme Court recognized a defence of entrapment resulting in a stay of proceedings if the police or police agents provide a person with an opportunity to commit a crime, unless the police are acting on a reasonable suspicion that the person is involved in crime, or pursuant to a "bona fide inquiry" into a crime in an area where it is reasonably suspected that criminal activity is occurring.[196] Even if such prerequisites for proactive investigations exist, the police must never go beyond providing persons with an opportunity and actually induce the commission of the crime.[197] The entrapment defence is available regardless of the accused's subjective intent. As in the case of section 24(2) of the Charter, this is to protect the administration of justice from disrepute.

The advent of the Charter and the entrapment defence represents a fundamental change from the pre-Charter environment, in which the courts, subject to some limited exceptions such as the requirement that confessions be voluntary, rarely examined the propriety or legality of police conduct as part of the criminal trial process. The use of the criminal trial to adjudicate the propriety of

police conduct is an important development that has undoubtedly increased the accountability of the police and resulted in new rules governing police conduct.

At the same time, it should be recognized that trials are relatively rare in the national security context and thus the probability that any particular police action will be subject to Charter challenge is quite low. Even when charges are laid, Charter violations may escape judicial scrutiny if the case is resolved through plea discussions. Even the establishment of a Charter violation at trial does not necessarily mean that unconstitutionally obtained evidence will be excluded. In any event, the exclusion of evidence or the entry of a stay of proceeding in a criminal trial because of police improprieties may not necessarily result in tangible consequences for the police officer involved. Nevertheless, the possibility of judicial review either in civil or criminal courts is an important part of the current review landscape that affects the RCMP in the conduct of its national security activities.

3.
SECURITY INTELLIGENCE REVIEW BODIES

There are a number of Canadian agencies that review the activities of security intelligence agencies. In this section, I describe the Security Intelligence Review Committee and the Office of the Inspector General, both of which review CSIS, and the Office of the Communications Security Establishment Commissioner, which reviews the CSE.

3.1
SECURITY INTELLIGENCE REVIEW COMMITTEE (SIRC)

The Security Intelligence Review Committee (SIRC) was established in 1984 as an independent, external review body that reports on the operations of CSIS directly to the Parliament of Canada.[198] SIRC's role has long been understood to be that of assuring Parliament and the Canadian public that Canada's security intelligence service is fulfilling its mandate to ensure the security of the state while respecting individual rights and liberties as guaranteed under Canadian law. To this end, SIRC examines past operations of CSIS and investigates complaints.

SIRC is a committee consisting of a Chair and not less than two and not more than four members.[199] All are privy councillors not serving in Parliament.[200] The *CSIS Act* provides that they are to be selected after "consultation" by the Prime Minister with the Leader of the Opposition and the leaders of each party in the House of Commons with twelve or more members in the House. The implication of this consultation, though never actually spelled out, is that the membership of SIRC should broadly reflect the makeup of the House, thus paralleling

the representative role of the parliamentary committee that was not created. However, mirror representation of Parliament has not always been the case in practice.[201] Each member of SIRC is appointed for a five-year term and is eligible to be reappointed for a second five-year term.[202] SIRC members must comply with the security requirements applicable to employees under the *CSIS Act* and are required to take an oath of secrecy.[203]

Considering the significance of SIRC as a Canadian model for review of security intelligence, I discuss its mandate and operations in detail in the next section.

3.1.1 SIRC Mandate and Operations

SIRC is mandated to "review generally the performance by the Service [CSIS] of its duties and functions,"[204] which are set out at sections 12 through 17 of the *CSIS Act*. The Act sets out certain aspects of the general review power, including the following:

- review the reports of the Director and certificates of the Inspector General with respect to the operational activities of the Service;
- review directions issued by the Minister to the Service;
- review arrangements entered into by the Service with provincial governments and their departments and with police forces in provinces to provide security assessments, and monitor the provision of information and intelligence pursuant to those arrangements;
- review arrangements entered into by the Service with foreign governments and their institutions or with international organizations of states and their institutions to provide security assessments, and monitor the provision of information and intelligence pursuant to those arrangements;
- review arrangements entered into and co-operation by the Service with departments of the federal government or with provincial governments and their departments, police forces in provinces, governments of foreign states and their institutions, or an international organization of states and its institutions, and monitor the provision of information and intelligence pursuant to those arrangements;
- review reports submitted at the direction of the Director of the Service involving potentially unlawful conduct by an employee of the Service;
- monitor requests made to the Service by the Minister of National Defence or the Minister of Foreign Affairs to assist, within Canada, in the collection of information or intelligence relating to foreign states and persons;

- review the regulations; and
- compile and analyze statistics on the operational activities of the Service.[205]

Another important element of SIRC's mandate is to ensure that CSIS activities are carried out in accordance with the Act, regulations and ministerial directions, and that the activities "do not involve any unreasonable or unnecessary exercise by the Service of any of its powers,"[206] by tasking CSIS or the IG to review particular matters and report back to it or, "where it considers that a review by the Service or the Inspector General would be inappropriate, conduct[ing] such a review itself."[207]

In addition to matters that form part of SIRC's regular reviews, SIRC may, on request by the Minister or at any other time, furnish the Minister with a special report concerning any matter that relates to the performance of its duties and functions.[208] Since 1984, SIRC has produced approximately 37 reports under section 54 on matters ranging from inquiries into particular allegations, such as a report to the Minister on the role of CSIS in relation to Maher Arar, to more systemic matters, such as the two 1998 reports on CSIS co-operation with the RCMP.

SIRC has the mandate to investigate two categories of complaints: complaints made with respect to "any act or thing done by the Service"[209] and complaints relating to the denial of security clearance for federal government employees or prospective employees, as well as for federal government contractors.[210]

SIRC also has a mandate to conduct investigations in relation to:

(a) reports made to SIRC by the Minister of Citizenship and Immigration pursuant to section 19 of the Citizenship Act regarding a proposal to refuse to grant citizenship or to issue a certificate of renunciation on the basis that there are reasonable grounds to believe the person will engage in activities constituting a threat to Canada or are a part of a pattern of criminal activity to further the commission of an indictable offence; and
(b) matters referred to SIRC by the Canadian Human Rights Commission pursuant to section 45 of the *Canadian Human Rights Act*, where a Minister advises the Commission that the practice to which a complaint under the Act relates is based on considerations relating to Canada's security.[211]

3.1.2 Review

CSIS has designated specific CSIS liaison officers to respond to SIRC's requirements. Since most of the material provided by CSIS is classified as secret or top

secret, SIRC reviews the material at CSIS Headquarters in order to avoid the risk involved in transporting it between CSIS and SIRC premises. CSIS has made available a separate office and computers at CSIS Headquarters for the exclusive use of SIRC staff. SIRC staff are designated as persons permanently bound to secrecy pursuant to the *Security of Information Act*.[212]

The standards that SIRC applies in evaluating CSIS activities are contained in four main instruments, which form the legislative and policy framework governing CSIS:

- The *Canadian Security Intelligence Service Act* is the founding legislation for both CSIS and SIRC.
- Ministerial directions, the principal means by which the Minister of Public Safety (the Minister) exercises his or her authority over CSIS as set out in section 6 of the Act, provide overall policy guidance to the Director of CSIS and govern a wide spectrum of CSIS activities; all ministerial directions and changes thereto are reviewed by SIRC.
- National requirements for security intelligence, issued by the Minister each year, provide CSIS with direction on where it should focus its investigative efforts and how it should fulfil its intelligence collection, analysis and advisory responsibilities.
- CSIS operational policies provide rules governing the entire range of operational activities. SIRC reviews all operational policy revisions on an ongoing basis.[213]

Each year, SIRC develops a research plan. Because of its small size in relation to CSIS, it operates on the basis of risk management.[214] Each year, it selects topics for in-depth inquiries, based on the following factors, among others:

- CSIS investigative priorities;
- particular activities with a significant potential to intrude on individual rights and freedoms;
- emerging priorities and concerns for Parliament and the Canadian people;
- the CSIS Director's classified report to the Minister on operational activities;
- the importance of producing regular assessments of each of the Service's operational branches, regional offices and selected Security Liaison Officer (SLO) posts abroad;
- the need to examine all of the services, duties and functions on a regular basis;
- developments with the potential to represent threats to the security of Canada;

- issues or concerns identified in previous Committee reports;
- commitments by the Committee to re-examine specific matters;
- issues identified in the course of the Committee's complaints functions; and
- new policy directions or initiatives announced by CSIS or the Government of Canada.[215]

In 2004–2005, for example, SIRC carried out 11 reviews and a section 54 inquiry. The 11 reviews included an examination of CSIS' investigation of transnational criminal activity, focussing on the targeting processes outlined in operational policy; information collection; and co-operation and exchanges of information with domestic and foreign partners. It also reviewed a counter-terrorism investigation, the activities of a CSIS regional office, a counter-proliferation investigation, CSIS' information operations centre, CSIS' exchanges of information with close allies, a counter-intelligence investigation regarding the activities of a foreign intelligence service,[216] CSIS' investigation of terrorist financing activities in Canada, and the terrorist entity listing process.[217] In 2002–2003, SIRC undertook a review of regional investigations that it described as relating to "Sunni Islamic Extremism" and a review of the matter of Ahmed Ressam. In 2001–2002, the topics for in-depth inquiry included source recruitment and domestic extremism.

In conducting these in-depth inquiries, SIRC typically reviews all relevant documents and files, both electronic and hard-copy, in the possession or control of CSIS. These include targeting authorizations, warrants and their supporting documents, operational reports, human source logs, internal CSIS correspondence, and records of exchanges of information with other agencies and departments, including international agencies, where relevant. SIRC also conducts interviews of CSIS personnel, seeks clarification on information reviewed, requests answers to follow-up questions and receives briefings from CSIS staff. Classified information is supplemented, where appropriate, with an in-depth review of open-source or public information.

In addition to conducting its selected reviews, SIRC reports on other operational activities, the investigation of complaints, CSIS accountability mechanisms, and inquiries under the *Access to Information Act* and *Privacy Act*. Examples of how SIRC discharges its mandate are provided below.

Targeting

Within CSIS, the Target Approval Review Committee (TARC) is the senior operational committee charged with considering and approving applications by CSIS officers to launch investigations.[218] TARC is chaired by the Director of CSIS and

includes senior CSIS officers and representatives from the departments of Justice Canada and Public Safety and Emergency Preparedness Canada.[219] In the course of its in-depth reviews, SIRC examines selected targeting authorizations made by TARC to ensure compliance with the *CSIS Act*, ministerial directions and relevant operational policies. Each year, SIRC reviews targeting authorizations in a selected region as part of the regional review.

In conducting its reviews, SIRC examines such issues as whether:

- CSIS had reasonable grounds to suspect a threat to the security of Canada in seeking its targeting approval;
- the level and intrusiveness of the investigation was proportionate to the seriousness and imminence of the threat;
- CSIS collected only that information strictly necessary to advise the government of a threat;
- in conducting its investigations, CSIS respected the rights and civil liberties of individuals and groups; and
- information exchanges with other agencies conformed with the law, ministerial direction and relevant MOUs.[220]

An example of the type of targeting reviewed by SIRC is "issue-based" targeting. This type of targeting authorizes an investigation to take place in circumstances where CSIS suspects a threat to the security of Canada, but the particular persons or groups associated with the threat have not been identified. The targeting authority allows CSIS to "investigate the general threat and to try to identify the persons or groups who are taking part in threat-related activities."[221]

After reviewing this activity in its 1998–1999 report, SIRC determined that there was a place for issue-based targeting in the array of options legally available to CSIS, adding the caveat that investigations under issue-based targeting authorities should be carefully monitored by senior management and urging the Service to "make every effort to make the transition from issue-based to individual (identity-based) targeting as expeditiously as . . . reasonable."[222]

In 2002–2003, SIRC identified some concerns regarding the termination of investigations in a timely manner where the activities of the target no longer constituted a threat. In its report for that year, it recommended that "CSIS maintain a strict awareness of operational policy and executive directive requiring the timely termination of targeting authorities in the absence of targets' threat-related activity."[223]

Foreign Intelligence

Foreign intelligence refers to information about the "capabilities, intentions or activities" of a foreign state or person. Under section 16 of the *CSIS Act*, CSIS may collect foreign intelligence at the written request of the Minister of Foreign Affairs or Minister of National Defence and with the approval of the Minister of Public Safety. The collection must take place in Canada and may not be directed against Canadian citizens, permanent residents or Canadian companies. SIRC regularly examines Ministers' requests for section 16 operations. It scrutinizes the requests to ensure compliance with the Act and with a government MOU stipulating that any request must contain an explicit prohibition against targeting Canadians, permanent residents and Canadian companies, and that the request should indicate whether the proposed activity is likely to involve Canadians.[224]

Part of SIRC's scrutiny of section 16 requests involves the review of working files, which may reveal errors. For example, in its annual report for 1997–1998, SIRC reported an instance where CSIS had mistakenly intercepted the communications of a person for three days, though no information had been collected or retained. SIRC also scrutinizes the appropriate retention of foreign intelligence. In the event that CSIS chooses not to retain section 16 information for a domestic (section 12) investigation, SIRC's jurisdiction ends once the material has been provided to the requesting Minister.[225]

When reviewing section 16 activities, SIRC scrutinizes CSIS requests for information made to the CSE to ensure that they are appropriate and comply with existing law and policy. The reports that CSE provides to CSIS are "minimized" in order to comply with the prohibition on the collection of information on Canadian nationals and Canadian companies. For example, the actual identity of Canadians contained in CSE reports provided to CSIS is shielded by employing phrases such as "a Canadian business person." In specific circumstances, however, CSIS may request identities from the CSE if it can show that the information relates to activities that could constitute a threat to the security of Canada.[226] In its 2000–2001 report, SIRC reported one request that had involved a prominent Canadian who had been approached by a foreign national, and a second request concerning a sensitive institution (trade union, media organization, religious body or university campus) involved in political campaigns in a foreign country. CSIS informed SIRC that the information obtained had been removed from its files following the SIRC review in which the problem had been identified.[227]

Access to the foreign intelligence (section 16) database is restricted to those CSIS employees who have received special clearance and indoctrination. The

database is not accessible to intelligence officers involved only in domestic investigations pursuant to section 12 of the *CSIS Act*. SIRC examines the procedures in place to ensure the section 16 database is not accessible to those who do not have a need to know.

Foreign Arrangements

SIRC reviews a number of elements pertaining to foreign arrangements. It looks at the written arrangements entered into by CSIS with individual foreign intelligence services, which establish the scope of co-operation with those services. It scrutinizes new arrangements or the expansion of existing ones to determine compliance with the *CSIS Act* and ministerial directions and the Minister's conditions for approval. SIRC also examines information relevant to the human rights record of the foreign intelligence service's host country, including open-source reporting from reputable human rights agencies. SIRC flags relationships where CSIS must be vigilant in ensuring that no information received from an agency is the product of human rights violations and that no intelligence transferred to a foreign agency results in such abuses.

SIRC also examines the information exchanged under specific foreign arrangements in the course of its regular reviews of individual Security Liaison Officer (SLO) posts abroad.[228] In the context of such reviews, it looks at CSIS relations with foreign security and intelligence agencies, the management of controls over the dissemination of CSIS information, post profiles and foreign agency assessments prepared by SLOs, the nature of information collected and disclosed, and developments specific to the foreign agencies within a given post's ambit.[229]

SIRC also scrutinizes information sharing. In its annual report for 1997–1998, for example, it noted that CSIS had handled a request from a Canadian law enforcement agency to ask several allied intelligence services to conduct records checks on more than 100 people suspected of being involved in transnational crime. SIRC found the grounds for some of the requests to be of doubtful validity. For instance, it noted that information had been requested about a person said to have been "caught shoplifting."[230]

In the course of its work, SIRC may identify situations where policies are silent or inadequate. In such cases, SIRC will make recommendations. For example, in 2004–2005, SIRC recommended that, instead of relying on guidelines, CSIS create formal policies for the preparation, updating and annual submission of CSIS documents used to assess exchanges with foreign agencies, particularly given the Service's growing exchanges with foreign organizations.[231]

Warrants

SIRC annually reviews a number of aspects of CSIS use of Federal Court warrants, such as warrant acquisition and implementation, court decisions and regulations. It also collects warrant statistics. As SIRC stated in its report for 2001–2002:

> Warrants are one of the most powerful and intrusive tools in the hands of any department or agency of the Government of Canada. For this reason alone, their use bears continued scrutiny, which task the Committee takes very seriously. In addition, our review of the Service's handling of warrants provides insights into the entire breadth of its investigative activities and is an important indicator of the Service's view of its priorities.[232]

In the context of a review, SIRC may select some warrant applications for review. In such cases, SIRC examines all documents relating to how the warrant applications were prepared, including affidavits and supporting documentation, working files relating to affidavits, requests for targeting authority, and TARC minutes. In reviewing this documentation, SIRC seeks to ascertain whether:

- the allegations in the affidavits are factually correct and are adequately supported in the documentation;
- all pertinent information is included in the affidavits; and
- the affidavits are complete and balanced, and the facts and circumstances of the cases are fully, fairly and objectively expressed.[233]

In its 1998–1999 report, for example, SIRC indicated that it had reviewed three applications in a given region relating to two target groups in the counter-terrorism area and had "identified a number of statements made by the Service which accurately reflected neither the operational nor the open source information available to the Service."[234]

In regard to warrant implementation, SIRC reviews a selection of active warrants in a given region in order to ensure that warrant powers have been properly implemented, assess the use of powers granted in the warrant and determine whether CSIS has complied with all clauses and conditions contained in the warrants. SIRC also determines whether or not, in its implementation, CSIS has met the "strictly necessary" test for collecting information set out in section 12 of the *CSIS Act*.

3.1.3 Complaints

One of SIRC's functions under the *CSIS Act* is to conduct investigations in relation to:

- complaints "with respect to any act or thing done by the Service" as described in the *CSIS Act*;
- complaints relating to denials of security clearances to federal government employees and contractors;
- matters referred by the Canadian Human Rights Commission, where the complaint raises considerations relating to Canada's security; and
- Minister's reports in respect of the *Citizenship Act*.[235]

Examples of the kinds of complaints that SIRC investigates with respect to "any act or thing" include:

- allegations of unreasonable delay in conducting a security screening investigation;
- allegations that CSIS failed to investigate threats to the security of Canada; and
- allegations of improper investigation of lawful advocacy, protest and dissent.

From the time of its inception to March 31, 2005, SIRC received 883 cases (not including complaints dealing with the application of the *Official Languages Act* in the workplace). These cases consisted of:

- 711 complaints filed pursuant to section 41 of the *CSIS Act* (any act or thing);
- 131 complaints filed pursuant to section 42 (denial of security clearance);
- 17 complaints regarding citizenship issues;
- 11 complaints regarding immigration issues; and
- 13 files referred from the Canadian Human Rights Commission.

The total number of cases is not indicative of the number of complaints SIRC accepted jurisdiction to investigate. When SIRC receives a complaint, it performs a preliminary review to determine whether it has jurisdiction. Some matters may not be within its mandate. Others may be resolved without an investigation. Moreover, under section 41 of the *CSIS Act*, SIRC may not accept jurisdiction if it determines that the complaint is trivial, frivolous or vexatious or was made in bad faith, or that the complaint is subject to a grievance procedure

established under the *CSIS Act* or the *Public Service Labour Relations Act*.[236] SIRC has produced 118 written reports following investigations of complaints involving either a written or oral hearing from the time of its creation to March 31, 2005.

Approximately 20 percent of SIRC's resources are currently devoted to investigation and hearing of complaints: about 15 percent to investigations and 5 percent to hearings.

Where a complaint leads to a hearing, there are special procedures set out in the *CSIS Act* and in SIRC's Rules of Procedure[237] designed to balance the individual's procedural fairness interests with the government's national security concerns.

When SIRC determines that it has jurisdiction to investigate a complaint under section 42 (security clearance denial), it must send a statement to the complainant summarizing such information available to SIRC "as will enable the complainant to be as fully informed as possible of the circumstances giving rise to the denial of the security clearance."[238] Where the Canadian Human Rights Commission refers a complaint to SIRC, SIRC must also provide a statement to the complainant summarizing the information available to it on the circumstances giving rise to the referral.[239]

Hearings of complaints are conducted *in camera.* SIRC has the power to summon witnesses, compel the production of documents, and administer oaths.[240] The complainant, CSIS and relevant departments are all given the right to make representations to SIRC, present evidence, and be represented by counsel. However, the *CSIS Act* provides that "no one is entitled as of right to be present . . ., to have access to or to comment on representations made . . . by any other person."[241]

SIRC's Rules of Procedure applicable to all its investigations provide for discretionary disclosure of evidence and representations to parties, subject to section 37 of the Act. They provide that it is within the discretion of the member conducting the investigation, in "balancing the requirements of preventing threats to the security of Canada and providing fairness to the person affected,"[242] to disclose the representations of one party to one or more of the other parties.

The Rules of Procedure provide for similar discretion to determine whether a party may cross-examine witnesses called by other parties and to exclude parties during the giving of evidence.[243] In the case of an *ex parte* hearing (where parties are excluded), SIRC counsel will cross-examine witnesses. As one commentator has noted:

> [S]ince committee counsel has the requisite security clearance and has had the opportunity to review files not available to the complainant's counsel, he or she is

> also able to explore issues and particulars that would be unknown to the complainant's counsel.[244]

When a party is excluded from a hearing for reasons of national security, it is within the discretion of the presiding member, subject to section 37 of the Act and after consultation with the Director of CSIS, to provide the excluded party with a summary of the evidence given or representations made.[245]

The Supreme Court of Canada has considered SIRC's Rules of Procedure and has held that the rules recognize and strike a fair balance between the competing interests of the individual in fair procedures and the state interest in effectively conducting national security and criminal intelligence investigations and protecting police sources.[246] The court held that the individual should be given sufficient information to know the substance of the allegations and be able to respond, but details such as criminal intelligence investigation techniques and police sources were not required to be disclosed.

3.1.4
CSIS and RCMP

Since its creation, SIRC has regularly examined CSIS-RCMP co-operation by conducting specific reviews and obtaining annual updates from CSIS on information exchanges and the nature of the relationship. Among the Service's domestic liaison partners, the RCMP is the body to which SIRC has always paid particular attention. The CSIS-RCMP relationship and roles are the cornerstone of the threat assessment and national security matrix. Four studies warrant specific mention: CSIS Cooperation with the RCMP – Part I (1997–98), CSIS Cooperation with the RCMP – Part II (1998–99), Review of Transnational Criminal Activity (1998–99), and SIRC's review of Project Sidewinder (1999–2000).

The goal of CSIS Cooperation with the RCMP – Part I (hereinafter referred to as Part I) was to identify systemic problems in the relationship between CSIS and the RCMP that would impact on the ability of either agency to fulfil its responsibilities, and in the Memorandum of Understanding (MOU), the principal instrument in which the nature of the co-operative arrangement is articulated. Part I looked at the use of liaison officials, located at headquarters and in regional offices of both agencies, as the primary channel for the exchange of operational information and intelligence. Liaison staff were given conditional access to material, in that the generating agency decided whether or not to accede to requests for further disclosure to, or use of the information by, the other agency. Part I noted the tension created by the differences regarding disclosure of information. CSIS placed restrictions on the material and intelligence it passed on

to the RCMP in order to avoid exposing sources and investigative methods in the course of a legal proceeding. RCMP investigators expressed frustration at the impediment to the exercise of their responsibility to take enforcement action.

Part I also reported on what was, at the time, a relatively new area of overlapping operational activity, transnational crime, stating that the lack of clarity regarding the respective roles of CSIS and the RCMP resulted in confusion as to expectations and areas of responsibility.

CSIS Cooperation with the RCMP – Part II (Part II) examined the CSIS-RCMP operational relationship and, more specifically, contacts and co-operation between the Service's regional offices and the corresponding RCMP geographic divisions. The report noted the RCMP's dissatisfaction with restrictions placed by CSIS on disclosure of its information in light of the legal requirements for discovery and disclosure inherent in criminal proceedings.

Part II also followed up on the Service's collection of strategic intelligence on transnational criminal activity and the confusion about the role of CSIS. The report concluded that there was no evidence to support the RCMP's view at that time that CSIS was withholding intelligence on transnational criminal activity.

The Review of Transnational Criminal Activity (TCA Review) examined whether CSIS activities — limited in this investigation to the collection of strategic intelligence — were consistent with its mandate, whether they distinguished between and respected the investigative thresholds for strategic and tactical intelligence, and whether CSIS shared information on transnational criminal activity with the RCMP. The TCA Review report concluded that the distinction between strategic and tactical intelligence was not adequately defined, CSIS found it difficult to avoid the collection of tactical intelligence, and CSIS should leave the matter of transnational crime to the appropriate law enforcement agencies unless it could bring a unique perspective to the area.

SIRC's review of Project Sidewinder focused on the activities and findings of a joint CSIS-RCMP project that the media alleged had been aimed at examining efforts by the Government of the People's Republic of China and Asian criminal gangs to influence Canadian business and politics. The review revealed significant differences of opinion and institutional perspective between CSIS and RCMP, but concluded that they were was not symptomatic of a more widespread problem. There were differences of opinion about what constituted good strategic analysis, but they had not had a lasting negative impact on the broader CSIS-RCMP relationship.

With regard to the participation of CSIS in INSETs across Canada, SIRC is limited to receiving information about and assessing CSIS' involvement in and

contribution to the teams. It does not have authority to assess the workings of INSETs, the use of the information they receive or the role of the RCMP.

3.1.5
SIRC and Other Review Bodies

SIRC meets periodically with the Inspector General of CSIS to discuss issues of mutual interest, and staff from the Inspector General's office and SIRC meet to exchange and discuss their respective review plans. This allows SIRC to share observations regarding specific CSIS investigations and avoid duplication in the review of CSIS activities in a given fiscal year. Identification of operations being examined by the Inspector General helps SIRC to set priorities. While SIRC has the authority under the *CSIS Act* to direct the Inspector General to conduct a review of specific activities and report to it with its findings, it does so very infrequently.

There is no legislated requirement for SIRC to meet or consult with the Communications Security Establishment (CSE) Commissioner. As a practical matter, SIRC participates on a regular basis in international conferences and symposia and has regular contact and discussion with foreign review agencies and oversight bodies.

3.1.6
Obtaining Information

In carrying out its review function, SIRC is entitled to full access to all information it requires from CSIS and the Inspector General, save Cabinet confidences.[247] It thus regularly sees information provided by foreign governments and agencies, some of which may be covered by caveats. Although the *CSIS Act* gives it the authority to do so, SIRC generally does not access documents subject to solicitor-client privilege. However, it has been provided with summaries and excerpts of legal opinions, as well as oral briefings by CSIS counsel providing explanations of legal advice. The legal advice has become material in the conduct of reviews where SIRC is seeking to determine whether CSIS has acted in accordance with legal advice from the Department of Justice Canada and, as such, has acted lawfully in carrying out its operations.

SIRC's powers are limited to the activities of CSIS. Where an intelligence function or product moves from CSIS to another body, SIRC lacks the legal authority to follow it to determine how information was used by the recipients. It cannot confirm that information to which caveats were attached was properly handled and secured by a receiving body. If a department or agency shares CSIS information with a third party without seeking CSIS' consent, SIRC will only

learn of the matter if CSIS has a record of the third-party disclosure. Obviously, an agency that chooses to act in this manner is unlikely to inform CSIS.

While SIRC has recommendation powers only, complaint reports may recommend amendments to existing administrative measures either by CSIS or by government ministries or departments in cases involving security clearance. SIRC once recommended that a complainant be compensated by CSIS for the legal costs of the proceeding before SIRC. In another instance, it recommended financial compensation. At times, it has recommended that the Deputy Head grant the complainant the security clearance that had been previously denied or revoked.[248]

In cases of investigations regarding the revocation of security clearance or referrals from the Canadian Human Rights Commission pursuant to section 45(2) of the *Canadian Human Rights Act*, SIRC may access documents held by whatever federal department or agency is named in the complaint.

3.1.7
Reporting by SIRC

SIRC reports to Parliament annually, through the Minister.[249] It may also furnish the Minister with a special report concerning any matter that relates to the performance of its duties and functions, on request by the Minister or at any other time.[250] SIRC has produced about thirty-seven such special reports since 1984, some of which have involved relatively high profile issues that have come before the public, such as the bombing of Air India Flight 182, the Heritage Front affair, and the role of CSIS in relation to Maher Arar.

SIRC reports on both its review and complaint investigation functions. It has powers to make findings and recommendations only, and the Supreme Court of Canada has held that such recommendations are not binding on the government.[251] Following an investigation of a complaint about "any act or thing done by the Service," SIRC reports to both the Minister and the Director of CSIS with its findings and recommendations; it also reports its findings and may, if it thinks fit, report any recommendations to the complainant. In the case of an investigation of a complaint about a denial of a security clearance, it reports to the Minister, the Director of the Service, the deputy head of the department or agency concerned and the complainant. The report includes any recommendations it considers appropriate, along with "those findings of the investigation that the Committee considers it fit to report to the complainant."[252]

3.1.8 Inspector General of CSIS

The Office of the Inspector General reviews CSIS activities and is mandated to provide independent advice in their regard to the Minister.[253]

The Inspector General (IG) is responsible to the Deputy Minister of Public Safety[254] and is independent of CSIS.[255] The IG is meant to serve as the eyes and ears of the Minister of Public Safety with regard to the activities of CSIS,[256] providing independent assurance that CSIS complies with the law, ministerial direction and operational policy. However, the Inspector General is not an independent review body in the same way as SIRC or the CSE Commissioner.

The Inspector General's functions include:[257]

- monitoring CSIS compliance with operational policies;
- reviewing CSIS operational activities, including specific CSIS activities as directed by SIRC;
- reporting on CSIS compliance with the *CSIS Act* and directions from the Minister under section 6(2) of that Act; and
- submitting annual certificates to the Minister stating the extent to which the Inspector General is satisfied with the annual report of the Director of CSIS.[258]

In addition to formal certificates and reports, the IG provides ongoing advice or commentary in various forms to the Minister, Deputy Minister and CSIS in relation to compliance matters and the effectiveness of the control/accountability framework. The Minister may also, on occasion, ask that certain reviews be conducted.[259]

The IG provides SIRC with copies of its reports, and the annual certificates from the IG (verification of the CSIS Director's annual reports) are transmitted to SIRC by the Minister.[260] SIRC meets periodically with the IG to discuss issues of mutual interest and respective review plans.

No provisions exist for publication of IG reports, although parts have from time to time been declassified in redacted form in response to Access to Information requests, and redacted copies of the annual certificates are posted on the website of the Office of the Inspector General.[261] Other IG reports are submitted to the Minister, but not made public.[262]

The Inspector General informed the Commission that, in selecting matters to review, she attempts to ensure that they are as representative as possible of CSIS activities, the different branches and the different regions of Canada. Decisions about what to review are based on what the IG has learned in

previous years or through core studies, what is topical or high-risk, and what matters may be of interest to the government and Minister.[263] Consultations with SIRC help to avoid duplication and thus make the most effective use of the limited resources of both the IG and SIRC.

The types of review of CSIS activities conducted by the IG and discussed in past annual certificates include:[264]

- review of warrant applications, target choices[265] and human source case management;
- detailed examinations of investigations of threats posed, including domestic extremist investigations and counter-intelligence investigations;
- review of section 16 intelligence collection (information concerning foreign states and persons);
- special studies of the Service's domestic liaison arrangements;
- comprehensive briefings on the front-end screening programs of refugee claimants;
- discussions with senior management at Headquarters and in the field (Vancouver, Edmonton, Toronto, Montreal and Halifax);
- inspection of CSIS internal documents (branch accountability reports);
- inspection of physical surveillance operations;
- a special study of government security screening; and
- review of cases reported to the IG by the Director where CSIS employees contravened internal policies.

The IG has unrestricted access to any information under the control of CSIS that he or she deems necessary for the discharge of his or her responsibilities. The *CSIS Act* is quite clear that, with the exception of Cabinet confidences, "[n]o information . . . may be withheld from the Inspector General on any grounds."[266] The IG also has access to all CSIS personnel.

3.2
OFFICE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

The Office of the Communications Security Establishment Commissioner (CSE Commissioner) was created in 1996, although it had no legislative basis until 2001. Initially, the CSE Commissioner was directed by Order in Council "to review the activities of the [CSE] for the purpose of determining whether those activities are in compliance with the law."[267] The many legislative amendments contained in the *Anti-terrorism Act* passed in December 2001 included an

amendment to the *National Defence Act*[268] enshrining the role of the CSE and the CSE Commissioner.

The Act provides that the Governor in Council may appoint a supernumerary judge or a retired judge of a superior court as CSE Commissioner for a term of not more than five years.[269] In carrying out his or her duties, the Commissioner has all the powers of a commissioner under Part II of the *Inquiries Act*, including the power to summon witnesses and hear evidence under oath. The Commissioner is empowered to engage the services of legal counsel, technical advisers and assistants.[270]

The *National Defence Act* sets out the duties of the CSE Commissioner as follows:

(a) to review the activities of the Establishment to ensure that they are in compliance with the law;
(b) in response to a complaint, to undertake any investigation that the Commissioner considers necessary; and
(c) to inform the Minister and the Attorney General of Canada of any activity of the Establishment that the Commissioner believes may not be in compliance with the law.[271]

The CSE Commissioner is required to submit an annual report to the Minister on the Commissioner's activities and findings, to be tabled before Parliament.[272] The Commissioner also provides the Minister with classified reports. In the Annual Report for 2005–2006, the CSE Commissioner stated that his main role was to give assurances to the Minister of National Defence that the intrusive powers granted to the CSE by Parliament were used in accordance with the legislation.The CSE Commissioner also maintains relationships with other review bodies both in and outside Canada. In 2005–2006, the Commissioner initiated what has come to be known as the Review Agencies Forum, involving staff from the Office of the CSE Commissioner, SIRC, the Office of the Inspector General of CSIS, and the CPC. The Forum provides an opportunity for staff of the review agencies to discuss issues of mutual interest and concern and identify best practices in review.[273]

3.2.1 Review Function

As part of the review function, the Commissioner monitors control and accountability mechanisms, the scope and application of policies and procedures, employee training programs, internal investigations and complaints, use and retention of collected information, and use of technology by the CSE.[274]

The *Anti-terrorism Act* expanded the CSE's foreign intelligence collection role to permit the Minister of National Defence to authorize interception of private communications of Canadians in certain circumstances, provided certain conditions are met.[275] In doing so, the Minister must be satisfied that measures taken by the CSE will protect the privacy of Canadians. The Commissioner is specifically directed to review activities carried out under each ministerial authorization to ensure that they comply with the authorization and to include his or her findings in the annual review.[276]

In the Annual Report for 2003–2004, the Commissioner reported on a general issue "about the structure of and process for using ministerial authorizations," noting that "[c]ertain weaknesses in policies and procedures related to these activities were brought to CSE's attention" and that some issues had been resolved, while others remained.[277] In the 2005–2006 Annual Report, the CSE Commissioner stated that his office had completed seven reviews, six of which had involved CSE activities carried out under ministerial authorizations, including one dealing with foreign intelligence collection and five dealing with information technology security. None of the reviews had reported unlawful conduct.[278]

In addition to reviews of ministerial authorizations, the Commissioner may conduct reviews of activities of the CSE to ensure they comply with the law. In 2005–2006, for example, the Commissioner examined the CSE's foreign intelligence collection activities directed at countering the threat posed by the proliferation of weapons of mass destruction and their delivery systems, and provided the Minister with a classified report setting out the findings of that review.[279] The CSE Commissioner is also completing a major, two-phased review of CSE activities in support of the RCMP (in the context of the CSE's mandate to inform the Minister and the Attorney General of Canada of any activity that may not be in compliance with the law).[280]

In carrying out the review function, the Commissioner has full access to all information in the CSE's possession and access to all CSE personnel.[281]

Upon completion of a review, the Commissioner provides a classified report to the Minister, with his or her opinion on the lawfulness of the activities reviewed and any recommendations he or she considers appropriate in the circumstances.[282]

3.2.2 Complaints Function

Any Canadian citizen or permanent resident of Canada may file a complaint regarding the lawfulness of CSE activities. The Commissioner has authority to

refuse to deal with a complaint if he or she deems it to be frivolous, vexatious or made in bad faith. Moreover, the Commissioner will not deal with a matter for which there are other avenues of redress or with a matter that arose with the complainant's knowledge more than a year before the complaint was filed. When the Commissioner's office receives a complaint, the Commissioner decides on the action to be taken based on the recommendations of the Complaints Review Committee. At this stage, conflict resolution methods may be used to resolve the complaint. If a formal investigation ensues, the Commissioner informs the complainant, the Chief of the CSE and the Minister of National Defence, and assigns an investigator. Following an investigation, the Commissioner prepares an interim report, with findings and recommendations. The Chief may be asked to respond, with details. The final report is then prepared and submitted to the CSE Chief and the Minister, and the complainant is advised in writing of the results of the investigation.[283]

I note that the vast majority of the Office's work involves conducting reviews rather than dealing with complaints.

3.2.3
Implementation of Recommendations

In the Annual Report for 2005–2006, the CSE Commissioner stated that 75 percent of the nearly 100 recommendations made by the CSE Commissioner since the office was established in 1996 had been accepted by the CSE and had been or were in the process of being implemented. Half of the remaining recommendations were under consideration or being implemented with some modifications. The remainder had been bypassed by events or had not been accepted by the CSE. Where the CSE either accepts recommendations with modifications or rejects them, CSE officials discuss the matters with the CSE Commissioner.[284]

4.
GENERAL REVIEW BODIES

The final review bodies that I discuss in this chapter are bodies with jurisdiction across the federal government. Such bodies are not restricted to any particular agency, such as the RCMP or CSIS, nor are they limited to an activity such as law enforcement or security intelligence. Their jurisdiction extends to both police and security intelligence agencies and all federal national security actors. The accountability bodies in question are the Information Commissioner of Canada, the Privacy Commissioner of Canada, the Canadian Human Rights Commission and the Auditor General of Canada.

4.1
OFFICE OF PRIVACY COMMISSIONER OF CANADA

The Office of the Privacy Commissioner of Canada was established under the *Privacy Act*, the purpose of which is to "extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information."[285] The Act also provides individuals with a right to request correction of personal information when there is an error or omission in that information.[286] The Office of the Privacy Commissioner is also responsible for overseeing compliance with the *Personal Information Protection and Electronic Documents Act*, which applies to personal information collection, retention, access, use and disclosure in the private sector.

In order to discharge his or her mandate, the Privacy Commissioner undertakes the following types of activities:

- investigation of privacy complaints (collection, retention, use and disclosure of personal information, and corrections to personal information);
- audits and reviews of government agencies and departments to examine compliance with the *Privacy Act* and assist in developing privacy management regimes; and
- research, public education and legal and policy analyses of bills, legislation and privacy issues and practices. A key part of this work is appearing before Committees of the Senate and House of Commons to provide expert advice on the privacy implications of bills and other policy matters under consideration by Parliament.[287]

National security affects the work of the Privacy Commissioner in several ways. For example, there are a number of statutory exemptions that allow government institutions to refuse individuals access to personal information about themselves, including access for the purpose of correcting erroneous personal information in the hands of government. In the national security context, the most relevant exemptions pertain to personal information obtained in confidence from governments of foreign states or foreign institutions, information the disclosure of which could be injurious to international affairs or defence, and information pertaining to law enforcement or investigations, or security clearances.[288]

In the course of investigations of complaints, the Privacy Commissioner has significant powers to compel the production of information, including the power to compel testimony under oath and to enter premises occupied by

a government institution and obtain copies of documents found on such premises.[289] By statute, the Privacy Commissioner has access to all information in control of a government institution "other than a confidence of the Queen's Privy Council for Canada" as defined in section 70(1) of the *Privacy Act*.[290]

Of relevance in the national security field is the fact that there are a number of "exempt banks," that is, whole collections of information exempt from the *Privacy Act*. By executive order, the following personal information banks are designated exempt: Criminal Operations Intelligence Records, under the control of the RCMP;[291] Canadian Security Intelligence Service Investigational Records, under the control of CSIS;[292] and National Security Investigations Records, under the control of the RCMP.[293] The Privacy Commissioner may conduct investigations of the files contained in such personal information banks, in the course of which he or she has the power to compel testimony under oath, enter premises and compel access to information.[294] Where, upon investigation, the Privacy Commissioner considers that files contained in an exempt personal information bank should not be contained therein, he or she must make a report containing findings and recommendations to the government institution that has control of the bank and may include that report in annual or special reports to Parliament.[295]

The Office of the Privacy Commissioner has been very engaged in privacy issues relating to national security, particularly since September 11, 2001. In discussing the review of privacy impact assessments, the Privacy Commissioner has specifically noted the trend of increased sharing of information among police and national security agencies for law enforcement and anti-terrorism purposes and has recommended the development of overall privacy management frameworks.[296] The Office has audited the Canada Border Services Agency (CBSA) and reviewed information regarding transborder data flows.[297] It has conducted compliance reviews of a number of federal national security actors, including the RCMP, CSIS and the CSE, to determine the extent to which the events of 9/11 have impacted privacy management practices. One of the Office's audit plan priorities is a review of exempt banks, which have not been audited in over fifteen years.[298] However, the Privacy Commissioner does not have the resources to thoroughly audit, review or investigate all national security actors.

The Privacy Commissioner, as an officer of Parliament, reports directly to Parliament through the Speaker of the House of Commons and Speaker of the Senate.[299]

4.2
OFFICE OF THE INFORMATION COMMISSIONER OF CANADA

The Supreme Court of Canada has recognized that the overarching purpose of access to information legislation is to facilitate democracy.[300] Such legislation helps ensure that citizens have the information required to participate meaningfully in the democratic process. It also plays an important role in transparency and helps ensure that politicians and bureaucrats remain accountable to the citizenry.

The Information Commissioner of Canada is an independent officer of Parliament who investigates complaints regarding access to information under the *Access to Information Act*. The right of access to information is subject to a number of exemptions. Of particular interest in the national security field are the exemptions contained in:

- section 13: information received in confidence from a foreign government, international organization of states, provincial, municipal or Aboriginal government;
- section 15: information the disclosure of which could reasonably be expected to be injurious to the conduct of international affairs, the defence of Canada or allied states, or the detection, prevention or suppression of subversive or hostile activity (including activities directed toward intelligence gathering, activities threatening the safety of Canadians, and activities directed toward the commission of terrorist acts); and
- section 16: information obtained in the course of investigations pertaining to such matters as crime prevention, law enforcement or activities suspected of constituting threats to the security of Canada within the meaning of the *Canadian Security Intelligence Service Act*.

The Commissioner has strong investigative powers. He or she may summon persons to appear before him or her and compel testimony under oath, enter premises occupied by a government institution, and examine or obtain copies of all records to which the *Access to Information Act* applies under the control of a government institution.[301]

The Act does not apply to confidences of the Queen's Privy Council (Cabinet confidences) as defined therein. In addition, where the Attorney General issues a certificate prohibiting disclosure of information under section 38.13 of the *Canada Evidence Act*, all proceedings in respect of a complaint are discontinued.[302] The Commissioner and persons acting on behalf of or under the direction of the Commissioner have access to information subject to caveats,

but are subject to a statutory confidentiality provision and a non-disclosure provision regarding information reviewed by them, but not ordered disclosed.[303]

Where a government institution denies access to information on the basis of national security, international affairs or defence, a complaint may only be investigated by one of four specially designated investigators within the Office of the Information Commissioner.[304] Those investigators must have top secret security clearance and the materials must be brought to secure premises at the Office for review. The purpose of the review is to determine whether the exemption properly applies to the records.

The Information Commissioner may also initiate complaints. In 2005–2006, the Commissioner initiated 760 complaints: 481 against the RCMP, 126 against the Privy Council Office, and 153 against DFAIT.[305] All pertained to delays in responding to existing access requests. The Information Commissioner has an annual caseload of approximately 2,000 cases. National security actors, including CSIS, the RCMP, the CSE, the CBSA, DFAIT and DND account for some 10 to 15 percent.

The Information Commissioner makes recommendations, but does not have binding order powers.[306] The Commissioner reports to Parliament through the Speaker of the Senate and Speaker of the House of Commons.[307]

In the hands of investigative journalists, academics and private citizens, the *Access to Information Act* has provided a tool for disclosure of information regarding various aspects of national security policy and performance. Indeed, much information in reports of review bodies such as SIRC and the IG has been disclosed only as a result of requests made under the *Access to Information Act*. However, some government departments and agencies have been critical of the perceived negative effect of the law on the operations of government.[308] The 2001 *Anti-terrorism Act* introduced several new limitations on access to national security information.[309] Some have argued that reasonable access to information consistent with national security is a constituent of any accountability system, and that the Information Commissioner in his or her capacity as an ombudsman or advocate on behalf of citizens seeking access plays an important role in an effective accountability mechanism.[310]

4.3
CANADIAN HUMAN RIGHTS COMMISSION

The Canadian Human Rights Commission deals with statutory human rights protection, including protection against discrimination in employment and services, in all areas of federal jurisdiction, under the *Canadian Human Rights Act*.[311] The Canadian Human Rights Tribunal, established pursuant to the

Act, holds public hearings into complaints of discrimination referred to it by the Commission.

A statutory gateway exists between the Commission and SIRC with respect to review of human rights issues with national security aspects. The *Canadian Human Rights Act* provides that, where a minister of the Crown provides written notice to the Commission that the practice to which a complaint relates is "based on considerations relating to the security of Canada," the Commission may dismiss the complaint or refer the matter to SIRC.[312] Under the *CSIS Act,* SIRC has the mandate to conduct an investigation into a matter referred to it by the Commission.[313]

Once a matter is referred to SIRC, the Commission must stay proceedings and refrain from dealing with the complaint until SIRC has provided a report on the matter.[314] SIRC has 45 days to provide its report to the Commission, the referring minister and the complainant.[315] Upon receipt of the report, the Commission must either dismiss the complaint or deal with it under the *Canadian Human Rights Act*.[316]

I note that a jurisdictional dispute has developed between SIRC and the Commission. The Chief Commissioner of the Commission, Mary Gusella, testified before the Subcommittee on Public Safety and National Security of the Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness that the interpretation of legislative provisions has led to legal and practical issues between SIRC and the Commission. Historically, the Commission referred human rights complaints involving national security issues to SIRC and SIRC advised it on how to deal with the complaints in a manner that respected those security issues, leaving the merits of the human rights aspects to the Commission.[317] However, according to the Commission, SIRC has begun to deal with the merits of the human rights complaints as well. The Commission's stated primary concern is to ensure that coordinated systems are acting to respect national security while protecting and promoting human rights.

Members of the Canadian Forces and the RCMP are deemed to be employed by the federal Crown.[318] However, the Commission will seek to have complaints against RCMP members dealt with initially by the CPC, in order to exhaust that avenue of redress first. It will only take such a complaint if it concludes that there is an outstanding discrimination issue after the matter has been dealt with by the CPC.[319]

The Commission may search premises pursuant to a judicially issued warrant, subject to "such limitations as the Governor in Council may prescribe in the interests of national defence or security."[320] A complaint investigator reports to the Commission, following which the Commission may dismiss the complaint,

refer the complainant elsewhere if appropriate, or request that the Chairperson of the Canadian Human Rights Tribunal institute an inquiry under section 49 of the Act.[321]

Members and employees of the Commission are specifically required under the *Canadian Human Rights Act* to comply with security requirements applicable to information they obtain and must take any applicable oath of secrecy. Furthermore, every Commission member and employee must take "every reasonable precaution" to avoid disclosing information the disclosure of which:

- might be injurious to international relations, national defence or security or federal-provincial relations;
- would disclose a confidence of the Queen's Privy Council for Canada;
- would be likely to disclose information obtained or prepared by any investigative body of the Government of Canada in relation to national security, in the course of investigations pertaining to the detection or suppression of crime generally, or in the course of investigations pertaining to particular offences against any Act of Parliament;
- might cause harm to sentenced individuals;
- might impede the functioning of a court of law, quasi-judicial board, commission, other tribunal or inquiry;
- might disclose legal opinions or advice provided to government or privileged communications between lawyer and client in a matter of government business.[322]

Provisions exist to deal with national security concerns where the Commission refers a matter to the Tribunal. While Tribunal hearings are public, the *Canadian Human Rights Act* stipulates that the member or panel conducting the inquiry may, on application, take any measures and make any order considered necessary to ensure the confidentiality of the inquiry if satisfied that:

(a) there is a real and substantial risk that matters involving public security will be disclosed

. . .

(d) there is a serious possibility that the life, liberty or security of a person will be endangered.[323]

Finally, the Act provides that, if an investigator or Tribunal member or panel requires the disclosure of any information and a minister of the Crown or any other interested person objects, the Commission may apply to the Federal Court for a determination of the matter and the Court may take any action it

considers appropriate. The objection to disclosure is determined in accordance with the *Canada Evidence Act*.[324]

Both the Commission and the Tribunal are required to report yearly to Parliament on their respective activities.

4.4
OFFICE OF THE AUDITOR GENERAL OF CANADA

The Office of the Auditor General of Canada audits a wide range of activities of the federal government and the three territories. Audits include financial, management effectiveness and performance audits. Historically, audits have covered a broad range of activities, including health, culture, the environment, finance, agriculture, transportation, and scientific research.[325] In recent years, they have included activities of the federal government in the area of national security. The Auditor General initiated the first ever audit of Ottawa's security and intelligence functions as a whole in the 1990s. Clearly identified as the first of a regular cycle, it was unprecedented in scope. In the ensuing report, the Auditor General was highly specific in recommendations for tightening controls and maintaining accountability in the Canadian intelligence community.[326]

The Auditor General's 1996 Report indicated that the audit had specifically examined the "arrangements in place for the control and accountability of Canada's intelligence community."[327] The audit dealt with topics such as the roles that should be played by the Prime Minister, responsible ministers, internal accountability mechanisms and external review bodies in holding national security actors to account.

In November 2003, the Auditor General issued another report, in which she assessed the level of external independent review over each agency either involved directly in or providing assistance with the collection of intelligence within Canada, including CSIS, the RCMP, DND, the CSE, the Canada Customs and Revenue Agency[328] and the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).[329]

In March 2004, the Auditor General audited the overall management of the initiative taken to enhance national security and intelligence coordination in response to 9/11.[330] The audit looked at specific issues, such as the interoperability of security and intelligence information systems and the sharing of information, fingerprint identification, the use of watch lists for border control, and the security clearance of airport workers requiring passes to restricted areas.[331] As with previous audits, the focus was on efficiency, proper management and accountability, not on specific operational details. An April 2005 report set out the results of audits of four government activities having national

security implications: the 2001 anti-terrorism initiative (a continuation of the earlier March 2004 audit in this domain), DND's C4ISR initiative[332] and activities at the Passport Office and Natural Resources Canada. Again, the focus was on whether public funds had been spent properly and managed well, rather than on operational details.[333]

The most recent report touching on national security was a November 2005 report, in which the Auditor General reiterated earlier calls for an increased role for Parliament in scrutinizing spending and performance in security and intelligence matters, in a context where detailed information is often required to be kept secret.[334]

4.4.1 Mandate

The Auditor General of Canada is an officer of Parliament who reports to the Standing Committee on Public Accounts of the House of Commons. He or she is required to do so annually, and may make no more than three additional reports in any year to the House, related to the work of his or her office and whether he or she is receiving all the information and explanations required. These reports are intended to call attention to anything that the Auditor General considers of significance and of a nature that should be brought to the attention of the House of Commons, including sufficiency of financial and other controls, the cost-effectiveness of government operations and the overall effectiveness of programs.[335]

The Auditor General may also produce special reports to the House of Commons on any matter of pressing importance or urgency that, in his or her opinion, should not be deferred until the presentation of the next regular report.[336] Moreover, when requested by the Governor in Council, he or she may inquire into and report on any matter relating to the financial affairs of Canada, public property, and any person or organization that has received financial aid from the government or for which government financial aid is being sought.[337]

The Auditor General conducts three different types of legislative audits as his or her central means of holding the government to account. The first type is the financial audit, which looks at whether the government is keeping proper accounts and records and presenting its financial information fairly. The next is a special examination of Crown corporations, a form of audit wherein the Auditor General provides an opinion on the management of the corporation as a whole. The third is the performance audit, the purpose of which is to determine whether programs are being run with due regard for economy, efficiency, effectiveness and environmental impact. Performance audits do not question

the merits of government policies. Rather, they examine the government's management practices, controls, and reporting systems based on its own public policies and on best practices.[338]

The Office of the Auditor General conducts approximately 30 performance audits a year in federal departments and agencies. The *Auditor General Act* gives the Office considerable discretion to determine what areas of government to examine when doing such audits. The Office begins planning its program of audits several years in advance, conducting a thorough risk analysis, identifying the areas most significant and relevant to Parliament, and taking into account such practical issues as the availability of its financial and human resources. According to the Office of the Auditor General, its focuses on areas in which federal government organizations face the highest risk — in other words, areas that cost taxpayers significant amounts of money or could threaten the health and safety of Canadians were something to go wrong. The Office may also deem a topic area significant if it is of great interest to parliamentarians and Canadians. The Auditor General has specifically cited national security as one such area.[339] The Auditor General will pay particular attention to audit requests from parliamentary committees, but the ultimate decision about what to audit rests with the Auditor General.[340]

Audit topics that fall outside the Office's mandate include, but are not limited to, policy decisions (the prerogative of Parliament and government) and areas under the exclusive jurisdiction of provincial or municipal governments.[341]

The Auditor General has extensive powers to obtain information. Under the *Auditor General Act*, he or she is entitled to access at all convenient times all information that relates to the fulfilment of his or her responsibilities and is entitled to receive from members of the federal public administration any information considered necessary for that purpose. The only exception is where another Act of Parliament specifically refers to this broad access to information provision and somehow contradicts it.

The Auditor General may examine any person on oath on any matter pertaining to any account subject to audit by him or her and, for the purposes of any such examination, may exercise all the powers of a commissioner under Part I of the *Inquiries Act*.[342]

Performance audits are quite extensive and may take up to 18 months to complete. They consist of a planning phase, an examination phase, and a reporting phase. The reporting phase incorporates an opportunity for the audited department or agency to correct facts and provide comments before the report is submitted to the House of Commons.[343]

The Auditor General notifies the Speaker of the House of his or her intention to table a report at least 30 days before the tabling date and provides a short summary of each audit topic. He or she notifies all members of Parliament and senators at this same time. About a week before the report is tabled, the Auditor General offers to brief ministers whose organizations are included in the report. Until then, the Office deals only with officials in the public service, giving them an opportunity to check facts, provide additional information, and respond to recommendations.[344]

All of the Auditor General's reports are automatically referred to the Standing Committee on Public Accounts for further review.[345] This and other parliamentary committees hold hearings to discuss issues raised in the report, after which the Public Accounts Committee may table a report in the House of Commons that includes recommendations to the government. The government is expected to table a response to the report within 150 days. These responses are approved by Cabinet.[346]

Notes

1 Canada, Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, Domestic Models of Review of Police Forces (Background Paper), Dec. 10, 2004, available on the Commission's website, www.aracommission.ca.

2 Officers Confidential Memorandum Number 10 as quoted in Canada, *Report of the Commission of Inquiry Relating to Public Complaints, Internal Discipline and Grievance Procedure within the Royal Canadian Mounted Police* (Ottawa: Information Canada, 1976), p. 40 (Chair: Judge René J. Marin) [Marin Commission report].

3 *An Act to amend the Royal Canadian Mounted Police Act and other Acts in consequence thereof*, S.C. 1986, c. 11.

4 Marin Commission report.

5 Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Freedom and Security Under the Law*, Second Report (Ottawa: Minister of Supply and Services Canada, 1981) (Chair: Justice David McDonald) [McDonald Commission report].

6 Marin Commission report, p. 69.

7 Ibid., pp. 102, 104–6.

8 Ibid., pp. 103,104.

9 Ibid., p. 102.

10 Ibid.,

11 Ibid., p. 103.

12 Bill C-43, *An Act respecting the office of the Ombudsman and matters related or incidental thereto*, S.C. 1977–78.

13 Marin Commission report, p. 102.

14 McDonald Commission report, vol. 2, p. 986.

15 Ibid., p. 970.

16 Ibid., p. 987 [emphasis in original].

17 Ibid., pp. 985–6.
18 Ibid., p. 988.
19 Ibid., p. 981.
20 Ibid., p. 967.
21 Ibid., p. 978.
22 Albert J. Reiss, Jr., *The Police and the Public* (New Haven, CT: Yale University Press, 1971), pp. 194–195, as quoted in the McDonald Commission report, vol. 2, p. 978.
23 McDonald Commission report, vol. 2, p. 971.
24 Ibid., p. 981.
25 *Alberta (A.G.) v. Putnam*, [1981] 2 S.C.R. 267. See also Donald J. Sorochan, "The APEC Protest, the Rule of Law, and Civilian Oversight of Canada's National Police Force," in W. Wesley Pue, ed., *Pepper in Our Eyes: The APEC Affair* (Vancouver: UBC Press, 2000), p. 67 [Sorochan].
26 Sorochan, p. 70.
27 *Royal Canadian Mounted Police Act*, R.S.C. 1985, c. R-10, ss. 45.42 (2)–45.42 (3) [*RCMP Act*].
28 Ibid., s. 45.35(1).
29 *Canada (Commissioner of the Royal Canadian Mounted Police)(Re)(C.A.)*, [1994] 3 F.C. 562 , pp. 586–87.
30 *An Act to amend the Royal Canadian Mounted Police Act and other Acts in consequence thereof*, S.C. 1986, c. 11.
31 SI/88-103 (proclaimed all of S.C. 1986, c. 11, except Part VII, in force June 30, 1988); SI/88-214 (proclaimed Part VII in force September 30, 1988). See *Royal Canadian Mounted Police Act (Can.) (Re) (C.A.)*, [1991] 1 F.C. 529.
32 Commission for Public Complaints Against the RCMP, Press Release, "New English Name for the RCMP Public Complaints Commission" (January 5, 2001), online, CPC, http://www.cpc-cpp.gc.ca/DefaultSite/NewsRoom/index_e.aspx?articleid=258 (accessed Aug. 23, 2006).
33 *RCMP Act*, s. 45.29(4). In addition to the Chair and Vice-Chair, there may be one representative for each of the provinces that contract for the services of the RCMP (after consultation with the province concerned) and up to three other appointees, plus alternates: Ibid., ss. 45.29(1)–45.29(2)
34 Paul Ceyssens, *Legal Aspects of Policing,* vol. 2 (Saltspring Island, B.C.: Earlscourt Legal Press, 2002), p. 7-13. [Ceyssens].
35 Canada, Commission for Public Complaints Against the RCMP, *2005-2006 Annual Report* (Ottawa: Minister of Public Works and Government Services, 2006), p. 3, online, http://www.cpc-cpp.gc.ca/app/DocRepository/1/AR0506_e.pdf (accessed Oct. 24, 2006). [CPC 2005/2006 Annual Report]; Canada, Commission for Public Complaints Against the RCMP, *2004-2005 Departmental Performance Report*, online, http://www.cpc-cpp.gc.ca/app/DocRepository/1/PDF/dpr0405_e.pdf (accessed Oct. 24, 2006) [CPC 2004-2005 Annual Report].
36 *RCMP Act*, s. 45.35.
37 Canada, Commission for Public Complaints Against the RCMP, *2004-2005 Annual Report* (Ottawa: Minister of Public Works and Government Services, 2005), p. 12, online, http://www.cpc-cpp.gc.ca/app/DocRepository/1/AR0405_e.pdf (accessed Aug.23, 2006). [CPC 2004/2005 Annual Report]; CPC 2005/2006 Annual Report, p. 9.
38 *RCMP Act*, s. 45.37.
39 CPC 2004/2005 Annual Report, p.15.
40 *RCMP Act*, ss. 45.35(2), 43.35(3).
41 In his testimony before the Commission, then RCMP Deputy Commissioner Garry Loeppky stated: "The investigation is done by the RCMP and the results are provided to the complainant and copied to the Commission": Loeppky testimony, Arar Commission Factual Inquiry Public Hearing (July 6, 2004), p. 1458. However, this occurs only if the complaint was originally

made to the CPC. See also Ceyssens, p. 7-46: "The Act does not require the Commission to monitor or even be notified of a complaint."

42 *RCMP Act*, s. 45.47.

43 Ibid., s. 45.36.

44 CPC 2004/2005 Annual Report, p. 30; CPC 2005/2006 Annual Report, p. 9.

45 *RCMP Act*, ss. 45.36(5), 45.36(6).

46 Ibid., s. 45.41

47 Ibid., s.45.42(3).

48 CPC 2005/2006 Annual Report, p.12.

49 *RCMP Act*, s. 45.43(1).

50 Ibid., s. 45.43(2).

51 "Press Releases," online, Commission for Public Complaints Against the RCMP, http://www.cpc-cpp.gc.ca/DefaultSite/NewsRoom/index_e.aspx?articleid=48 (accessed Aug. 23, 2006).

52 *RCMP Act – Part VII Subsection 45.45(14): Commission Interim Report* (2003), online, Commission for Public Complaints Against the RCMP, online, http://www.cpc-cpp.gc.ca/DefaultSite/Reppub/index_e.aspx?articleid=58 (accessed Aug. 23, 2006); W. Wesley Pue, *Pepper in Our Eyes: The APEC Affair* (Vancouver: UBC Press, 2000).

53 Commission for Public Complaints Against the RCMP, Press Release, "RCMP Public Complaints Commission to Hold Public Hearing into Incidents during the APEC Forum" (February 20, 1998), online, http://www.cpc-cpp.gc.ca/DefaultSite/Archive/index_e.aspx?articleid=266 (accessed Aug. 24, 2006).

54 Commission for Public Complaints Against the RCMP, News Release, "Commission for Public Complaints Against the RCMP Initiates Complaint into RCMP Conduct in Relation to the Deportation and Detention of Mr. Maher Arar" (October 23, 2003), online, http://www.cpc-cpp.gc.ca/DefaultSite/Archive/index_e.aspx?Articleid=463 (accessed July 28, 2006).

55 Canada, Commission for Public Complaints Against the RCMP, *Chair's Final Report Pursuant to Subsection 45.46(3) of the RCMP Act Following a Public Interest Investigation Pursuant to Subsection 45.43(1) of the RCMP Act with Respect to the Events of May 2 to 4, 1997 in the Communities of Saint-Sauveur and Saint-Simon, New Brunswick* (March 22, 2001), online, http://www.cpc-cpp.gc.ca/DefaultSite/Reppub/index_e.aspx?ArticleID=343 (accessed July 28, 2006).

56 Commission for Public Complaints Against the RCMP, News Release, "Mental Health Week: RCMP Officers Need Better Training" (May 4, 2004), online, http://www.cpc-cpp.gc.ca/DeafultSite/ Archive/index_e.aspx?Articleid=500 (accessed July 28, 2006).

57 Commission for Public Complaints Against the RCMP, News Release, "Commission for Public Complaints Against the RCMP Initiates a Public Interest Investigation into Allegations Involving Kingsclear Youth Training Center in New Brunswick" (May 27, 2004), online, http://www.cpc-cpp.gc.ca/DefaultSite/Whatsnew/index_e.aspx?ArticleID=504 (accessed Aug. 23, 2006).

58 CPC 2004/2005 Annual Report.

59 *RCMP Act*, s. 45.46(2).

60 Only cabinet documents may be withheld: *Canadian Security Intelligence Service Act*, S.C. 1984, c. 21, s. 39(3) [*CSIS Act*].

61 *CSIS Act*, s. 38.

62 Ibid., s. 6(2).

63 *RCMP Act*, s. 45.41(2)(b).

64 CPC 2004/2005 Annual Report, p. 35.

65 Ibid., pp. 35-37.

66 *RCMP Act*., s. 45.45(4).

67 Ibid., s. 45.45(11).

68 Shirley Heafey, "Civilian Oversight in a Changed World" (Speech delivered to the Canadian Institute for the Administration of Justice, March 26, 2002), p. 4, online, http://www.cpc-cpp.gc.ca/DefaultSite/NewsRoom/index_e.aspx?articleid=274 (accessed July 26, 2006).

69 Ibid., pp. 4–5. See also *Canada (Royal Canadian Mounted Police Public Complaints Commission) v. Canada (Attorney General)*, 2005 FCA 213.

70 *RCMP Act*, s. 45.34.

71 *Police Pursuits and Public Safety* (1999), online, Commission for Public Complaints Against the RCMP, http://www.cpc-cpp.gc.ca/DefaultSite/Reppub/index_e.aspx?articleid=94 (accessed July 27, 2006).

72 Unless otherwise attributed, information in this section is based on meetings and communications by the Arar Commission with the offices of the Military Police Complaints Commission and Canadian Forces Provost Marshal. I do not review the role of the Military Ombudsman in this chapter. The Ombudsman's mandate is specifically limited, in that it may not deal with matters that can be dealt with through existing mechanisms, such as SIRC, the MPCC and the CSE Commissioner. Thus, the Ombudsman is unlikely to review the national security activities of Canadian officials. The only exception is where compelling circumstances justify an investigation by the Ombudsman of a matter that would otherwise fall within the jurisdiction of SIRC or the MPCC.

73 The *Code of Service Discipline* is set out in the *National Defence Act*, Part III. See also *Criminal Code*, s. 2 (definition of "peace officer," (g)(i)); *National Defence Act*, s. 156.

74 *Criminal Code*, s. 2 (definition of "peace officer," (g)(ii)); *R. v. Nolan*, [1987] 1 S.C.R. 1212; *R. v. Haynes (N.S.C.A.),* [1994] N.S.J. No. 152.

75 Under s. 250.17 of the *National Defence Act*, the Chairperson of the MPCC must submit a yearly report to the Minister on the Commission's activities during that year, along with recommendations, if any. The Minister must, in turn, have a copy of the report laid before each House of Parliament on any of the first fifteen days on which that House is sitting after the Minister receives it.

76 *The First Independent Review by the Right Honourable Antonio Lamer P.C., C.C., C.D., of the provisions and operation of Bill C-25, An Act to amend the* National Defence Act *and to make consequential amendments to other Acts, as required under section 96 of Statutes of Canada 1998, c. 35*, submitted to the Minister of National Defence, September 3, 2003, p. 77, online, Canadian Forces Grievance Board, http://www.cfgb-cgfc.gc.ca/pdf/LamerReport_e.pdf (accessed Aug. 23 2006) [Lamer review]. See also *Updating Civilian Oversight of Canada's Military Police: Achieving Results for Canadians*, Special Report, pp. 3–4, online, Military Police Complaints Commission, http://www.mpcc-cppm.gc.ca/300/301_e.aspx (updated December 2005; accessed Aug. 22, 2006) (Interim Chairperson: Henry Kostuck) [Kostuck].

77 *National Defence Act*, R.S.C. 1985, c. N-5, as amended.

78 For an overview, see Military Police Complaints Commission of Canada, "Crisis in Building Confidence: A Brief to the Standing Committee on National Defence on Bill C-7, an Act to Amend the *National Defence Act*," May 31, 2006, pp. 3–6.

79 The Provost Marshal is the head of the Canadian Military Police and Commanding Officer of the Canadian Forces National Investigation Service (CFNIS).

80 From the time of its creation in December 1999 to approximately October 2004, the MPCC received 266 conduct complaints and six interference complaints. During this same period, it conducted 27 reviews in response to review requests and eight investigations in the public interest.

81 *National Defence Act*, s. 250.18.

82 *Complaints About the Conduct of Members of the Military Police Regulations*, App. 7.2, Vol. IV, *Queen's Regulations and Orders for the Canadian Forces*, approved by P.C. 1999–2065, November 18, 1999, s. 2.

83 Or the delegated Deputy Provost Marshal.

84 *National Defence Act*, ss 250.21, 250.26. If the complaint is about the conduct of the Provost Marshal, the Chief of the Defence Staff is responsible for dealing with the complaint and has all the powers and duties of the Provost Marshal. In practice, these duties of the Provost Marshal are delegated to the Provost Marshal's deputies: Military Police Complaints Commission, "Submissions with respect to the Independent Review of Bill C-25 (An Act to Amend the *National Defence Act*) to the Right Honourable Antonio Lamer," April 9, 2003, p. 9.

85 Meeting with Military Police Complaints Commission, September 8, 2004.

86 See Lamer review pp. 75–77 and Recommendation 60. See also Kostuck. (See note 76 for both.)

87 Canada, Bill C-7, *An Act to amend the National Defence Act*, 1st Sess., 39th Parl., 2006 (First Reading, April 27, 2006).

88 *National Defence Act,* ss. 250.21 (b) and 250.22.

89 Ibid., s. 250.3.

90 Ibid., s. 250.28.

91 Ibid., s. 250.29.

92 Ibid., s. 250.31(1).

93 Ibid., s. 250.31(2).

94 Ibid., ss. 250.38, 250.4.

95 Ibid., s. 250.32.

96 Ibid., s. 250.51.

97 Ibid., s. 250.53.

98 Ibid., s. 250.34.

99 Ibid., ss. 250.38**,** 250.41. During a public hearing, the MPCC may not receive any evidence or information that would be inadmissible in a court of law by reason of any privilege under the law of evidence; any answer given or statement made before a board of inquiry or summary investigation; any answer or statement that tends to criminate the witness or subject the witness to any proceeding or penalty and that was in response to a question at a hearing under Div. 3, Part IV of the Act into another complaint; any answer given or statement made before a court of law or tribunal; or any answer given or statement made while attempting to resolve a conduct complaint informally under s. 250.27(1).

100 *National Defence Act*, s. 250.42.

101 Ibid., s. 250.44.

102 Ibid., s. 250.45.

103 Arthur Maloney, *The Metropolitan Toronto Review of Citizen-Police Complaint Procedure: Report to the Metropolitan Toronto Board of Commissioners of Police* (1975) [unpublished, archived at Library of Public Safety and Emergency Preparedness Canada] [Maloney report].

104 Ibid., pp. 211–213.

105 Ibid., pp. 217, 223.

106 Ontario, *The Royal Commission into Metropolitan Toronto Police Practices* (Toronto: Royal Commission into Metropolitan Toronto Police Practices, 1976) (Commissioner: Hon. Justice Donald R. Morand).

107 Metropolitan Toronto, Task Force on Human Relations, *Now Is Not Too Late* (Toronto: Municipality of Metropolitan Toronto, 1977) (Chair: Walter Pitman).

108 Cardinal Gerald Emmett Carter, *Report to the Civic Authorities of Metropolitan Toronto and Its Citizens* (Toronto: Municipality of Metropolitan Toronto, 1979).

109 Clare E. Lewis, Sidney B. Linden, and Judith Keene, "Public Complaints Against Police in Metropolitan Toronto – The History and Operation of the Office of the Public Complaints Commissioner" (1986), 29 *Criminal Law Quarterly* 115, p. 119.

110 *An Act for the establishment and conduct of a Project in The Municipality of Metropolitan Toronto to improve methods of processing Complaints by members of the Public against Police Officers on the Metropolitan Police Force*, S.O. 1981, c. 43.

111 Ibid., s. 14(3).

112 Ibid., s. 15(2).

113 Ibid., s. 19(1).

114 Ibid., s. 19(14).

115 *An Act to revise the Metropolitan Police Force Complaints Project Act, 1981*, S.O. 1984, c. 63.

116 *An Act to revise the Police Act and amend the law relating to Police Services*, S.O. 1990, c. 10.

117 Ibid., ss. 78, 91(2).

118 Ibid., s. 74.

119 Ibid., s. 93(2).

120 Ibid., s. 97 (1).

121 *An Act for the establishment and conduct of a Project in The Municipality of Metropolitan Toronto to improve methods of processing Complaints by members of the Public against Police Officers on the Metropolitan Police Force*, S.O. 1981, c. 43, s. 19(12).

122 *An Act to revise the Police Act and amend the law relating to Police Services*, s. 97(1).

123 Roderick M. McLeod, *A Report and Recommendations on Amendments to the Police Services Act Respecting Civilian Oversight of Police* (Toronto: Miller Thomson, 1996). See generally Dianne L. Martin, "Legal Sites of Executive-Police Relations: Core Principles in a Canadian Context" (Paper delivered at the Ipperwash Inquiry / Osgoode Hall Law School Symposium, June 29, 2004), pp. 20ff, online, http://www.ipperwashinquiry.ca/policy_part/meetings/pdf/Martin.pdf#search=%22%22legal%20sites%20of%20executive-police%20relations%22%20%2B%20dianne%201.%20martin%22%22 (accessed July 13, 2006).

124 *An Act to revise the Police Act and amend the law relating to Police Services*, s. 35 (creating s. 57(1) of the *Police Services Act*).

125 *Police Services Act*, R.S.O. 1990, c. P.15, s. 56(1).

126 Ibid., ss. 22, 25(1)(a).

127 Ibid., s. 70; Ontario, *Consultation Report of the Honourable George W. Adams, Q.C. to the Attorney General and Solicitor General Concerning Police Cooperation with the Special Investigations Unit* (1998), online, Special Investigations Unit, http://www.siu.on.ca/adams.asp (accessed July 6, 2006) [Adams report 1998]; Hon. George W. Adams, *Review Report on the Special Investigations Unit Reforms prepared for the Attorney General of Ontario* (Toronto, 2003), online, Ministry of the Attorney General, http://www.attorneygeneral.jus.on.ca/english/about/pubs/adams (accessed July 6, 2006) [Adams review report 2003].

128 Murray W. Chitra, Chair, Ontario Civilian Commission on Police Services, *Policing in Canada: Structure and Accountability Mechanisms* (Paper delivered to the Policing and Police Commissions in Multi-Ethnic Societies Round Table, Colombo, Sri Lanka, February 21, 2003), p. 12.

129 *Police Services Act*, ss. 59(3), 59(4).

130 Ibid., s. 59(6).

131 Ibid., s. 61(2).

132 Ibid., s. 61(7).

133 Hon. Patrick J. LeSage, *Report on the Police Complaints System in Ontario* (2005), p. 28, online, Ontario Ministry of the Attorney General, http://www.attorneygeneral.jus.gov.on.ca/english/about/pubs/LeSage/en-fullreport.pdf (accessed July 13, 2006) [LeSage].

134 *Police Services Act*, ss. 64(2)–64(3).

135 Ibid., s. 64(6).

136 Ibid., ss. 64(11)–64(15). Note that such disposition is only permitted if the officer consents. Otherwise, a hearing is required.

137 *Police Services Act*, ss. 64(10), 68(1).

138 Ibid., s. 71(1).

139 Ontario Civilian Commission on Police Services, Annual Report 2004 , online, OCCPS, http://www.occps.ca/englishwebsite/aboutoccps/annualreport2004.pdf (accessed Oct. 24, 2006), p 6.

140 Ibid., p. 8.

141 Ibid., pp. 39 and 46.

142 Formerly the Ministry of the Solicitor General.

143 LeSage, p. 83.

144 Ontario, Special Investigations Unit, Annual Report 2002–2003 (Toronto: Special Investigations Unit, 2003), p. 1, online, SIU, http://www.siu.on.ca/siu_images/SIU%202003ReportENG.pdf (accessed July 12, 2006).

145 *Police Services Act*, s. 113. See also Adams report 1998 (see note 127).

146 *Police Services Act*, s. 113(3).

147 *An Act to revise the Police Act and amend the law relating to Police Services*, s. 113.

148 Adams report 1998.

149 Adams review report 2003, p. 9 (see note 127).

150 The transfer of responsibility from the Solicitor General to the Attorney General occurred in September 1992 following a report by Stephen Lewis on police and race relations in Toronto. See Adams report 1998, p. 10.

151 Ontario, Special Investigations Unit, Annual Report 2004–2005 (Toronto: Special Investigations Unit, 2005), p. 17, online, SIU, http://www.siu.on.ca/siu_images/SIU%20Eng%20Final%20Web.pdf.

152 *An act respecting police organization and amending the Police Act and various legislation*, S.Q. 1988, c. 75.

153 *Police Act* [Quebec], S.Q. 2000, c. 12.

154 Ibid., s. 171.

155 Quebec, Commissaire à la déontologie policière, *Rapport Annuel 2000–2001*, (Quebec: Publications du Québec, 2001), p. 12.

156 *Police Act* [Quebec], ss. 174, 189. See also Ceyssens, p.7-67 (see note 35).

157 *Police Act* [Quebec], s. 148.

158 Ibid., s. 147. See also Ceyssens, p. 7-59.

159 *Police Act* [Quebec], ss. 162–163.

160 Canadian Association for Civilian Oversight of Law Enforcement (CACOLE), *Compendium of Civilian Oversight Agencies in Canada*, Hyacinthe Miller, ed., (CACOLE, 2006). p. 36, online, http://www.cacole.ca/Resource%20Library/Compendium/CACOLE%20Compendium%202006.pdf (accessed Nov. 1, 2006) [CACOLE Compendium].

161 O.C. 920–90, 27 June 1990, Gazette Officielle du Québec 1990, Part 2, vol. 122, No. 28, p. 1760, s. 12.

162 Paul Monty, then Police Ethics Commissioner for Quebec, speaking notes (January 2004), pp. 2–3 (unpublished, on file with author).

163 CACOLE Compendium, p. 32.

164 *Police Act* [Quebec], s. 234.

165 Ibid., ss. 129, 198; Ceyssens, p. 7-15.

166 *Police Act* [Quebec], ss. 130, 199; Ceyssens, p. 7-17.

167 *An act respecting police organization and amending the Police Act and various legislation*, S.Q. 1988, c. 75, s. 101.

168 *An act to amend the act respecting police organization and the Police Act as regards police ethics*, S.Q. 1997, c. 52, s. 36.

169 *Police Act* [Quebec], s. 145; see also Ceyssens, p. 7-48.

170 *Police Act* [Quebec], s. 143.

171 Ibid., s. 166; Ceyssens, p. 7-23, note 7.

172 *Police Act* [Quebec], s. 260.

173 See note 161. S. 12.

174 Conversation with Paul Monty, then Police Ethics Commissioner for Quebec, June 7, 2004.

175 *Police Act* [Quebec], s. 143; Ceyssens, p. 7-28.

176 *Code of ethics of Québec police officers* (see note 161), ss. 5(2), 6(1), 8(2), 11(1).

177 *Domestic Models of Review of Police Forces* (see note 1).

178 Email correspondence to Commission from Cyndy Dyck, Office of the Police Complaint Commissioner of British Columbia, August 12, 2004 [Dyck correspondence]; see also Office of the Police Complaint Commissioner, British Columbia, 1998 Annual Report, online, www.opcc.bc.ca (accessed Oct. 24, 2006).

179 Commission of Inquiry into Policing in British Columbia, *Closing the Gap: Policing and the Community* (Vancouver, B.C.: Commission of Inquiry into Policing in British Columbia, 1994) (Commissioner: Hon. Justice Wallace T. Oppal), online, http://www.pssg.gov.bc.ca/publications/oppal/ClosingTheGap.pdf (accessed August 12, 2004).

180 Ibid., p. 19.

181 CACOLE Compendium, p. 5 (see note 160).

182 Ibid., p. 6.

183 *Police Act* [B.C.], R.S.B.C. 1996, c. 367 (as am.), ss. 47(1), 47(2).

184 Philip C. Stenning, *Review of Part 9 (Complaint Procedure) of the British Columbia Police Act, as Amended by Section 36 of S.B.C. 1997, c. 37* (August 11, 1998) [unpublished, archived at the Office of the British Columbia Police Complaint Commissioner], p. 19.

185 *Police Act* [B.C.], s. 56.

186 Ibid., s. 56.1(1). See also Dyck correspondence (see note 178).

187 Ibid., s. 59.1(2)(a).

188 Ibid., ss. 60, 60.1(2)(a).

189 Ibid., s. 60(4).

190 CACOLE Compendium, p. 7.

191 *Police Act* [B.C.], s. 62(1).

192 [1959] S.C.R. 121.

193 *Proulx v. Quebec*, [2001] 3 S.C.R. 9.

194 *Odhavji Estate v. Woodhouse*, [2003] 3 S.C.R. 263.

195 McDonald Commission report, vol. 2, p. 1041.

196 *R. v. Barnes* [1991] 1 S.C.R. 449.

197 *R. v. Mack* [1988] 2 S.C.R. 903.

198 Unless otherwise indicated, information in this section is based on meetings and communications between Policy Review legal counsel and SIRC.

199 *CSIS Act*, s. 34(1).

200 In practice, some SIRC members have been named privy councillors in order to assume office.

201 Some members of SIRC have been without past political affiliation. It has not been possible for SIRC to continue to mirror Parliament following major electoral changes in party representation, such as after the 1993 general election. There has never been an appointment of a member with past affiliation with the *Bloc Québécois* (although the leader of that party in the

House has consulted over the appointment of members from the province of Quebec). Moreover, it took six years following the appearance of the Reform Party / Canadian Alliance as an official party in the House for it to gain a representative on SIRC. There has always been one member with past affiliations to the New Democratic Party.

202 *CSIS Act*, ss. 34(2)–34(3).

203 Ibid., s. 37.

204 Ibid., s. 38.

205 Ibid., s. 38(a).

206 Ibid., s. 40.

207 Ibid.,

208 Ibid., s. 54.

209 Ibid., s. 41(1)(a).

210 Ibid., s. 42(3).

211 Ibid., s. 38(c). Prior to amendment of the *CSIS Act* in 2001, SIRC also conducted investigations and hearings with respect to ss. 39 and 81 of the *Immigration Act*, regarding recommendations of deportation where it is alleged that a person is either a security threat or, following conviction for a serious criminal offence, that the person is involved in organized crime.

212 "Meeting Between the Security Intelligence Review Committee and the Arar Inquiry Policy Review – Discussion Points," June 21, 2004 [Discussion Points], and meeting of June 22, 2004 (Arar Commission Policy Review).

213 Ibid.,

214 *Reviews* (updated January 13, 2004), online, Security Intelligence Review Committee, http://www.sirc-csars.gc.ca/reviews_e.html (accessed Aug. 23, 2006).

215 Canada, Security Intelligence Review Committee, SIRC Annual Report 2004-2005 (Ottawa: Public Works and Government Services Canada, 2005), p. 12 [SIRC Annual Report 2004–2005]. SIRC's annual reports are available online at http://www.sirc-csars.gc.ca/reports_e.html (accessed February 21, 2006).

216 This investigation took place in 2003–2004. It is detailed in Canada, Security Intelligence Review Committee, SIRC Annual Report 2003–2004 (Ottawa: Public Works and Government Services Canada, 2004), pp. 13-14 [SIRC Annual Report 2003-2004].

217 SIRC Annual Report 2004–2005, pp. 4–36.

218 For an overview of the Target Approval Review Committee, see Jack Hooper testimony, Arar Commission Factual Inquiry Public Hearing (June 22, 2004), pp. 458–474.

219 Canada, Security Intelligence Review Committee, SIRC Annual Report 1999–2000 (Ottawa:Minister of Supply and Services Canada, 2000), p. 13 [SIRC Annual Report 1999-2000].

220 Canada, Security Intelligence Review Committee, SIRC Annual Report 2002–2003 (Ottawa: Public Works and Government Services Canada, 2003), pp. 15–16 [SIRC Annual Report 2002–2003].

221 Canada, Security Intelligence Review Committee, SIRC Annual Report 2001–2002 (Ottawa: Public Works and Government Services Canada, 2002), p. 11 [SIRC Annual Report 2001–2002].

222 Canada, Security Intelligence Review Committee, SIRC Annual Report 1998–1999 (Ottawa: Minister of Supply and Services Canada, 1999), p. 34 [SIRC Annual Report 1998–1999].

223 SIRC Annual Report 2002–2003, p. 17.

224 Canada, Security Intelligence Review Committee, Annual Report 1997–1998 (Ottawa: Minister of Supply and Services Canada, 1998) [SIRC Annual Report 1997–1998], p. 53.

225 SIRC Annual Report 2001-2002, p.15.

226 Canada, Security Intelligence Review Committee, SIRC Annual Report 2000–2001 (Ottawa: Public Works and Government Services Canada, 2001), p. 27.

227 Ibid., p. 28.

228 SIRC Annual Report 2002–2003, p. 23.
229 SIRC Annual Report 2001–2002, p. 16.
230 SIRC Annual Report 1997–1998, p. 22.
231 SIRC Annual Report 2004–2005, p. 32.
232 SIRC Annual Report 2001–2002, p. 48.
233 Ibid., p. 21.
234 SIRC Annual Report 1998–1999, p. 39.
235 *CSIS Act*, s. 38(c).
236 Ibid., s. 41.
237 Canada, *Rules of Procedure of the Security Intelligence Review Committee in Relation to its Function Under Paragraph 38(c) of the* Canadian Security Intelligence Service Act, March 1985, s. 46(2), online, Security Intelligence Review Committee, http://www.sirc-csars.gc.ca/complaints_rules_e.html (accessed July 14, 2006) [SIRC Rules of Procedure].
238 *CSIS Act,* s. 46.
239 *Canadian Human Rights Act,* R.S.C. 1985, c. H-6, s. 45(6).
240 *CSIS Act,* s. 50.
241 Ibid., s. 48(2).
242 SIRC Rules of Procedure, s. 46(2).
243 Ibid., ss. 48(2)–48(3).
244 Murray Rankin, "The Security Intelligence Review Committee: Reconciling National Security with Procedural Fairness", 3 C.J.A.L.P. 173, p. 184.
245 SIRC Rules of Procedure*,* ss. 48(4)–48(5).
246 *Canada (Minister of Employment and Immigration) v. Chiarelli*, [1992] 1 S.C.R. 711. The case involved the review of the deportation of a permanent resident based on alleged links with organized crime. Although national security information was not involved, the court's reasoning is applicable here.
247 *CSIS Act*, s. 39. There are actually two exceptions to complete access. SIRC, like the IG, is excluded from receiving Cabinet confidences, including Cabinet communications to CSIS. Moreover, in 1988, SIRC entered into a "Third Party-Access Protocol" with CSIS that potentially limits SIRC access to CSIS documents containing information provided by third parties (foreign governments and organizations) if the latter withhold consent, although CSIS "will use its best efforts to obtain authority to disclose information provided by third parties when requested to do so by SIRC": Memorandum from Chairman of SIRC to Director of CSIS, May 25, 1988, with Annex of same date. In the mid-1990s, SIRC publicly complained when a CSIS document it had sought was instead returned to its donor agency: Security Intelligence Review Committee, *Annual Report 1995–96* (Ottawa: Minister of Supply and Services Canada, 1995), p. 5.
248 "O'Connor Commission – Questions and Answers" (SIRC responses to questions by the Arar Commission Policy Review), August 15, 2005.
249 *CSIS Act*, s. 53.
250 Ibid., s. 54.
251 *Thomson v. Canada (Deputy Minister of Agriculture)*, [1992] 1 S.C.R. 385.
252 *CSIS Act*, s. 52(2).
253 Unless otherwise noted, information in this section is based on meetings and communications between Policy Review legal counsel and the Inspector General of CSIS.
254 *CSIS Act*, s. 30.
255 *Keeping Canadians Safe*, "Inspector General of the Canadian Security Intelligence Service" (webpage), online, Public Safety and Emergency Preparedness Canada, www.psepc-sppcc.gc.ca/abt/wwa/igcsis/igcsis-en.asp (accessed Aug. 23, 2006).

256 *Report of the Auditor General of Canada to the House of Commons*, Nov. 1996 (Ottawa: Minister of Supply and Services Canada, 1996), ch. 27, "The Canadian Intelligence Community – Control and Accountability," s. 27-93, online, Office of the Auditor General of Canada, http://www.oag-bvg.gc.ca/domino/reports.nsf/html/9627ce.html (accessed Aug. 23, 2006) [1996 Report of the Auditor General of Canada].

257 *Keeping Canadians Safe*, "Inspector General of the Canadian Security Intelligence Service" (webpage). See also *CSIS Act*, ss. 30, 33, 40.

258 In interviews, the IG termed this the "validation process." It is a detailed review of the CSIS Director's annual report, including a detailed validation of the facts behind, quite literally, every statement. The aim is to complete this validation process by the end of the calendar year in which the Director's report to the Minister is issued, although, on certain occasions, this certificate has come years late.

259 See *Keeping Canadians Safe*, "A Strategic Perspective for the Inspector General of CSIS", online, Public Safety and Emergency Preparedness Canada, http://www.psepc-sppcc.gc.ca/abt/wwa/igcsis/stratper-en.asp (accessed July 24, 2006) ["A Strategic Perspective"].

260 *CSIS Act*, s. 33(3).

261 *Keeping Canadians Safe*, "Inspector General of the Canadian Security Intelligence Service" (webpage).

262 See "A Strategic Perspective" (see note 259).

263 For example, the Minister once requested that the IG look into and report on the matter of an employee at CSIS who had lost some classified documents. Specific requests of this kind from the Minister appear to be rare occurrences. There is no express statutory provision for requests from the Minister, but the view held by the IG is that the power is implied, given the spirit and theory behind the IG's office.

264 *Keeping Canadians Safe*, Certificate of the Inspector General CSIS – 2001, 2002, 2003, online, Public Safety and Emergency Preparedness Canada, http://www.psepc-sppcc.gc.ca/abt/wwa/igcsis/cert2001-en.asp, http://www.psepc-sppcc.gc.ca/abt/wwa/igcsis/cert2002-en.asp, http://www.psepc-sppcc.gc.ca/abt/wwa/igcsis/cert2003-en.asp (accessed Aug. 24, 2006).

265 *CSIS Act*, s. 12. The IG considers whether key legal and policy standards related to targeting were followed. This includes a review of whether "reasonable grounds" existed to justify the targeting and techniques used, whether the specific activities of the proposed target constituted "threats to the security of Canada," whether the investigation was focused to the extent "strictly necessary" and the scope and intrusiveness of the investigation were proportionate to the seriousness of the threat and, where the proposed targeting and investigation involved activities related to lawful advocacy, protest or dissent, or sensitive institutions and values, whether those interests were appropriately considered and protected.

266 *CSIS Act*, s. 31(2).

267 P.C. 1996–899, June 19, 1996.

268 *National Defence Act*, R.S.C. 1985, c. N-5 (as amended).

269 Ibid., s. 273.63(1).

270 Ibid., ss. 273.63(4), 273.63(5).

271 Ibid., s. 273.63(2).

272 Ibid., s. 273.63(3).

273 Canada, Communications Security Establishment Commissioner, *Annual Report 2005–2006* (Ottawa: Public Works and Government Services Canada Canada, 2006), p. 14, online, Office of the Communications Security Establishment Commissioner, http://csec-ccst.gc.ca/ann-rpt/2005-2006/ann-rpt_e.pdf (accessed Aug. 11, 2006) [CSE Commissioner Annual Report 2005–2006].

274 "Review Function," online, Office of the Communications Security Establishment Commissioner, http://www.csec-ccst.gc.ca/functions/review_e.php (accessed Aug. 11, 2006).

275 *National Defence Act,* s. 273.65.

276 Ibid., ss. 273.65(4)(e), 273.65(8).

277 Canada, Communications Security Establishment Commissioner, *Annual Report 2003–2004* (Ottawa: Public Works and Government Services Canada Canada, 2004), p. 9 [CSE Commissioner Annual Report 2003–2004].

278 CSE Commissioner Annual Report 2005–2006, p. 9.

279 Ibid., p. 11.

280 Ibid., p. 16.

281 The CSE Commissioner takes the position that nothing in Part V.1 of the *National Defence Act* or in the *Inquiries Act* precludes the Commissioner from accessing information holdings protected by Cabinet privilege.

282 CSE Commissioner Annual Report 2005–2006, p. 9.

283 "Complaints Procedure," online, Office of the Communications Security Establishment Commissioner, http://www.csec-ccst.gc.ca/functions/complaints-proced_e.php (accessed Aug. 23, 2006).

284 CSE Commissioner Annual Report 2005–2006, p. 13.

285 *Privacy Act*, R.S.C. 1985, c. P-21, s. 2.

286 Ibid., s. 12.

287 Office of the Privacy Commissioner of Canada, *Privacy: Annual Report to Parliament 2005–2006* (Ottawa: Public Works and Government Services Canada Canada, 2006), p. 9, online, OPCC, http://www.privcom.gc.ca/information/ar/200506/200506_pa_e.pdf (accessed July 5, 2006) [Privacy Commissioner's Annual Report 2005–2006].

288 *Privacy Act*, ss. 19, 21, 22, 23.

289 Ibid., s. 34.

290 Ibid., s. 34(2).

291 *Exempt Personal Information Bank Order No. 13 (RCMP)*, S.O.R./90-149.

292 *Exempt Personal Information Bank Order No. 14 (CSIS)*, S.O.R./92-688.

293 *Exempt Personal Information Bank Order No. 25 (RCMP)*, S.O.R./93-272.

294 *Privacy Act*, s. 36. As provided for in s. 70(1) of the Act, the Privacy Commissioner does not have access to Cabinet confidences.

295 *Privacy Act*, s. 36.

296 Privacy Commissioner's Annual Report 2005–2006, p. 59.

297 *Audit of the Personal Information Management Practices of the Canada Border Services Agency – Trans-Border Data Flows*, Final Report (June 2006), online, Office of the Privacy Commissioner of Canada, http://www.privcom.gc.ca/information/pub/ar-vr/cbsa_060620_e.asp (accessed August 15, 2006).

298 S. 59(2) of the *Privacy Act* specifically limits investigation of national security, defence and international affairs to specially designated officers and employees, in recognition of secrecy issues.

299 *Privacy Act*, s. 40.

300 *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403.

301 *Access to Information Act*, s. 36.

302 Ibid., s. 69.1.

303 Ibid., ss. 62, 64.

304 Ibid., s. 59(2).

305 Information Commissioner of Canada, *Annual Report, Information Commissioner, 2005–2006* (Ottawa: Public Works and Government Services Canada Canada, 2006), p. 27, online, http://www.infocom.gc.ca/reports/pdf/oic05_06E.PDF (accessed Aug. 23, 2006).

306 *Access to Information Act*, s. 37(1).

307 Ibid., ss. 38–40.

308 Donald J. Savoie, *Breaking the Bargain: Public Servants, Ministers, and Parliament* (Toronto: University of Toronto Press, 2003), pp. 49–52.

309 The Information Commissioner made submissions on changes effected by the *Anti-terrorism Act* in Office of the Information Commissioner of Canada, "Remarks to Senate Special Committee on Anti-Terrorism (Review of the Anti-Terrorism Act)," Ottawa, May 30, 2005, online, OICC, http://www.infocom.gc.ca/speeches/speechview-e.asp?intspeechId=112 (accessed July 12, 2006).

310 Reg Whitaker, "Access to Information and Research on Security and Intelligence: The Canadian Situation" in Peter Hanks and John D. McCamus, eds., *National Security: Surveillance and Accountability in a Democratic Society* (Cowansville, Quebec: Éditions Yvon Blais, 1989), pp. 183–196.

311 The Act protects anyone living in Canada against discrimination by any of the following federally regulated employers or service providers: federal departments, agencies and Crown corporations, including chartered banks, airlines, television and radio stations, interprovincial communications and telephone companies, buses and railways that travel between provinces, First Nations, and other federally regulated industries, such as certain mining operations. The Canadian Human Rights Commission provides a list on its website of private sector employers under federal jurisdiction. Source: http://www.chrc-ccdp.ca/discrimination/federally_regulated-en.asp?pm=1 (accessed Aug. 23, 2006).

312 *Canadian Human Rights Act*, s. 45.

313 Ibid., s. 38(c).

314 Ibid., s. 45(4).

315 Ibid., s. 46(1).

316 Ibid., s. 46(2).

317 Opening Statement of Mary Gusella, Chief Commissioner, Canadian Human Rights Commission, to the Subcommittee on Public Safety and National Security of the Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness, House of Commons, 38th Parl., 1st Sess., June 15, 2005, online, Parliament of Canada, http://www.parl.gc.ca/infocomdoc/38/1/snsn/meetings/evidence/snsnev17-e.htm#lnt-1350869 (accessed July 21, 2006). [Opening Statement of CHRC Chief Commissioner to House Subcommittee on Public Safety and National Security].

318 *Canadian Human Rights Act*, s. 64.

319 Opening Statement of CHRC Chief Commissioner to House Subcommittee on Public Safety and National Security.

320 *Canadian Human Rights Act*, s. 43.

321 Ibid., s. 44.

322 Ibid., s. 33(2).

323 Ibid., s. 52.

324 Ibid., s. 58.

325 "What Do We Audit?" online, Office of the Auditor General of Canada, http://www.oag-bvg.gc.ca/domino/other.nsf/html/auqdn_waqv_e.html (accessed July 21, 2006) ["What Do We Audit?"].

326 1996 Report of the Auditor General of Canada, ch. 27 (see note 256).

327 Ibid., para. 27.36.

328 Now the Canada Border Services Agency and Canada Revenue Agency.

329 *Report of the Auditor General of Canada to the House of Commons*, Nov. 2003 (Ottawa: Public Works and Government Services Canada Canada, 2003), paras. 10.120–10.162, online, OAGC, http://www.oag-bvg.gc.ca/domino/reports.nsf/html/20031110ce.html (accessed July 24, 2006).

330 "A Message From the Auditor General of Canada" in *Report of the Auditor General of Canada to the House of Commons*, Mar. 2004 (Ottawa: Public Works and Government Services Canada Canada, 2004), online, OAGC, http://www.oag-bvg.gc.ca/domino/reports.nsf/html/20040300ce.html/$file/20040300ce.pdf (accessed July 24, 2006).

331 *Report of the Auditor General of Canada to the House of Commons*, Mar. 2004 (Ottawa: Public Works and Government Services Canada Canada, 2004), ch. 3, s. 3.22, online, OAG, http://www.oag-bvg.gc.ca/domino/reports.nsf/html/20040303ce.html/$file/20040303ce.pdf (accessed July 24, 2006).

332 C4ISR is the military acronym for command, control, communications, computers (C4), intelligence, surveillance and reconnaissance (ISR).

333 "A Message From the Auditor General of Canada" in *Report of the Auditor General of Canada to the House of Commons*, Apr. 2005 (Ottawa: Public Works and Government Services Canada Canada, 2005), online, OAG, http://www.oag-bvg.gc.ca/domino/reports.nsf/html/20050400ce.html/$file/20050400ce.pdf (accessed July 24, 2006).

334 *Report of the Auditor General of Canada to the House of Commons*, Nov. 2005 (Ottawa: Public Works and Government Services Canada Canada, 2005), paras. 28–29, online, OAG, http://www.oag-bvg.gc.ca/domino/reports.nsf/html/20051100ce.html/$file/20051100ce.pdf (accessed July 24, 2006). The Auditor General notes that "[i]t is our understanding that the government has continued to work on a mechanism that would increase the role of Parliament in security and intelligence matters. The details have yet to be presented to Parliament. I encourage the government to do so."

335 *Auditor General Act*, R.S.C. 1985, c. A-17, s. 7.

336 Ibid., s. 8.

337 Ibid., s. 11.

338 "What is Legislative Auditing," online, Office of the Auditor General of Canada, http://www.oag-bvg.gc.ca/domino/other.nsf/html/auqdn_lavg_e.html (accessed Aug. 23, 2006) ["What is Legislative Auditing?"].

339 Ibid.,

340 The Auditor General receives many audit requests from individual citizens, groups, members of Parliament, senators, and others. The requests are all carefully reviewed and given consideration in the selection process: "What Do We Audit?."

341 "What is Legislative Auditing?"

342 *Auditor General Act*, s. 13(4).

343 "What is Legislative Auditing?"

344 Ibid.

345 The reports of the Commissioner of the Environment and Sustainable Development are referred to the Committee on Environment and Sustainable Development.

346 "What is Legislative Auditing?"

VII

Review of National Security Activities: The International Experience

1. INTRODUCTION

The Policy Review mandate requires me to base my recommendations in part on an examination of review models used by other countries. In this chapter I set out my observations about these models.

I begin with an overview of the foreign review models that I selected for examination.[1] My research with respect to the eight countries leads me to a number of general observations.[2] I discuss below issues relating to the structure of review mechanisms; common challenges in the review of national security policing; and features essential for review of national security policing.

I then turn to a detailed examination of each of the eight countries. I discuss the principal review models in each country, where necessary setting out the constitutional and governmental context. I then describe the law enforcement and security intelligence structures, and the principal review and oversight structures.

Appendix C of this Report contains a list of the foreign agencies, as well as other persons with whom my counsel consulted by either teleconference, meetings in person or written correspondence. Their generous assistance is very much appreciated. Appendix D contains a list of the persons who participated in the Roundtable of International Experts on Review and Oversight, who also kindly contributed their time to assist in my consideration of the many questions raised by the Policy Review.

For convenience, a list of the many acronyms used in this chapter is included at the end of the chapter.

1.1 OVERVIEW

1.1.1 Structure of Review Mechanisms

There are significant differences in the way that review and oversight of national security activities is organized in different countries. The structure of review mechanisms is closely related to a country's history, constitutional structure and existing government institutions, and to the organization of its police and security agencies. Within these different structures, however, review agencies confront many similar challenges.

Germany has no independent body that reviews complaints against the police. In the other seven countries that I examined, police forces involved in national security activities are subject to review by something more than a purely complaint-based body. Five of these eight countries have some form of review body with jurisdiction over both policing and intelligence activities; Belgium, Germany and New Zealand do not.

Some review bodies have jurisdiction over police forces with both intelligence-gathering and traditional policing responsibilities, while others have general jurisdiction over all public authorities. Some review bodies, like the Norwegian EOS Committee or the U.K.'s covert investigation review authorities, have functionally defined jurisdiction that encompasses the activities of both police and intelligence agencies. In Australia and the U.K., jurisdiction over the national security activities of the police is shared between two different review bodies. In the United States, oversight is conducted by inspectors general for specific departments and agencies rather than by police or intelligence function.

In summary:

- Police forces in **England and Wales**, which all carry out national security policing to varying degrees, are subject to the complaint-processing jurisdiction of the Independent Police Complaints Commission (IPCC) and the Investigatory Powers Tribunal. For certain covert activities, they are also subject to the review-based jurisdiction of the Interception of Communications Commissioner (ICC) and the Office of Surveillance Commissioners (OSC). The police are subject to these reviews of certain covert activities, no matter what type of investigation they are carrying out, for example, national security or conventional law enforcement. Indeed because the jurisdiction of the ICC and the OSC is function-based — defined by the covert activity in issue — a large number of public authorities fall

within their jurisdiction. Police forces in the U.K. are also subject to substantial "effectiveness and efficiency" scrutiny by Her Majesty's Inspectorate of Constabulary. The IPCC handles complaints against the Serious Organised Crime Agency, which, among other functions, has an important role combating money-laundering and terrorist financing in its capacity as the United Kingdom's financial intelligence unit. Many of the police-like powers of Customs and Immigration authorities in England and Wales are, or will soon be, reviewed by the IPCC.

- Police forces in **Northern Ireland** are subject to similar regimes, including reviews of certain defined covert activities. The applicable complaint-based bodies are the Police Ombudsman for Northern Ireland, rather than the IPCC, and the Investigatory Powers Tribunal that also has jurisdiction in England and Wales.
- National security policing in **Australia** is conducted by the Australian Federal Police, who are under the complaint-processing jurisdiction of the Commonwealth Ombudsman, as well as the review-based jurisdiction of the Ombudsman with respect to covert investigative activities in certain circumstances. The Commonwealth Ombudsman has jurisdiction over approximately 150 other public authorities, including most of Australia's intelligence agencies, and the new, integrated Australian Crime Commission (ACC). Integration among domestic agencies, including across federal and state/territory jurisdictions, is an emerging issue in Australia. The Ombudsman is increasingly working in co-operation with other accountability bodies, including the review authority for the security intelligence services. Indeed there have been formal recommendations for co-operation among review bodies, and a statutory provision for "arrangements" between review bodies was created to avoid accountability gaps with respect to review of the ACC.
- National security policing in **Belgium** is conducted by divisions of the regular police, which fall under the complaint-processing and review jurisdiction of an independent standing committee answerable to Parliament called Committee P. Committee P also has jurisdiction over other public authorities with police powers, such as customs authorities. Committee P has a statutory obligation to share information and collaborate with Committee I, a similarly constituted body that reviews Belgium's intelligence agencies.
- There is no independent review body for the police forces in **Germany**, nor any agency similar in structure to Canada's SIRC to review its intelligence agencies. A specialized parliamentary committee, the Parliamentary Control Panel, reviews activities conducted by the German intelligence services,

such as the reception and analysis of air passenger information and financial transaction information. A separate body, the G-10 Commission, reviews interceptions of private communications.

- National security policing in **Norway** is conducted largely by a division of the regular police called the Police Security Service, which has a separate statutory mandate. The Police Security Service is under the complaint-processing and review jurisdiction of the EOS Committee, which also reviews Norway's two security intelligence agencies. Since the jurisdiction of the EOS Committee is functionally defined, questions have arisen in Norway as to whether there are sections of the ordinary police, and of other authorities such as immigration, that fall under this functional definition.
- The **New Zealand** Police conduct national security policing and are subject to the complaint-based jurisdiction of the Police Complaints Authority. The Police Complaints Authority also has jurisdiction to investigate, on its own motion, incidents where a member of the Police appears to have caused death or serious bodily harm. The security intelligence services are reviewed by a separate body.
- National security policing in **Sweden** is largely conducted by a division of the police called the Security Service, or *Säpo*, which operates under direction from government ordinances and which has separate offices and structures. The ordinary police also carry out national security policing. Both fall under the jurisdiction of the Parliamentary Ombudsmen's office, as do the intelligence services, the immigration and customs authorities, and the administration of foreign affairs. The Ombudsmen's office has a complaint-processing and review mandate over these agencies. However, its role as "secondary supervisor" and its small size preclude close and regular scrutiny of any of these agencies.
- National security policing within the **United States** is conducted principally by the FBI, which is subject to the complaint-processing, audit, review and investigation jurisdiction of the Inspector General of the Department of Justice. An Inspector General reviews the Department of Homeland Security, which also engages in law enforcement and intelligence activities related to national security and which includes U.S. Customs and Border Patrol, U.S. Citizenship and Immigration Services, and the Transportation Security Authority. In addition, the CIA, the Department of Defense, which includes a number of constituent intelligence agencies, and the State Department, including the Bureau of Research and Intelligence, all have inspectors general.

The different ways that countries organize their police and security services make strict comparisons of structure difficult. Overall, the jurisdiction of foreign review bodies over law enforcement or intelligence matters is somewhat fluid and may overlap with the jurisdiction of other accountability bodies. Nevertheless, while the institutional structures that different countries choose to review domestically focused national security agencies are quite different, the tools that are given to these review bodies and the challenges they face are relatively similar.

1.1.2 Common Challenges

Foreign review agencies are grappling with many common challenges in providing for the accountability of law enforcement and security intelligence agencies. These include the following:

- Increased integration and information sharing among domestic and foreign national security actors.
- An increased blurring of the distinction between security intelligence and criminal intelligence.
- An overlap in counter-terrorism investigation between ordinary police units and national security police units (e.g., proceeds of crime investigations occurring in both contexts), such that national security policing is difficult to define.
- The burden on resources that complaint-processing can cause in a policing context. To help ease this burden, several agencies have the power to refer investigations of complaints back to the police or to other agencies. In England and Wales the IPCC also has the power to actively supervise the investigation of a complaint by the police.
- Issues regarding the coordination of review and criminal prosecutions. In several countries review bodies have had experience with investigations that overlap with criminal investigations or proceedings. In general, review bodies proceed carefully with their investigations in these circumstances and consult with prosecuting authorities. Review bodies may defer releasing their reports until criminal proceedings have been concluded.

The way that different countries are dealing with the integration of the activities of different government actors in the national security field holds valuable lessons for Canada. Many of the review bodies that we surveyed consider the review of the integrated national security activities of different government

actors to be a pressing challenge for their agencies. Most noted the advantages of an accountability system that allows for monitoring integrated activity.

The majority of review bodies that we surveyed have developed some means of addressing issues of integration in the national security field, either by creating an accountability body with jurisdiction over multiple government agencies or by establishing robust mechanisms for information exchange and co-operation between accountability bodies. Only in New Zealand and Germany do agency-based review bodies have little power either to share information or conduct joint reviews with accountability agencies for other organizations. However, the New Zealand Police Complaints Authority does consult on a general level with other accountability bodies to avoid duplication around complaints.

In Australia, the Commonwealth Ombudsman, who has general jurisdiction over public authorities, including the police and security intelligence services, has the statutory power to enter into arrangements with other accountability bodies to coordinate review. The Parliamentary Ombudsman also conducts informal joint reviews with other accountability bodies, although information sharing is somewhat limited. Further, the Inspector General of Intelligence and Security, who reviews only the security and intelligence agencies, is obliged by statute to consult with the Ombudsman before beginning an inquiry. The increasing level of federal-state integration in national security operations has also prompted a parliamentary committee to call for greater co-operation between state ombudsmen, the Commonwealth Ombudsman and the Inspector General of Intelligence and Security. As a result, the Inspector General and the Commonwealth Ombudsman have just signed a protocol governing joint investigations.

In Belgium, the body that reviews police activity (Committee P) and the body that reviews intelligence activity (Committee I) are required by statute to exchange information and co-operate in investigations. In addition, the reports of the two committees are submitted to the same standing parliamentary commissions. With the chair of the Privacy-Protection Commission, the chairs of Committee P and Committee I sit on a joint committee that hears reviews of security clearance decisions. Committee P also co-operates on a formal basis with the Centre for Equal Opportunities and Opposition to Racism. Committee P has jurisdiction over both federal and local police officers, which facilitates review since Belgium is a federal state.

Issues surrounding the integration of national security activities have also arisen in Norway. The EOS Committee, Norway's review body for public security and intelligence activity, currently faces questions as to whether its

functionally defined review mandate extends beyond the security intelligence agencies to cover the national security activities of the ordinary police force, the immigration authorities and the customs service. The EOS Committee already has the power to investigate in areas that fall outside its functionally defined mandate to clarify issues related to investigations that fall within its mandate. The Committee has had problems, however, following the course of a police investigation involving both the regular police force and the Police Security Service, including information-sharing activity. The EOS Committee and the Police Complaints body also communicate in certain circumstances regarding issues that touch on the jurisdiction of both bodies.

In Sweden, responsibility for review of public authorities, including the Swedish Security Service, the regular police force, the military-operated intelligence agencies, the customs and immigration authorities, and foreign affairs, is divided among the four Parliamentary Ombudsmen. The Ombudsmen meet regularly to share information, and are considering conducting more formalized, joint reviews of public authorities whose work is interrelated or integrated.

The IPCC in England and Wales has the power to exchange information with other accountability bodies. The Commission has conducted joint investigations with other review agencies and, recently, a formal statutory gateway was created to allow for information-sharing and joint investigations with the Parliamentary Ombudsman to facilitate investigations of certain complaints against Her Majesty's Revenue and Customs Department. A similar statutory gateway has been proposed for complaints in the context of immigration enforcement activities, over which the Independent Police Complaints Commission will soon receive jurisdiction. Through its jurisdiction over the Serious Organised Crime Agency, the IPCC also has jurisdiction over the former Customs and Immigration investigation branches and over financial intelligence activities. Similarly, the Police Ombudsman for Northern Ireland has jurisdiction over certain aspects of Customs activity and expects to receive jurisdiction over most immigration enforcement activity in the near future.

The security intelligence community in the United States is the largest and most complex of any of the countries that I studied. Perhaps as a result, it is in the U.S. that co-operation amongst oversight bodies is most highly developed. By law, inspectors general have access to information held by other federal government departments or agencies. Inspectors general often share information and jointly investigate matters that touch on two or more areas of responsibility, either on their own initiative or at the request of Congress. An Intelligence Community Inspectors General Forum has also been established to bridge areas of responsibility, as well as to identify matters requiring joint investigation and

common themes in review and oversight activity. The inspectors general for the Department of Homeland Security and the Department of Justice have also concluded agreements with other accountability bodies, like the Civil Liberties Protection officials in the Department of Homeland Security and the Office of the Director of National Intelligence regarding the division of responsibility in areas of shared jurisdiction. The U.S. inspectors general also stressed the need for a form of comprehensive observation of all national security activities. In the United States, this role is currently played by congressional committees.

Overall, the international review agencies that I surveyed consider the ability to share information, co-operate with other accountability bodies, and access information about a range of government departments and agencies to be important tools to ensure that increasingly integrated national security activities can be monitored efficiently and effectively. In Australia and Belgium, information sharing and coordination among review agencies also helps to overcome problems of jurisdiction that arise in the context of a federal state, a solution that is particularly relevant to Canada.

1.1.3 Essential Review Features

Across different jurisdictions, certain features are seen as essential to assuring accountability for covert activities by the state.

All of the review agencies that I surveyed are legally required to maintain the secrecy of sensitive information. The ability to maintain secrecy is viewed as vital to the ability of a review agency to gain the trust of the agencies that it reviews and of the executive branch of government. Similarly, to foster public trust and confidence, independent, publicly credible bodies or individuals must be responsible for review. In every jurisdiction, the appointment process for members of review bodies is designed to engender public confidence in both the independence and the competence of reviewers.

An important power of the review bodies that I studied is wide access to documents, premises and personnel, subject to limited exceptions. All of the review bodies surveyed have a general power to access relevant documents. Most have the power to question the personnel of the agencies over which they have jurisdiction, as well as powers of entry onto agency premises. For no review body that I surveyed may the agency being reviewed decide which documents are relevant, and, thus, determine those to which the review body has access. Access varies widely, however, in relation to documents covered by Cabinet privilege or an equivalent, information subject to third-party caveats, or information that would disclose the identity of informants or human sources.

Finally, jurisdiction to conduct both broad-scale, self-initiated reviews and process complaints was considered extremely useful by a number of review agencies. Representatives of several of the review bodies told me that a coordinated framework for complaint handling and self-initiated review provides greater opportunities for law enforcement to learn from particular incidents. In addition, several review bodies noted that by keeping track of trends in complaints and by aggregating complaints for investigation, they were able to identify systemic problems in the agencies they review.

DETAILED OBSERVATIONS[3]

2.
AUSTRALIA

2.1
OVERVIEW

As a federal country, Australia has police forces at both the state/territorial level and the federal level. The federal-level police force — the Australian Federal Police (AFP) —plays the principal role in national security law enforcement.[4] Australia also has six intelligence agencies at the federal level, and a special investigatory and criminal intelligence agency called the Australian Crime Commission (ACC). The ACC is a new integrated body of federal and state/territorial representatives from various police and other domestic agencies. It has special powers for criminal investigation and intelligence operations and extensive powers to share information with other agencies.[5]

Since 9/11, Australia has taken several counter-terrorism measures, including enhancing investigation and information-sharing powers, and creating new terrorism offences in the *Criminal Code*.[6]

Both the AFP and the ACC are reviewed by the Commonwealth Ombudsman, a primarily complaint-based mechanism with some review power over certain covert activities.[7] The Commonwealth Ombudsman also has jurisdiction over most federal bodies, including some of the intelligence agencies, but the Office's powers in respect of the Australian Intelligence Community (AIC)[8] are limited. Australia's security intelligence agencies are primarily overseen by the complaint- and review-based regime of the Inspector-General of Intelligence and Security (IGIS).

A notable feature of Australia's accountability mechanisms is their legislative provision for "arrangements" between accountability bodies to close "accountability gaps" created by integration among domestic police and security

intelligence structures, and between national and state bodies. In addition, the IGIS was recently given a statutory obligation to consult with the Ombudsman before beginning an inquiry, with a view to avoiding duplicating inquiries.[9]

2.2 LAW ENFORCEMENT AND SECURITY INTELLIGENCE

2.2.1 Australian Federal Police

As I have noted, the Australian Federal Police play the principal role in national security law enforcement in Australia. The AFP provides police services in relation to federal law[10] (including counter-terrorism laws)[11] and property, and protection of federal interests,[12] as well as "protective services" to dignitaries and protected witnesses.[13] The AFP operates in accordance with the *Australian Federal Police Act 1979* and ministerial directives issued under the Act.

The AFP's main operational units are Counter-Terrorism, Border and International Network, Economic and Special Operations, Intelligence, Protection and International Deployment Group.[14] The AFP collects intelligence, including intelligence related to counter-terrorism.[15]

The national security activities of the Australian Federal Police include domestic and international co-operation. Domestically, for example, the AFP often works co-operatively with state/territory police forces and participates in Joint Counter-Terrorism Teams with members of these forces.[16] It also operates the Transnational Crime Coordination Centre, which provides domestic and international law enforcement agencies with a point of contact for collaborating on the investigation and prevention of transnational crime, including terrorism.[17] In addition, the AFP has the Law Enforcement Cooperation Program, with liaison officers in foreign countries to facilitate information exchange.[18] Its liaison officers in London, Washington and Kuala Lumpur are dedicated to counter-terrorism.[19]

2.2.2 Australian Crime Commission

The Australian Crime Commission was created in January 2003.[20] The ACC includes members from the Australian Federal Police, state/territory police forces, the Australian Customs Service, the Australian Securities and Investments Commission, the Australian Tax Office, the Australian Security Intelligence Organisation and others.[21] The ACC collects, analyzes and disseminates criminal intelligence; and undertakes "special (intelligence) operations" and "special

investigations," using various investigative powers, where authorized by its board. It also provides reports and strategic criminal intelligence assessments to its board, and advises it on national criminal intelligence priorities.[22]

The Australian Crime Commission's board consists of the Commissioner of the AFP (who is the chair), the eight state and territory police commissioners, the Director-General of Security (i.e., the head of the Australian Security Intelligence Organisation), the Chair of the Australian Securities and Investments Commission, the CEO of the Australian Customs Service, the Secretary of the Attorney-General's Department, the Chief Police Officer of the Australian Territory and the CEO of the ACC.[23] A board determination that an intelligence operation is a "special operation" or that an investigation is a "special investigation"[24] allows an "examiner"[25] to exercise special powers. In particular, an examiner may conduct a private examination under oath of a witness concerning the operation or investigation.[26] An examiner may also require government agencies to provide information in certain cases.[27]

When the ACC obtains evidence that would be admissible in a prosecution for an offence, it must provide the evidence to law enforcement authorities.[28] In addition, the CEO may give information to domestic or foreign law enforcement agencies,[29] other Australian government departments[30] or the Australian Security Intelligence Organisation.[31]

2.2.3
Australian Security Intelligence Organisation

The Australian Security Intelligence Organisation (ASIO) gathers and analyzes intelligence to advise the federal government and other Australian "authorities" about threats to national security.[32] ASIO's functions are set out in its governing statute.[33] They include collecting, correlating, evaluating and communicating intelligence; advising ministers and Australian "authorities"; collecting foreign intelligence within Australia; and providing government agencies with security assessments used in determining security clearances and permissions to enter the country.[34] ASIO's governing statute also sets out its powers, including limitations such as a prohibition on enforcing security measures.[35] ASIO is further regulated by guidelines from its responsible minister, the Attorney-General.[36] The organization currently has approximately 980 staff, but has funding approval to expand to 1,860 by June 30, 2011.[37]

2.2.4
Australian Secret Intelligence Service

The Australian Secret Intelligence Service (ASIS) is Australia's foreign intelligence collection agency, relying on human sources to obtain information.[38] Established in 1952,[39] ASIS first received a legislative basis in 2001.[40] ASIS' functions, powers and limitations are set out in its governing statute.[41] Its activities are further limited by the *Rules to Protect the Privacy of Australians*, issued by the Minister for Foreign Affairs.[42] ASIS may perform its activities only in the interests of "national security," "foreign relations" or "national economic well-being" to the extent that those matters are affected by the "capabilities, intentions or activities of people or organisations outside Australia."[43] A recent government inquiry into Australia's intelligence agencies found that ASIS is taking on a growing role in gathering intelligence on non-state actors, representing "perhaps the most substantial transition in its history."[44] ASIS does not have law enforcement responsibilities or "police functions."[45]

2.2.5
Defence Signals Directorate

The Defence Signals Directorate (DSD) is Australia's signals intelligence agency. It is situated within the Intelligence and Security Group of the Department of Defence. Like ASIS, DSD's functions, powers and limitations were first defined by legislation in 2001.[46] DSD may collect signals intelligence only outside the domestic Australian telecommunications network,[47] and only to the extent that Australia's "national security," "foreign relations" or "national economic well-being" are "affected by the capabilities, intentions or activities of people or organisations outside Australia."[48] DSD does not have police functions or law enforcement responsibilities.[49]

2.2.6
Office of National Assessments

According to its governing statute, the Office of National Assessments (ONA) assembles "information" and produces analytical assessments on "international matters that are of political, strategic or economic significance to Australia" for provision to ministers and others in government.[50] ONA bases its assessments on information from various sources, including secret intelligence collected by other agencies.[51] It has approximately 140 staff.

2.2.7
Defence Imagery and Geospatial Organisation

The Defence Imagery and Geospatial Organisation (DIGO) acquires, produces and distributes imagery and geospatial-based intelligence in support of Australian Defence Force and government decision makers.[52] DIGO is part of the Department of Defence. It is characterized as a "single source collection and analytical agency," although it seems its role is still somewhat in flux.[53]

2.2.8
Defence Intelligence Organisation

The Defence Intelligence Organisation (DIO) conducts foreign intelligence assessments relevant to Australian security, relying on information gathered both covertly and overtly. Unlike ONA, DIO is not a separate statutory body, but operates within the Department of Defence.[54]

2.3
REVIEW AND OVERSIGHT

2.3.1
Commonwealth Ombudsman

2.3.1.1
Jurisdiction

The Australian Federal Police, the Australian Crime Commission, most of Australia's intelligence agencies, and approximately 150 other public authorities are subject to the jurisdiction of the Commonwealth Ombudsman.[55] In 2005, the Commonwealth Ombudsman was also given extended jurisdiction over immigration matters,[56] including a specific mandate to review the circumstances of people who have been in immigration detention for more than two years.[57]

The Ombudsman's office describes its review model as "generalist," with "clusters of specialties" for activities such as security intelligence, policing and immigration. It finds this model desirable principally because complaints against public authorities have much in common — individuals want public officials to discharge their functions with due respect for the rules that regulate those functions. Its broad jurisdiction allows the Office to observe and draw on such commonalities in fulfilling its mandate. It also avoids the tendency toward "capture" of a review body, which occurs when a body loses its independence by becoming too close to the decision making and operations of the agency it is

reviewing. Further, its multi-agency review jurisdiction allows the Office to observe the full scope of integrated activities.

The Ombudsman's office advised that as a specialized area, intelligence activities likely do need review by a separate body such as the Inspector-General of Intelligence and Security. Indeed, the Office ordinarily defers to the IGIS to review the intelligence agencies. It urged, however, that complaint themes for conventional and national security policing also have much in common — individuals want police officers to respect applicable laws and procedures regardless of the type of investigation. Moreover, national security policing will always be a small and closely related aspect of general policing, and separating the two may be neither possible nor desirable. The Office noted the benefits of collaboration among review bodies.

2.3.1.2
Mandate

The Commonwealth Ombudsman is charged with investigating activity for propriety on grounds set out in its governing statute. These include compliance with law, reasonableness and proper exercise of discretion.[58]

2.3.1.3
Functions

The Commonwealth Ombudsman carries out this mandate principally through complaint handling, but can also initiate its own investigations ("own motion" investigations).[59] The Office is also tasked with reviewing some covert investigative activities carried out by certain agencies, including the AFP and the ACC. Among these are telephone-intercept activities and certain covert operations carried out by law enforcement agencies in "serious offence" cases.[60]

Complaint processing

The Ombudsman receives approximately 20,000 complaints a year, of which five percent involve law enforcement authorities. The majority of complaints are referred to either the agency that has been called into question or another external review body. Pursuant to statute, the Ombudsman's office is notified of all but "minor" complaints against AFP members.[61] It refers most such complaints to the AFP for investigation, although it retains oversight of the AFP's investigations. Similarly, the Office has referred complaints about the intelligence agencies within its jurisdiction to the Inspector-General of Intelligence and Security, as discussed below.[62]

Investigating complaints against the police can often raise difficult questions about the relation of the investigation to a criminal investigation or prosecution into a related set of events. For example, a review body may come into possession of potentially exculpatory information during a criminal investigation. While there is no statutory provision covering such a situation, the Ombudsman does have the general power to make disclosures in the public interest. The Ombudsman stated that he would likely disclose exculpatory information where there might otherwise be a miscarriage of justice, but would be less likely to disclose inculpatory information. Since the Ombudsman has the power to collect information that might be self-incriminating, any risk of disclosure would make agencies and the public less likely to provide information. However, the Office has disclosed such information where there was a credible threat to life or well-being.

Similarly, the Ombudsman's office may have before it a complaint that relates to a criminal prosecution in process at the same time. In such a situation, the Office will often defer its investigation until the prosecution has been completed. This avoids an excessive burden on those involved, conflict between what is said in court and what is said to the Ombudsman, and any suggestion that the Ombudsman's office is effectively doing the work of the prosecution or the defence. In addition, the evidence in a criminal prosecution is often useful to the complaint investigation.

"Own Motion" Investigations and Review Function Over Some Activities

The Commonwealth Ombudsman may also identify matters for investigation on his own initiative.[63] The Ombudsman stated that he had recently been making increased use of his "own motion" investigation powers and his review powers to address issues arising from integrated activities, noting that these powers are particularly important in covert areas of activity where complaints are unlikely. One such area is Australian Crime Commission activity because the ACC's role does not bring its staff into close contact with members of the public.[64]

As part of its review functions, the Ombudsman reviews the AFP's and the ACC's records for compliance with record-keeping requirements for telecommunications interception warrants and reports on any breaches of the *Telecommunications (Interception) Act 1979* discovered in the process.[65] The *Crimes Act 1914* also requires the Ombudsman to review the propriety of "controlled operations."[66] Controlled operations usually involve law enforcement officers engaging in conduct that, unless authorized by a statutory certificate, would constitute an offence. Similarly, the *Surveillance Devices Act 2004* requires

the Ombudsman to review the use by law enforcement agencies of defined surveillance devices for compliance with the Act.[67]

The Ombudsman recently completed an own motion investigation into the cancellation of visas and the subsequent detention of long-term permanent residents of Australia. The investigation was initiated because of several serious complaints made to the Ombudsman.[68]

Arrangements to Address Accountability Gaps[69]

Although it has not yet done so, the Office of the Ombudsman can also enter into investigation "arrangements" with other accountability bodies with jurisdiction over members of the integrated Australian Crime Commission.[70] The rationale for this statutory mechanism seems to be an acknowledgment that accountability gaps could exist, partly because many members of the ACC are seconded from numerous other domestic agencies and thus covered by various legislative frameworks, and partly because the ACC combines both federal-level and state-level personnel.[71]

The Ombudsman's office often works informally with many other review bodies in reviewing matters that touch both areas of responsibility, including in particular the Inspector-General of Intelligence and Security. While they are constrained to some extent by secrecy legislation, the Ombudsman and the Inspector-General have found joint investigations and other forms of co-operation highly useful. For example, the two offices have conducted several joint reviews concerning complaints flowing from the execution of overt entry and search warrants by the Australian Security Intelligence Organisation that were supported by the Australian Federal Police and various state police forces. Because of such integrated police and intelligence activities — which can include state police — the Parliamentary Joint Committee on ASIO, the Australian Secret Intelligence Service and the Defence Signals Directorate recently recommended that "consideration be given" to "greater liaison between" the Ombudsman, the state ombudsmen and the Inspector-General, including a memorandum of understanding or protocol governing possible joint reviews of combined ASIO/police operations.[72] A memorandum of understanding was concluded between the Ombudsman and the IGIS on December 14, 2005.

2.3.1.4
Powers

The Ombudsman has the power to compel all documents and information that he or she believes to be relevant,[73] and can enter police premises and cause individuals to attend to answer questions under oath.[74] Recent legislative

amendments have clarified that an agency that provides documents to the Ombudsman for the purpose of an investigation, but without a statutory notice having been issued by the Ombudsman, will not thereby have waived legal professional privilege or be in breach of the *Privacy Act* or a secrecy provision in another enactment.[75] However, in some cases the Ombudsman may be prevented from requiring information or production, or from entering a particular place, by a certificate from the Attorney-General on grounds such as public interest, security or Cabinet privilege.[76] Because the Office and the agencies under review tend to work co-operatively to address such concerns, these certificates are rare.

Following an investigation, the Ombudsman can make findings and recommendations and, in the case of complaints, can ask that the respective department or agency report back to the Office on any corrective action taken in response.[77] The Ombudsman does not have binding remedial powers.

2.3.1.5
Reporting

The Ombudsman submits reports of its complaints investigations to the minister responsible for the respective department or agency.[78] Where a department or agency has not taken recommended corrective action within a reasonable time, the Ombudsman may submit a report to the Prime Minister[79] and a special report to the House of Representatives and the Senate.[80]

Upon completing an investigation, the Ombudsman reports to the Commissioner of the AFP actions by AFP members that merit criticism, and can request further action.[81] If in the Ombudsman's view, adequate and appropriate action is not taken, the Office may inform the Prime Minister and provide a report to Parliament.[82]

When a complaint is filed about the AFP, the Ombudsman must inform complainants of the outcome.[83] The Ombudsman's governing statutes are otherwise silent as to reporting obligations to complainants.

The Ombudsman also submits annual reports to the responsible minister, for "presentation to the Parliament,"[84] and may similarly submit special reports on any matter that arises in connection with the Office's mandate.[85]

2.3.1.6
Appointment

The Commonwealth Ombudsman is appointed by the Governor-General for a term not exceeding seven years and may be reappointed.[86] The statute does not set out any requisite qualifications for appointment.

2.3.2 Inspector-General of Intelligence and Security

2.3.2.1 Jurisdiction

The Inspector-General of Intelligence and Security has varying review authority over six agencies: ASIO, ASIS, DSD, DIO, DIGO and ONA.[87]

The Inspector-General's office noted that its multi-agency jurisdiction offers several advantages: a comprehensive view of the activities of the various intelligence agencies; the ability to ensure consistent interpretations by the agencies of their shared legislation; and the ability to scrutinize integrated and information-sharing activities. It observed, however, that a review body with such multi-agency jurisdiction must be properly resourced to fulfill its mandate.

2.3.2.2 Mandate

The Inspector-General's mandate is generally expressed in the objects of the Act:

(a) to assist Ministers in the oversight and review of:
  (i) the compliance with the law by, and the propriety of particular activities of, Australian intelligence or security agencies;
  (ii) the effectiveness and appropriateness of the procedures of those agencies relating to the legality or propriety of their activities; and
  (iii) certain other aspects of the activities and procedures of certain of those agencies;
(b) to assist Ministers in ensuring that the activities of those agencies are consistent with human rights; and
(c) to allow for review of certain direction given to ASIO by the Attorney-General.[88]

2.3.2.3 Functions

The Inspector-General has a complaint-processing function, an "own motion" investigation function, and an inquiry function pursuant to ministerial or prime ministerial request. However, these functions, and the matters in which they can be engaged, vary according to the agency in question.[89] In general, the IGIS has

the broadest functions with respect to ASIO, and narrower ranges of functions with respect to ASIS, DSD, DIGO, DIO and ONA.

For example, with respect to ASIO, the IGIS can inquire into the legality and propriety of ASIO activities; the effectiveness and appropriateness of its procedures relating to legality or propriety; and the consistency of its activities with human rights instruments, all pursuant to either a complaint, the Inspector-General's own motion or the minister's request.[90]

With regard to ASIS, DIGO and DSD, however, the IGIS can inquire only into "the effectiveness and appropriateness of the procedures relating to legality or propriety of the activities of that agency" pursuant to ministerial request, and not pursuant to complaint or its own motion.[91]

The Act sets out further review powers and limits. These include the power to inquire into whether certain ministerial directions to ASIO are justified,[92] and a general prohibition on inquiries, without ministerial approval, into any matter that occurred outside Australia.[93] In all cases, the Inspector-General requires the minister's approval before inquiring into a matter that occurred outside Australia.[94]

The Inspector-General can also be directed by the Prime Minister to inquire into certain matters,[95] including into the actions of agencies outside its ordinary statutory purview. For example, the Prime Minister asked the Inspector-General to look into whether there was any intelligence that warned of the 2003 bombing in Bali. That review included the Australian Federal Police.[96]

2.3.2.4
Powers

The Inspector-General can compel any information from any person that he or she believes is relevant to any inquiry he or she is conducting. The statute does not exclude information covered by solicitor-client or Cabinet privilege, but does require the Inspector-General to arrange for the protection of any information with a national security classification.[97] Any information so obtained cannot be used as evidence in criminal proceedings except in very limited circumstances.[98]

The statute also provides for consultation with the Auditor-General to avoid duplication of inquiries.[99] A similar statutory provision for consultation with the Commonwealth Ombudsman was recently inserted into the *IGIS Act*.[100] The Inspector-General noted the co-operation that already exists between his Office and the Office of the Ombudsman.[101] He also noted the Parliamentary Joint Committee's recommendation for formalized co-operation, and the recent memorandum of understanding between the two offices that resulted, which I discussed earlier.

2.3.2.5
Reporting

After completing an inquiry, whether pursuant to a complaint, a ministerial request or his or her own motion, the Inspector-General must provide a draft copy of the report to the head of the agency in question. If the agency provides comments on the draft report within a reasonable time, the Inspector-General must include relevant comments in the final report.[102]

The Inspector-General must give copies of the final report to the head of the agency and to the responsible minister. Where the Prime Minister had requested the inquiry, the Inspector-General must also provide a copy to the Prime Minister.[103] The report must contain conclusions and recommendations, and may include a recommendation that an individual receive compensation.[104]

The head of the relevant agency may propose action in response to such reports. If the Inspector-General is not satisfied that the action is adequate and appropriate, he or she may discuss the matter with the responsible minister and provide a report to the Prime Minister.[105]

Where an individual has filed a complaint, the Inspector-General must provide a written response to the complainant, although this response does not necessarily include a copy of any report or other document otherwise produced. Before doing so, the Inspector-General must ensure that the head of the relevant agency agrees that the content of the response will not prejudice security, Australia's defence or Australia's relations with other countries.[106]

The Inspector-General must also provide an annual report to the Prime Minister, including comments on any inquiry concerning ASIO's collection or communication of intelligence about a particular individual, comments on any review, and comments on ASIS' and DSD's compliance with rules on the communication and retention of intelligence information on Australian persons.[107]

The Prime Minister must give copies of such reports to the Leader of the Opposition in the House of Representatives and cause a copy to be laid before each House of Parliament.[108]

2.3.2.6
Appointment

The IGIS is appointed by the Governor-General on the recommendation of the Prime Minister after consultation with the Leader of the Opposition.[109] The appointment is for a term not exceeding five years and may be renewed only once.[110]

3.
BELGIUM

3.1
OVERVIEW

Belgium is a constitutional monarchy with a parliamentary system of governance. Power is divided among three branches: legislative, executive and judicial. The legislative branch, Parliament, is made up of a House of Representatives and a Senate. The executive branch formally consists of the King and his ministers, but it is the Prime Minister and his or her ministers who exercise the powers of the executive branch. However, the King must sign legislation passed by Parliament for it to become law.[111]

Belgium is also a federal state. Legislative jurisdiction is divided among the federal government, three regions (Flanders, Wallonia and Brussels) and three linguistic communities (Flemish, French and German).[112] The federal government has legislative jurisdiction over foreign affairs, national defence and justice.[113] Its jurisdiction includes the authority to regulate law enforcement bodies and security intelligence agencies. The 10 provinces and 589 communities and municipalities also have some jurisdiction over internal security matters and public order.[114] Policing at the federal level is carried out by the Federal Police and at the local level by almost 200 local police forces.[115] Belgium has two security intelligence agencies: a civil security intelligence service and a military intelligence service.

The Belgian Parliament recently passed legislation creating terrorism-specific offences,[116] including offences specific to the financing of terrorism;[117] and legislation increasing police investigative powers.[118]

Belgium's review landscape is notable in part because its police agencies are all subject to the same review body, Committee P, and its two security intelligence agencies are subject to a similar body, Committee I. Both committees are governed by the same statute. Committee P is mandated to review the police forces' compliance with law, respect for individual rights and effectiveness. It has both complaint-based and review-based jurisdiction over all police forces and individuals vested with police powers. Indeed, Committee P's reports evidence a wide scope of review, from investigations into complaints from the public to various self-initiated reviews such as the review of warrants, studies of alleged discrimination, and studies of the effectiveness of the police forces, including their counter-terrorism efforts and information-sharing practices.

Committee I has a similar mandate with respect to scrutiny of Belgium's intelligence agencies.

The Belgian review model is also notable because Committee P and Committee I are empowered by law to conduct joint investigations, and are required to meet regularly and consult. Since 2005, the chairs of the two committees have also sat on a joint committee, together with the chair of the Privacy-Protection Commission. This joint committee hears appeals from security-clearance decisions. The Belgian model shows that when properly empowered, review bodies for different agencies can co-operate productively and effectively to monitor integrated national security activities.

3.2
LAW ENFORCEMENT AND INTELLIGENCE

3.2.1
Federal Police and Judicial Police

Belgium has police forces at both the federal and local levels, all provided for by statute.[119] The Federal Police are responsible for investigations affecting more than one local police zone and for providing support to local police forces. The Federal Police have five major divisions, one of which — the Judicial Police — carries out specific types of criminal investigations such as those related to drug trafficking and organized crime. The Federal Police also have "special" units for certain activities and investigative techniques, and divisions in charge of liaison with foreign agencies and local police forces.[120]

Within the Judicial Police is a counter-terrorism headquarters known as *programme Terro*. This body coordinates and provides operational support and expertise to field units and other domestic and international bodies involved in counter-terrorism,[121] including coordinating interaction between police units and intelligence agencies. Some local police forces also have special counter-terrorism units. The most notable is the Brussels police counter-terrorism division, known as the *DR3*, which comprises six investigative branches and handles the majority of counter-terrorism investigations in Belgium.[122] Belgium has approximately 46,000 police officers.[123]

Since 1984, Belgium has also had in place the *Groupe interforces antiterroriste* (GIA). Composed of representatives of the police and intelligence agencies, this body coordinates information exchange between these organizations. The GIA analyzes intelligence, coordinates responses and is linked to the government's national crisis centre.[124]

3.2.2
State Security Service and Intelligence and Security Service

Belgium has two intelligence agencies: the State Security Service (SE), and the military and general Intelligence and Security Service (SGRS).[125] Both are governed by statute.[126]

The SE is responsible for intelligence collection and analysis of any activity that threatens or could threaten internal domestic security and democratic and constitutional order, external security and international relations, economic and scientific capacity, and any other fundamental national interest as defined by ministerial committee.[127] These threats are further defined in the legislation, and include terrorism and extremism.[128]

The SGRS is responsible for intelligence collection and analysis of any activity that threatens or could threaten territorial integrity, military defence planning and missions, the security of Belgians abroad, and any other fundamental national interest as defined by ministerial committee.[129] It must also ensure the security of ministry of defence personnel, military installations, equipment and systems; and protect military secrecy.[130]

The governing statute for the SE and the SGRS sets out their powers and limitations, and oversees activities such as information collection, retention and sharing.[131] The legislation also creates the power in public servants and agencies, and in judicial authorities, to disclose information to these agencies in certain circumstances.[132]

3.3
REVIEW AND OVERSIGHT

3.3.1
Committee P

3.3.1.1
Jurisdiction

All of Belgium's police forces, as well as all persons "individually assigned to investigate and ascertain violations of the law," are subject to the jurisdiction of the Standing Police Monitoring Committee (Committee P).[133] A number of public authorities with personnel are generally understood to fall within this category, but disagreements abound as to whether they in fact do fall within Committee P's review[134] jurisdiction. These include personnel working in customs, transport and environment authorities.

Committee P expressed its preference for a review system like Belgium's, in which one agency specializes in reviewing police services and the other in reviewing intelligence services. The Committee observed that combined with a statutory mechanism for exchanging information and carrying out joint investigations, such a system allows each review body to specialize in the respective work of the police or intelligence services, and responds to the differences in operational culture, mandates and activities of the two services. Both Committee P and Committee I noted, however, that there is increasing overlap between intelligence activities and law enforcement activities.

3.3.1.2
Mandate

Committee P's mandate is to review the police forces' compliance with legal and constitutional protections of individual rights, as well as their coordination and effectiveness.[135]

The Committee reviews police activities, methods, internal regulations, directives and any document regulating members' conduct.[136] It addresses matters as diverse as allegations of theft of personal items by police officers, the quality of holding cells and food provided by the police to detainees, allegations of racism and discrimination, the adequacy of warrants, the efficiency of the federal police force's approach to terrorism, the propriety and efficiency of police integration with other domestic and international agencies, and the efficiency of police information-sharing systems.[137]

3.3.1.3
Functions

Committee P undertakes its reviews either on its own initiative; on the initiative of its investigation department[138]; upon receipt of a complaint; or upon request by a House of Parliament, a minister given such authority under the statute, or certain other authorities, such as prosecutors and local police authorities.[139]

In Committee P's view, combining a complaint-processing and a review function in one body is advantageous. The Committee finds that investigating complaints helps develop knowledge of and expertise in the activities under review, and that complaints often indicate problems in certain areas. Committee P has in fact shifted much of its focus from first-instance complaint processing to analyzing the information that complaints provide about potential systemic problems or other areas requiring greater scrutiny. In doing so, the Committee is increasingly leaving resolution of complaints to police forces while monitoring outcomes and retaining the right to investigate if it is dissatisfied.

Committee P made this shift for three main reasons:

(i) It recognized that its complaint-processing burden was becoming untenable;
(ii) It believes that police are best equipped to deal with most complaints and more likely to self-improve if they bear primary responsibility for complaint handling (under the scrutiny of, and with the threat of secondary recourse to, an external monitor); and
(iii) It views the analysis of complaint trends and potential systemic problems as a critical task.

3.3.1.4 Powers

Committee P has the right to any police document that it deems relevant to its activities.[140] When conducting investigations, the Committee can compel documents and information that it deems necessary from any person. In addition, police officers may give evidence to Committee P concerning matters covered by professional secrecy.[141] Where a police officer objects to disclosing information on the grounds that it places an individual in physical danger, the chair of Committee P determines the issue.[142]

Committee P's investigation department has the power to conduct reviews and investigations in places where the members of a police force work, and may seize objects or documents from these places, except those relating to ongoing investigations or legal proceedings in progress.[143] The police commander or deputy police commander may object to the seizure of objects or documents on the grounds that it may jeopardize the safety of an individual. In such cases, Committee P's chair will receive representations on the matter and determine whether the investigators may proceed with the seizure.[144] The Committee and its investigation department can also seek the assistance of interpreters and experts.[145] Committee P can make recommendations, but not binding orders.[146] In the context of Belgium's civil law system, Committee P's investigation department also undertakes judicial investigations into suspected criminal conduct by members of the police force.[147]

Under its governing statute, Committee P is required to exchange information with Committee I about its activities, send Committee I its reports and conclusions, hold joint meetings where complementary information can be exchanged, and jointly discharge its mandate in certain circumstances.[148] Committee I has an identical mandate.[149] These provisions have led committees P and I to conduct several joint investigations, including an investigation of

police and intelligence coordination and a current review of terrorism coordination among police and intelligence agencies.

Both committees spoke favourably about the potential benefits of such co-operation. Among such benefits are the exchange of information on the integrated activities of police and intelligence services, particularly in an era of increasing overlap in the mandates of police and intelligence services; and increased information sharing and co-operation. As Committee P stated, institutional co-operation among review bodies is vital where there is institutional co-operation among the bodies being reviewed — otherwise, there is too great a risk that one body or the other will escape scrutiny. However, the committees noted challenges that have arisen in carrying out joint investigations, including the following:

- differences in operational culture, approaches, structures and objectives between the police and intelligence services;
- differences in size of the respective forces and the corresponding Committee workload; and
- difficulty in reaching joint conclusions and recommendations. The committees noted, however, that much could be gained from joint investigations with separate conclusions and recommendations.

The committees also noted that because they receive reports from both committees and are empowered to request investigations, Parliament and the ministers can play a role in encouraging coordination and co-operation in review activities.[150] This parliamentary monitoring role is performed for the most part by standing parliamentary commissions with access to both committees' reports.

Since 2005, Committee P has co-operated with Committee I in another way. The chairs of Committee P and Committee I, along with the head of the Privacy-Protection Commission, sit on a committee that hears appeals from negative security-clearance decisions. Committee I's chair is both the chair of this committee and holds the chief bureaucratic position.[151]

Committee P also co-operates with the Centre for Equal Opportunities and Opposition of Racism, as regulated by law and developed in a co-operation protocol. In addition, Committee P has concluded protocols creating systems to exchange information with the federal and local police, and is in the process of negotiating further information-sharing protocols. Finally, Committee P maintains informal relationships with other national and international accountability bodies, which can result in the Committee conducting an inquiry.

3.3.1.5
Reporting

Committee P prepares reports of its investigations, including conclusions and recommendations, and submits them to the responsible minister, the relevant police authority and the House of Representatives.[152] It also submits annual reports to the relevant minister and to both Houses of Parliament, as well as follow-up reports where, in its view, its recommendations have not led to satisfactory corrective measures.[153] Where only one House of Parliament has asked Committee P to investigate a matter, the Committee submits a report to both bodies.[154]

3.3.1.6
Appointment and Composition

Committee P consists of five individuals appointed by the House of Representatives for a five-year term. To be eligible for appointment, an individual must have at least seven years of high-level experience in criminal law, criminology, public law or management, acquired in a setting similar to policing or intelligence. The Committee chair must be a judge. Although only two members of Committee P currently have top secret clearance, all will be so cleared in future.[155]

3.3.2
Committee I

3.3.2.1
Jurisdiction

Review of Belgium's intelligence agencies is carried out by the Permanent Committee for the Control of Intelligence Services (Committee I).[156] Committee I has jurisdiction over Belgium's two principal intelligence-collection bodies: the State Security Service (SE) and the military and general Intelligence and Security Service (SGRS).[157]

Committee I's jurisdiction used to be defined more broadly, and included any new public body with a mandate to collect and analyze information in the interest of security. Partly because of disagreements as to which agencies or activities this definition covered, the statute was amended in 1999.

Although Committee I no longer has jurisdiction over other bodies involved in intelligence, its monitoring of both the SE and the SGRS has several advantages in the Committee's view. It allows the Committee to compare the methods used and the information held by each service, and to observe how the two

agencies collaborate and coordinate. It also allows the Committee to note when information has flowed to another public authority, such as a police force, and when such other bodies might take actions that could require scrutiny. Committee I can then note these observations in its reports to Parliament, and Parliament can choose to ask the appropriate authorities to look into the matter. By formulating recommendations in such cases, Committee I can also caution or urge the intelligence agency in question to alter its actions accordingly.

3.3.2.2
Mandate

Committee I is mandated to scrutinize the intelligence agencies' respect for individual rights as guaranteed by statute and the Constitution, as well as their coordination and effectiveness.[158] The Committee reviews the agencies' activities and methods, internal regulations, directives and all documents regulating member conduct.[159]

Committee I's reviews have covered a range of topics — the role of intelligence services in protecting national scientific and economic capacity, the conduct of the SE and the SGSR in certain investigations, complaints from members of the public, the efficiency of the "protected persons" unit of the SE, and the information-sharing practices of the SE and the SGSR.[160]

3.3.2.3
Functions

Committee I can conduct reviews on its own initiative, on the initiative of its investigation department,[161] upon receipt of a complaint, or upon request by a House of Parliament or by a minister identified in the statute.[162] Committee I shared Committee P's view that combining a complaint-processing and review function in one body is advantageous. The two functions are seen to both build expertise and provide indicators that may contribute to more effective review in the other function.

3.3.2.4
Powers

Like Committee P in relation to Belgium's police forces, Committee I has the right to obtain any document from the intelligence services that it deems relevant to its activities.[163] When conducting investigations, Committee I can compel documents and information that it deems necessary from any person. Intelligence officers may also give evidence to Committee I concerning matters covered by professional secrecy.[164]

Committee I's investigation department has the power to inspect any premises where members of the intelligence services work, and may seize objects and documents from these premises, except those relating to ongoing investigations.[165] The relevant commander or deputy commander may object to the seizure of documents if it might jeopardize the physical safety of an individual, or if the documents contain classified information and the seizure might jeopardize the conduct of security or intelligence-related activities. In such cases, the intelligence service may make representations to the chair of Committee I, who will determine whether investigators may seize the objects or documents.[166] The Committee and its investigation department can also seek the assistance of interpreters and experts.[167] Committee I can make recommendations but not binding orders.[168] In the context of Belgium's civil law system, Committee I's investigation department also undertakes judicial investigations into suspected criminal conduct by members of the intelligence services.

As I noted above, Committee I and Committee P are required by statute to exchange information and reports, and to meet regularly.[169] Committee I concurred with Committee P that these provisions, while useful, are difficult to implement effectively.

3.3.2.5
Reporting

Like Committee P, Committee I prepares reports of its investigations, including conclusions and recommendations, and submits them to the responsible minister. However, Committee I submits these reports to the Senate rather than to both Houses of Parliament.[170]

Committee I submits its annual reports to both Houses of Parliament and to the relevant minister. It also submits reports to both Houses of Parliament and to the responsible minister where, in its view, its recommendations have not led to satisfactory corrective measures.[171] Where only one House of Parliament has asked Committee I to investigate a matter, the Committee submits a report to both bodies.[172]

3.3.2.6
Appointment and Composition

Committee I is composed of three individuals appointed by the Senate for a five-year term. To be eligible for appointment, individuals must have a law degree and at least seven years of high-level experience in criminal law, criminology, public law or management, acquired in a setting similar to policing or

intelligence. The Committee chair must be a judge. All members must have top secret clearance.[173]

4. GERMANY

4.1 OVERVIEW

Germany is a federal republic in which the division of powers between the federal government and the 16 states has helped to shape the institutional framework of policing and security intelligence. That framework has traditionally distinguished between police activity and intelligence activity, and assigned the bulk of responsibility for policing to the states.[174] The states also collect intelligence.[175]

Legislative changes since September 2001 — termed the "first security package" and the "second security package" — have altered aspects of both policing and intelligence.[176] The first security package amended substantive laws to target extremist and terrorist organizations. The second security package amended regulations to seventeen statutes and five statutory orders, broadening the scope of permissible actions for federal security and law enforcement authorities, and increasing information sharing between agencies.[177] Funding for national security and counter-terrorism was also increased.[178]

Notably, while Germany does have several of the accountability controls typically found in liberal democratic countries — judicial scrutiny, privacy-protection instruments and ministerial oversight, for example — it does not have an independent body to deal with complaints about the police.[179] Its intelligence agencies are scrutinized by a parliamentary committee called the Parliamentary Control Panel.

Since Germany has no independent review agency dedicated to its police services, I have not discussed German law enforcement agencies in this chapter. More information on policing in Germany is included in the Commission's Background Paper on International Models, which can be found on the Commission website, www.ararcommission.ca.

This section of the chapter therefore focuses on Germany's security intelligence landscape, and the applicable review and oversight mechanisms: the Parliamentary Control Panel and the G-10 Commission.

4.2
SECURITY INTELLIGENCE

Security intelligence services in Germany gather and evaluate information on foreign and internal security, in part through covert means. They may not be attached to any police authority.[180]

4.2.1
Federal Office for the Protection of the Constitution

The Federal Office for the Protection of the Constitution (BfV)[181] is Germany's federal domestic intelligence agency. It falls within the jurisdiction of the Federal Ministry of the Interior.[182] As set out in its governing statute, the BfV's main function is to gather and analyze information on activities that are directed against Germany's "free and democratic order" or state security, activities carried out by a foreign power in Germany, and activities in Germany that threaten German foreign interests through force or preparations for the use of force.[183] Since 2002, the BfV's mandate has also included gathering and analyzing information on activities "directed against the idea of international understanding," especially against the "peaceful coexistence of peoples."[184] In addition, the Office assists with security clearance checks of personnel for security-sensitive civilian or military positions.[185]

The BfV says it works "closely . . . with other security authorities, in particular the other federal intelligence services [the MAD and the BND] responsible for foreign intelligence, and with police and criminal prosecution authorities."[186] It uses both public information and covert intelligence methods.[187] Its powers were recently expanded to allow it to obtain, subject to certain conditions, information from financial institutions, airlines, postal service providers and telecommunications companies without disclosure to targeted customers.[188] The BfV does not have the powers to arrest, search or interrogate, or to seize property.[189] It may hand over a matter to the courts, public prosecution office or police to "decide independently" what action is required.[190] The BfV employs approximately 2,400 people.[191]

Every state also has its own Office for the Protection of the Constitution, with a structure comparable to that of the BfV. Each office has regional jurisdiction and is subject to state regulation. The BfV does not have direct control over the activities of the state offices, but is required to co-operate with them.[192] When a surveillance target's activities extend beyond the territory of a single state, the BfV will take over responsibility for the investigation.[193] Intelligence gathered by the states is stored centrally by the BfV.[194] The Federal Minister of

the Interior has raised the question of whether the BfV might in future be given the right to issue directives to the equivalent state-level authorities.[195]

4.2.2
Military Counterintelligence Service

Germany's Military Counterintelligence Service (MAD)[196] is part of the armed forces, but is solely a domestic-intelligence service.[197] Its statutory basis is in the *Military Counterintelligence Service Act*.[198] The MAD's functions include gathering and evaluating information on anti-constitutional activities within the German armed forces, and on activities such as espionage directed against the German armed forces.[199] However, the MAD is not involved in foreign military intelligence operations: these are conducted by the Federal Intelligence Service. The MAD's powers, like the BfV's, have recently been enlarged to encompass gathering and analyzing information on activities directed against the idea of international understanding, especially against the peaceful co-existence of peoples.[200] The MAD may also now demand information from telecommunications and teleservice companies, and transmit personal information to other agencies or institutions.[201] The MAD currently has about 1,300 staff.[202]

4.2.3
Federal Intelligence Service [203]

The Federal Intelligence Service (BND) is Germany's foreign intelligence and signals intelligence service.[204] It comes under the jurisdiction of the Head of the Federal Chancellery[205] and has a statutory basis in the *BND Act*.[206] Since 1994, the BND has been authorized to monitor international telecommunications without prior concrete suspicion in order to prevent certain offences.[207] However, the BND may not target the specific communication lines of German citizens.[208] Like the BfV and the MAD, the BND may now request information from financial service institutions, postal service providers, telecommunications services and airlines.[209] Recent legislation authorizes the BND to transmit personal information to the BfV, state offices for the Protection of the Constitution and the MAD, where necessary to those organizations' activities in certain circumstances.[210] The BND currently has approximately 6,000 staff.[211]

4.2.4
Commissioner for the Federal Intelligence Services

Coordination between the federal intelligence services, and between these services and other agencies, is the responsibility of the Commissioner for the Federal

Intelligence Services. The Commissioner must be a minister of state or a state secretary within the Federal Chancellery.[212]

4.3
REVIEW AND OVERSIGHT

Germany has no arm's-length agency to investigate complaints against its police forces, nor any agency similar in structure to Belgium's Committee I or Canada's SIRC to review its intelligence agencies. Instead, Germany's intelligence agencies are scrutinized by a legislative committee called the Parliamentary Control Panel (PKGr).[213] A separate body, the G-10 Commission, reviews interceptions of private communications.

4.3.1
Parliamentary Control Panel

4.3.1.1
Jurisdiction

Pursuant to its governing statute, the Parliamentary Control Panel has jurisdiction to review the activities of three agencies: the Federal Office for the Protection of the Constitution, the Military Counterintelligence Service and the Federal Intelligence Service.[214]

The Panel thus takes a functional approach to review, which "facilitates seamless oversight" because different parts of the intelligence machinery work closely together.[215]

4.3.1.2
Mandate

The PKGr's mandate is to scrutinize and report on the general intelligence activities of the federal government, as exercised by the three intelligence agencies.[216] Under the PKGr's statute, "activities" refer to procedures that "enable an intelligence service to operate and fulfill its task."[217] General activities are those that relate to typical procedures.[218] The Panel's mandate includes review of both the policies and operations of the intelligence services.[219]

The PKGr reviews certain information-gathering activities conducted by the intelligence services in Germany. For example, it reviews information gathering from financial and credit service institutions concerning accounts, account holders and financial transactions; and information gathering from airlines concerning their passengers' names, addresses and other information.[220]

The Panel also reviews intelligence operations of particular importance. An operation is considered of particular importance when knowledge of the operation "is essential for the exercise of effective parliamentary control in the public interest."[221] Intelligence operations that are the subject of media scrutiny and decisions to alter essential procedures fall within this definition.[222]

4.3.1.3
Functions

The PKGr carries out its monitoring work by hearing presentations from the executive and the heads of the intelligence services;[223] conducting self-initiated reviews of the intelligence services' files; and investigating complaints by members of the three services or by the public.[224] It also must approve the Federal Minister of the Interior's determinations on the risk categories in which strategic telecommunications surveillance may occur under the *G-10 Act*.[225] These categories include international terrorism, serious narcotics crime, international money laundering and counter-proliferation.[226]

The PKGr participates in drawing up guidelines for current and future intelligence activities.[227] It also consults with the government on the intelligence services' annual budgets, provides an assessment of draft budgets to the appropriate legislative budget committee[228] and reviews the implementation of budgetary plans for the intelligence services.[229]

The PKGr must meet at least once per quarter,[230] and in practice meets much more often.[231] To facilitate parliamentary review of complex security intelligence activities, laws and practices, a five-person secretariat provides independent expertise and research assistance in support of the Panel's review function.[232]

4.3.1.4
Powers

The federal government is obliged to provide the PKGr with comprehensive information concerning the typical procedures of the German intelligence services. Under this rubric, the federal government gives the PKGr information about both working procedures for the intelligence agencies and the results of intelligence operations.[233] The federal government also must provide the Panel with information on operations of particular importance.[234] In addition, the PKGr may call upon the federal government to report on other operations, a power it uses regularly.[235]

Upon request, the PKGr has the power to visit the security services at any time and to question intelligence service staff members.[236] It can also compel

information and documentation from the intelligence services and hold hearings,[237] although the federal government may refuse to disclose information obtained from foreign authorities and may withhold information to protect sources or third-party rights. The executive may also refuse to disclose information that "touches upon core aspects of executive responsibility," such as the decision-making process within the federal government, including consultations between different departments.[238] The government must provide reasons for such refusals to disclose.

The Panel may appoint an external expert to conduct specific inquiries on a case-by-case basis.[239] It also approves the G-10 Commission's rules of procedure.[240]

4.1.3.5
Reporting

The PKGr submits two reports to the Bundestag per legislative session — one mid-session and one at the end. These reports are subject to a statutory requirement of strict confidentiality, meaning that they may not disclose classified information. However, there is one exception to the rule of strict confidentiality. With the approval of two thirds of the PKGr, the Panel may publish its assessment of a current operation, although it does not publish the details of the operation itself.[241] This exception has been created to both satisfy the public's need for information about current controversies and strengthen the PKGr's role.

The PKGr must submit a special annual report on covert interception of communications by the intelligence services and on the new powers assigned to the intelligence services under the 2002 *Counter-Terrorism Act*,[242] namely, the review by the intelligence services of bank accounts, flight documents or telecommunication connection data.[243] These reports discuss the scope and method of measures the intelligence agencies used to intercept mail and telephone communications.[244]

The federal states must also report to the PKGr annually on any measures they have taken under the *Counter-Terrorism Act*.[245]

4.3.1.6
Appointment and Composition

The PKGr is composed of nine members elected by the Bundestag and representative of the political balance in the legislature. Each member must be elected by a majority of the Bundestag. This requirement is intended to demonstrate that Parliament as a whole has confidence in each Panel member, which in turn

is intended to create a relationship of trust between the Panel and the government's executive branch.[246]

The chair of the PKGr rotates on January first and July first every year, and is appointed alternately by the majority and minority groups in the Bundestag. Members remain part of the PKGr as long as they are members of the Bundestag and not of the executive branch. When a legislative session ends and a new Bundestag is elected, members remain in their roles until the Bundestag elects a new Panel.[247]

The small number of members is intended to reflect the need for secrecy and assure the intelligence services that any information the PKGr receives will be treated confidentially.[248] Panel secretariat staff undergo security checks but, on the basis that they are the elected representatives of the people, PKGr members are not subject to such checks.[249]

4.3.2 G-10 Commission

4.3.2.1 Jurisdiction

Article 10 of the German *Basic Law* guarantees a right to communications privacy. Any restriction on this right must accord with the provisions of the *Article 10 Act*, commonly known as the *G-10 Act*.[250] The G-10 Commission is responsible for approving any surveillance measures ordered by the federal intelligence services under this statute.[251] In relation to the BfV and the MAD, the G-10 Commission approves interceptions of the communications of individuals. It also approves strategic communications interceptions for signals intelligence purposes by the BND, which monitors communications channels as a whole and then identifies individual communications for closer study.

4.3.2.2 Mandate and Functions

The G-10 Commission must review and approve, on a case-by-case basis for compliance with the Act, all communications intercepts ordered under the *G-10 Act* and conducted by the federal intelligence services.[252] The G-10 Commission also reviews the federal intelligence services' entire process of collecting, processing and using data.[253] This mandate includes monitoring data-gathering and deletion procedures, and data-processing practices. The G-10 Commission also may consider individual complaints:[254] it generally receives between 20 and

30 complaints a year.[255] Before the Commission reviews any matter, its secretariat provides a preliminary assessment. The Commission must meet once a month.

4.3.2.3 Powers

The G-10 Commission exercises judicial, rather than political, control over the covert surveillance activities of the intelligence services. Unlike German courts, the G-10 Commission may refuse to approve an operation that it considers either unnecessary or inopportune.[256] The Commission's rulings are binding on the intelligence services and on the government. However, individuals affected by surveillance activities may request judicial review of the Commission's decisions.[257]

The Commission members and the secretariat staff may require information from the intelligence services and may access all relevant documents, including data stored electronically. The Commission may also require access to the intelligence services' premises.[258]

4.3.2.4 Reporting

The G-10 Commission is not required to submit reports.[259]

4.3.2.5 Appointment and Composition

The four full and four deputy members of the G-10 Commission are appointed by the PKGr. The Commission chair must be qualified to hold judicial office. Commission members are not normally members of the Bundestag, but may be. However, they are generally members of or closely associated with political parties, although they hold office independently and are not bound by any instructions. Members are expected to have technical, political or judicial expertise in a relevant area. All members are entitled to take part in the Commission's meetings.[260]

The Commission's secretariat staff must also be qualified to hold judicial office and must have some technical expertise in the area of communications surveillance and the applicable law.[261]

5. NEW ZEALAND

5.1 OVERVIEW

New Zealand is a member of the Commonwealth with constitutional and government structures similar to Canada's. However, it is a unitary state with only one police force, the New Zealand Police, whose activities include national security law enforcement activities. There are two principal security intelligence agencies, the New Zealand Security Intelligence Service (NZSIS) and the Government Communications Security Bureau (GCSB).

The New Zealand Police are subject to the complaint- and incident-based jurisdiction of the Police Complaints Authority. The security intelligence agencies are subject to the complaint- and review-based jurisdiction of the Inspector-General of Intelligence and Security (IGIS).

5.2 LAW ENFORCEMENT AND INTELLIGENCE

5.2.1 Police

The New Zealand Police are organized into twelve districts[262] and governed by statute.[263] There have been a number of recent counter-terrorism changes to their organization and powers.[264] The New Zealand Police also belong to the Combined Law Agency Group (CLAG), a "joint forum" of New Zealand law enforcement agencies.[265] The CLAG is described as the "primary vehicle for sharing information and for investigative co-operation on organised crime related matters."[266]

5.2.2 Intelligence Agencies

Both of New Zealand's two principal security intelligence agencies, the New Zealand Security Intelligence Service and the Government Communications Security Bureau, are civilian organizations. Other organizations, particularly the Defence Directorate of Intelligence and Security and the External Assessments Bureau, also assess and analyze foreign intelligence for government use.

5.2.2.1 New Zealand Security Intelligence Service

The New Zealand Security Intelligence Service is governed by statute.[267] Its mandate is to gather and analyze intelligence relevant to national security; advise ministers and public authorities on security matters; conduct security clearance inquiries; and co-operate with other authorities in New Zealand and abroad.[268] According to the NZSIS, the "largest single component" of its security intelligence advice relates to counter-terrorism.[269]

In collecting its intelligence, the NZSIS uses methods that include covert surveillance such as interception of both domestic and foreign communications. Its governing statute sets out the Service's powers and limitations. For example, the NZSIS may apply for warrants to carry out certain investigative activities such as search and seizure, but has no powers of arrest.[270]

5.2.2.2 Government Communications Security Bureau

The Government Communications Security Bureau is New Zealand's signals intelligence agency. It first became the subject of an enabling statute in 2003, which continued the GCSB and established it as a department of state.[271]

According to its governing statute, the GCSB's functions include gathering and analyzing foreign intelligence by intercepting communications; reporting to the responsible minister on foreign intelligence; decoding and deciphering signals intelligence; and co-operating with other authorities in New Zealand and abroad.[272] The GCSB maintains satellite communications interception stations[273] that "are useful to and are accessible by" other intelligence agencies, including American and Australian agencies.[274] The GCSB's governing statute also limits its powers.[275]

5.3 REVIEW AND OVERSIGHT

5.3.1 Police Complaints Authority

5.3.1.1 Jurisdiction

The Police Complaints Authority is the review body for the New Zealand Police. The Authority is complaint- and incident-based, and restricted in jurisdiction to the New Zealand Police.[276]

5.3.1.2 Mandate and Functions

The Authority investigates complaints alleging misconduct or neglect of duty, or concerning "any practice, policy, or procedure of the Police affecting" the complainant.[277] Complaints are investigated to determine whether the activity called into question was "contrary to law, unreasonable, unjustified, unfair, or undesirable."[278] The Authority may also, on its own motion, investigate cases in which a member of the Police appears to have caused death or serious bodily harm.[279]

The Authority may investigate complaints itself, "review" the Police investigation of the complaint, or "oversee" a Police investigation and direct the Police in doing so.[280]

5.3.1.3 Powers

The Police are required to provide the Authority with all necessary information and assistance.[281] The Authority may also compel production of information, documents or things, and may examine persons under oath.[282] However, the Authority's access will be blocked where either the Prime Minister certifies that the "giving of any information or the production of any document or thing might prejudice" New Zealand's security, defence or international relations, or the Attorney General certifies that doing so might prejudice the prevention, investigation or detection of offences, or involve disclosure of Cabinet secrets, injurious to the public interest.[283]

The Authority does not have the power to make binding recommendations to the Commissioner of the New Zealand Police. It may only communicate its opinion, with reasons and any recommendations, to the Commissioner.[284] The

Commissioner must notify the Authority of action proposed to be taken in response to Authority recommendations, and give reasons for any proposal not to implement the Authority's recommendations.[285]

5.3.1.4
Reporting

The Authority informs parties to a complaint of the results of an investigation "as soon as reasonably practicable . . . and in such manner as [the Authority] thinks proper."[286] If dissatisfied with the Commissioner's response to its recommendations, the Authority may send its opinion and recommendation to the Attorney-General and the Minister of Police, and transmit a report on the matter to the Attorney-General for tabling in the House of Representatives.[287]

The Authority also submits annual reports to the Minister of Justice, to be laid before the House of Representatives.[288] Sensitive or classified information would not appear in the annual reports, but would be dealt with in another manner according to the circumstances.

The Authority has the discretion to publish other reports on the exercise of its function or any particular case or cases.[289]

5.3.1.5
Appointment

The Authority is comprised of one person, who is appointed for a term of two to five years, with the possibility of reappointment,[290] on the recommendation of the House of Representatives.[291] The appointee must be a "barrister or solicitor of the High Court."[292]

5.3.1.6
Other

A review of the Police Complaints Authority in 2000 resulted in broad recommendations for change.[293] Subsequently, the Independent Police Complaints Authority Amendment Bill proposed more limited amendments to the Authority.[294] The bill would increase the renamed Authority's membership to three persons, including a chairperson who was a current or former judge. In the view of the Law and Order Select Committee, these changes were "needed to enhance the Authority's independence."[295] However, the Committee endorsed continuing the Authority's responsibility to maintain secrecy about its investigations, and preserving its recommendatory role.[296] The new structure has been delayed by the establishment of a Commission of Inquiry into alleged police misconduct, which has not yet issued its report.[297]

The Police Complaints Authority does not share information with other accountability bodies because of the secrecy provisions that govern its investigations. However, to avoid duplication of effort, the Authority does communicate on a general level with other bodies.

5.3.2 Inspector-General of Intelligence and Security

5.3.2.1 Jurisdiction

New Zealand's two intelligence agencies, the NZSIS and the GCSB, are reviewed by the Inspector-General of Intelligence and Security, whose jurisdiction is confined to these two bodies.

5.3.2.2 Mandate

The IGIS's mandate is to:

> assist each Minister who is responsible for an intelligence and security agency in the oversight and review of that intelligence and security agency and . . . in particular,
> (a) Assist the Minister to ensure that the activities of that intelligence and security agency comply with the law; and
> (b) Ensure that complaints relating to that intelligence and security agency are independently investigated.[298]

5.3.2.3 Functions

The IGIS carries out this mandate through five prescribed functions:

(i) complaint investigation;
(ii) investigation on the IGIS's own motion, with notification to the Minister, or at the Minister's request, into compliance with the law by the agencies;
(iii) inquiry at the Minister's request or on the IGIS's own motion, subject to the Minister's concurrence, into the propriety of particular activities of an agency where there has been adverse effect on any New Zealand person by an agency;
(iv) review of the effectiveness and appropriateness of the procedures adopted by the NZSIS to ensure compliance with legal requirements for interception warrants; and

(v) preparation and execution of programs for the "oversight and review" of the agencies, provided the Minister approves them.[299]

The IGIS is prohibited from inquiring into any action taken by the Minister[300] and "[e]xcept to the extent strictly necessary for the performance of his or her functions . . . into any matter that is operationally sensitive, including any matter that relates to intelligence collection and production methods or sources of information."[301]

5.3.2.4
Powers

The IGIS can compel documents and testimony,[302] and may receive evidence otherwise inadmissible in a court of law.[303] He or she has power of entry onto agency premises, with notice to the head of the agency.[304] The IGIS has access to all security records relevant to an investigation[305] except where the Minister certifies that disclosure would prejudice certain interests and that disclosure should not be made or should be limited.[306]

5.3.2.5
Reporting

The Inspector-General of Intelligence and Security cannot make binding orders. Upon concluding an investigation, he or she prepares a report with conclusions and recommendations for the Minister and the chief executive of the relevant agency.[307] In the case of a complaint, the IGIS also advises the complainant of his or her conclusions "in terms that will not prejudice the security or defence of New Zealand" or its international relations.[308] The IGIS may report to the Minister on an agency's compliance with recommendations, and on the adequacy of any post-inquiry remedial or preventative measures.[309]

The IGIS also submits an annual report to the responsible minister and the Prime Minister (who are traditionally one and the same).[310] The Prime Minister tables a version of this report in the House. Certain material may be excluded after consultation with the IGIS.[311]

5.3.2.6
Appointment

The IGIS is appointed by the Governor-General on the recommendation of the Prime Minister, after consultation with the Leader of the Opposition.[312] The appointee must be a retired judge of the High Court of New Zealand.[313] The term of appointment is three years, with reappointment permitted.[314]

6. NORWAY

6.1 OVERVIEW

Norway is a constitutional monarchy with a parliamentary system of governance. Power is divided among three branches: legislative, executive and judicial. The legislative branch, the Parliament, consists of a lower chamber and an upper chamber. The executive branch consists of the monarch, the Prime Minister and the Cabinet.[315]

As Norway is a unitary state, policing, security and intelligence responsibilities fall to the national government. There is a national police force; a Police Security Service with a separate statutory basis; and two security intelligence agencies, the Intelligence Service and the National Security Authority. [316]

The national police force and the Police Security Service are subject to a new external complaint-based review body called the Special Unit for Police Matters. The Police Security Service and the two security intelligence agencies are subject to the same complaint-based and review-based review body: the Norwegian Parliamentary Intelligence Oversight Committee (EOS Committee).[317]

The Norwegian government has undertaken several national security measures in recent years. These include appointing the Commission on the Vulnerability of Society to report on measures to increase security and safety,[318] and establishing the Directorate of National Protection[319] and, in 2002, the Centre for Information Security.[320]

6.2 LAW ENFORCEMENT AND INTELLIGENCE

6.2.1 National Police Force

Norway has only one police force: the Norwegian Police.[321] The force is established pursuant to the *Police Act*.[322]

There are 27 local police districts, each with a chief of police.[323] There are also five central police institutions, including the National Criminal Investigation Service, which assists the local police with technical and tactical expertise; and the Police Security Service.

Norway's ordinary police force does some national security policing inasmuch as certain divisions, such as the economics crime unit, are mandated to

investigate matters including terrorism-financing and other investigations related to national security. However, it is the Police Security Service that is charged with investigating matters involving classified material.[324]

6.2.2
Police Security Service

The Police Security Service is an agency within the national police force that has had a separate statutory basis since 2002.[325] The establishment of a statutory basis for the Police Security Service, as well as other reorganization in Norway's security intelligence and review landscape, followed a report by the Lund Commission. The Commission was established in 1994 to "inquire into all allegations of illegal or irregular surveillance of Norwegian citizens, by any of the intelligence and security agencies, from 1945 until the present."[326]

The Police Security Service is tasked with "preventing terrorism, espionage and threats to internal security."[327] It is considered one of Norway's three intelligence agencies and in recent years has been subject to the greatest degree of scrutiny by Norway's monitoring committee for intelligence agencies.[328]

6.2.3
Intelligence Service

The Intelligence Service gathers and analyzes foreign intelligence — principally signals intelligence.[329] According to its 1998 governing legislation, it is mandated to "procure, process and analyse information regarding Norwegian interests viewed in relation to foreign states, organizations or private individuals, and in this context [prepare] threat analyses and intelligence assessments to the extent that this may help to safeguard important national interests."[330] This mandate includes the "procurement of information concerning international terrorism."[331] The Service's governing statute also sets limitations on its powers, including a prohibition on monitoring or otherwise covertly procuring information on Norwegian territory, concerning Norwegian individuals or entities.[332]

The Intelligence Service is organized as part of Norway's armed forces.[333] It was formerly a military agency, but today its staff is mostly civilian.[334]

6.2.4
National Security Authority

According to its governing legislation, the National Security Authority (NSA) "coordinate[s] protective security measures and oversee[s] [Norway's] state of security." It is also "the executive body in relation to other countries and international organizations."[335] In other words, the NSA is responsible for proactive national

security, identifying national objects of special interest, and reducing Norway's vulnerability to internal and external threats.[336] It is also the highest authority in Norway for issuing and withdrawing personnel security clearances, classifiying and de-classifying information, and physically and electronically securing governmental and other sensitive premises against espionage.[337] The NSA does not conduct investigations or operations,[338] but has "unhampered access to any area where there is sensitive information or a sensitive object."[339] Established by legislation in 2001,[340] it replaced the former military Defence Security Service and is organized as a civilian directorate within the Ministry of Defence.[341]

The Norwegian government also has the Coordinating and Advisory Committee for the Intelligence, Surveillance and Security Services, which coordinates and advises responsible ministers on information exchange between Norway's three intelligence bodies.[342] The Committee consists of the three agency heads, and three high-ranking ministry officials.[343]

6.3 REVIEW AND OVERSIGHT

6.3.1 Complaints Against the Police

Complaints against Norway's police, including the Police Security Service, are investigated by a new complaint-based body that is external to the police: the Special Unit for Police Matters. The Special Unit does not conduct regular reviews, and does not play a major role in handling complaints about the Police Security Service.

Until January 1, 2005, complaints were investigated by the Special Investigating Body for Police Matters (known as SEFO), which was internal to the police. SEFO's principal mandate is to investigate whether police employees have committed a criminal act, thus establishing a high threshold for beginning an investigation.

The Norwegian Parliamentary Ombudsman for Public Administration has complementary jurisdiction to review complaints against the police, the immigration services and the customs administration.[344] The Parliamentary Ombudsman does not have jurisdiction to review any of the activities or agencies that fall within the EOS Committee's terms of reference, or the activities of the EOS Committee itself.[345]

6.3.2
Norwegian Parliamentary Intelligence Oversight Committee (EOS Committee)

6.3.2.1
Jurisdiction

Norway's intelligence agencies, including the Police Security Service, are subject to the review jurisdiction of the Parliamentary Intelligence Oversight Committee, otherwise known as the EOS Committee. The Committee is tasked with reviewing all "intelligence, surveillance and security services carried out by, under the control of, or on the authority of the public administration."[346]

This provision is interpreted as meaning that the purpose of the intelligence, surveillance and security activity must be to safeguard national security interests. Activities with different objectives, such as traffic surveillance or criminal intelligence are not included. In other words, the jurisdiction of the Intelligence Oversight Committee is defined functionally, rather than by agency.[347]

The EOS Committee also advises that to date, this function-based definition of jurisdiction has been interpreted as extending its authority only to the Intelligence Service, the National Security Authority and the Police Security Service. However, the functional definition of the Committee's jurisdiction is intended to capture any other public or private entity that might engage in such security or surveillance activity, including by statutory or organizational change, or by informal arrangement or contract.

The Committee noted that in an era of increased integration among public authorities engaged in counter-terrorism, new questions are arising about whether it should be monitoring certain activities of other bodies, including the ordinary police force, which often carries out counter-terrorism investigations with the help of the Police Security Service; and immigration and customs authorities.[348] These issues have not yet been formally tested. However, in its 2003 annual report the EOS Committee discussed whether its review jurisdiction could or should extend to the economic crimes unit of Norway's ordinary police force — the principal investigator of terrorism-financing cases — rather than the Police Security Service.[349] To clarify matters being investigated within its functionally defined mandate, the EOS Committee also has the power to investigate issues outside that mandate.[350]

The EOS Committee finds several advantages in its multi-agency jurisdiction. These include:

- insight into and knowledge of the entire security intelligence area, allowing for better assessment of complaints;
- the ability to verify one agency's statements about the role that another agency might have played;
- the ability to monitor communications and co-operation between the services; and
- the avoidance of disputes as to whether the Committee properly has jurisdiction.

An overlap of jurisdiction exists between the EOS Committee and the body responsible for complaints against the police force,[351] whether these complaints are made against ordinary police officers or the Police Security Service. Due to the overlap, the Director General of Public Prosecutions has issued guidelines to the complaint-based body to advise the EOS Committee of any allegations against the Police Security Service, investigations and recommendations, and any matters that may be of interest to it. The Committee has a more limited reciprocal duty to inform of any findings that indicate activity that might fall within the complaint-based body's jurisdiction. Given such overlap in jurisdiction, the EOS Committee maintains that such co-operation and communication are essential to fulfill the two bodies' respective mandates.

The Committee added that if it received a complaint against the ordinary police that appeared to deal with EOS-related questions, it would investigate the complaint. It has already had occasion to ask the Police Security Service to provide information from the ordinary police. However, the Committee has also encountered problems in following the course of an investigation, including information-sharing activity, between the Police Security Service and sections of the ordinary police such as the economic crimes unit, since it is commonly held that it does not have jurisdiction over the latter.[352]

6.3.2.2
Mandate

The EOS Committee is mandated to:

1. ascertain and prevent any exercise of injustice against any person, and ensure that the means of intervention employed do not exceed those required under the circumstances,
2. ensure that the activities do not involve undue damage to civic life, [and]

3. ensure that the activities are kept within the framework of statute law, administrative or military directive and non-statutory law.[353]

The Committee also has a more particularized mandate for each agency within its purview:

(a) For the intelligence service: to ensure that activities are held within the framework of the service's established responsibilities, and that no injustice is done to any person.
(b) For the security service: to ensure that activities are held within the framework of the service's established responsibilities; monitor clearance matters in relation to persons and enterprises for which clearance is advised against by the security staff, or refused or revoked by the clearance authority; and ensure that no injustice is done to any person.
(c) For the surveillance service: to monitor surveillance matters, operations and measures for combating terrorist activities by means of electronic surveillance and mail surveillance; and monitor to ensure that the collection, processing, registering and filing of information concerning Norwegian residents and organizations is carried out in accordance with current regulations, and meets the requirements for satisfactory routines within the framework of the purpose stated in section 2 of the Act.
(d) For all services: to ensure that the co-operation and exchange of information between the services is held within the framework of service needs.[354]

In carrying out its mandate, the Committee is bound to "show consideration for national security and relations with foreign powers."[355]

6.3.2.3
Functions

The EOS Committee carries out its mandate through three principal functions: investigations of complaints; self-initiated reviews; and investigations, on its own initiative, into "matters and factors that it finds appropriate to its purpose, and particularly matters that have been subjected to public criticism."[356]

The EOS Committee finds advantages both to combining and to separating the two functions of complaint-processing and self-initiated reviews. On the one hand, combining the two functions allows for improved monitoring and resource efficiency and decreased risks of proliferating classified documents, inasmuch as one body, rather than two, is carrying out the complaint-handling and self-initiated review functions. On the other hand, as noted above in the discussion of Australia's Commonwealth Ombudsman, an agency that performs regular

self-initiated reviews of the intelligence agencies' files can become too close to their decision making and operations to independently examine complaints, in which case separating the two functions might be desirable. However, the Committee noted that precautions can be taken to avoid such "capture." These include not advising before operations are undertaken and not giving input on procedures or policies. Indeed, the EOS Committee is prohibited from such activities by its governing statute, and believes, as did the legislator, that this is an important safeguard of independence. Specifically, the EOS Committee's governing statute prohibits it from "instruct[ing]" the agencies, and from "be[ing] used by these for consultations."[357] According to one commentator, this prohibition on consultations was set out in the statute to preclude the possibility of the Committee exercising ongoing oversight of the agencies, and thereby compromising "the need for critical independence."[358]

6.3.2.4
Powers

The EOS Committee has the power to compel documents and testimony, including from the ordinary police force, other parts of the public administration, and the private sector.[359] Indeed, the Committee can carry out investigations with these other bodies, as long as the investigation is to further an investigation within its jurisdiction.[360]

The Committee does not have access to the ministries' "internal documents."[361] The Committee chair also recently stated that the Committee does not ask for access to files that relate to the identity of sources/agents or that reveal the capacities of foreign co-operating services.[362] This derives in part from the Committee's statutory obligation to "show consideration for national security and relations with foreign powers."[363]

The EOS Committee also has communications links with SEFO and its successor, the Special Unit for Police Matters.

Upon concluding an investigation or self-initiated review, the Committee makes findings and recommendations. It does not make binding orders.[364]

6.3.2.5
Reporting

In the context of complaint investigations, the Committee is required to make statements to complainants that are as complete as possible without revealing classified information. These statements must also be sent to the head of the agency, and if the Committee finds "valid grounds for criticism or other

comments," to the ministry concerned.[365] Statements to complainants must be unclassified. The Committee may decide whether they should be made public.[366]

The Committee also files annual reports with the Parliament. These reports are unclassified,[367] unless in the Committee's view the Parliament "should familiarize itself with classified information."[368] The Committee may also file a special report where it finds that there are "factors" that should be made known to the Parliament immediately.[369]

6.3.2.6
Appointment and Composition

The Committee is composed of seven members, who are elected by the Norwegian Parliament for a five-year period.[370] Sitting members of the Parliament are not eligible, but "care is . . . taken to ensure that [the Committee appointees] reflect the main political interests represented in Parliament."[371] They must have the highest level of national security classification and are bound to a duty of secrecy.[372]

7.
SWEDEN

7.1
OVERVIEW

Sweden is a constitutional monarchy and parliamentary democracy. Power is divided among three branches: the legislative Parliament; the executive, which consists of the monarch, the Prime Minister and the Cabinet; and the judiciary.[373]

A unitary state, Sweden has one national police force, which includes the police security service known as Såpo. Sweden also has several security intelligence agencies. All of the law enforcement, security and intelligence agencies fall under the review jurisdiction of Sweden's Parliamentary Ombudsmen. The Office has complaint-based and self-initated review mandates, but for reasons that I discuss below, carries out only occasional scrutiny of these agencies.

In recent years, the Swedish government has taken a number of national security measures. It passed the *Act on Criminal Responsibility for Terrorist Crime*, which, among other things, created terrorism offences and increased the right to use secret surveillance,[374] and the *Act on Extradition from Sweden under the European Arrest Warrant*.[375] Both acts were based on European Union directives.[376] It also established a commission to review Sweden's emergency preparedness following 9/11,[377] created the Swedish Emergency Management

Agency[378] and allocated separate funds for "strengthening Swedish emergency preparedness."[379]

7.2 LAW ENFORCEMENT AND SECURITY INTELLIGENCE

7.2.1 National Police Service

Sweden's national police service comprises police authorities for each of the country's 21 counties, and includes the National Criminal Investigation Department, the National Counter-Terrorism Unit, the Security Service, and liaison officers in other countries.[380] The duties and powers of the police service are set out in statute.[381] The service has approximately 23,000 employees.[382]

7.2.2 Security Service

The Security Service's mandate is to "direct and perform police activities aiming at the prevention and detection of offences against national security, and also — even if activities do not refer to such offences — police activities relating to counter-terrorism . . . . "[383] The Security Service collects "security intelligence," as it "gathers intelligence on various matters that may be used to combat international terrorism or to counter threats to [Sweden's] democratic system and national security."[384]

The Security Service works closely with the "regular police service" to prevent crime. That is, "regular police units perform investigations and operational field work while the [Security Service] provides crime intelligence, resources and methodological know-how." The Service also works closely with government agencies within the "Swedish Total Defence System," and uses a "central register" for compiling the intelligence that it collects.[385]

The Security Service describes its "prime task" as "crime prevention," stating that "[t]o be able to prevent and detect crimes against national security, [it] must engage in security intelligence gathering . . . [meaning intelligence] that may be of importance to external and internal security and to counter-terrorism activities."[386] The Security Service's work includes intelligence processing, analysis and national security threat assessments.[387]

7.2.3
Military Intelligence and Security Service

Sweden's Military Intelligence and Security Service collects and analyzes intelligence related to foreign military threats to Swedish security. This body was first placed on a statutory basis in 2000[388] and operates under the armed forces.

7.2.4
National Defence Radio Centre

Sweden's National Defence Radio Centre (FRA)[389] carries out signals and communications intelligence, and operates under the armed forces. General instructions for the Radio Centre are set out in a statute. However, this statute does not explicitly define the Radio Centre's powers.[390]

7.2.5
Other

In addition to those bodies that gather intelligence, the Swedish Emergency Management Agency (SEMA), which was created in July 2002, uses "research and intelligence to compile knowledge" that might be "useful" to Swedish public authorities. SEMA is also charged with coordinating information security in Sweden. The National Defence Radio Centre assists SEMA by contributing expertise.[391]

7.3
REVIEW AND OVERSIGHT

7.3.1
Parliamentary Ombudsmen's Office

7.3.1.1
Jurisdiction

The Swedish police service and security services[392] are all subject to review by the Office of the Parliamentary Ombudsmen,[393] which has general jurisdiction over public authorities.[394]

The Ombudsmen's office divides its review responsibilities among its four elected Ombudsmen, according to the agency in question. The police force and the Security Service are the responsibility of the Chief Ombudsman, but the military-operated intelligence agencies are the responsibility of another Ombudsman, who also reviews the Customs authorities.[395] A third Ombudsman

reviews the immigration authorities and the administration of foreign affairs.[396] This Ombudsman recently completed an in-depth review of the propriety of the co-operation and interaction between police authorities and immigration authorities related to the arrest and deportation of a failed asylum-seeker.[397]

According to the Chief Ombudsman, such division of responsibility among the four Ombudsmen affords specialization and efficiency. The four Ombudsmen also meet regularly to share information and discuss cases, especially those involving two or more public authorities. Indeed, to give a more comprehensive picture for monitoring purposes, the office is considering more formalized joint, self-initiated reviews of public authorities whose work is integrated or interrelated. The Chief Ombudsman observed that in an increasingly complex public sector, being able to see a full picture and to share information is advantageous. On the other hand, he noted that intelligence agencies and police involved in national security activities need a form of dedicated review that allows for regular and specialized supervision, which the generalist ombudsman model does not provide.

7.3.1.2
Mandate

The Parliamentary Ombudsmen's mandate is to ensure that public authorities, including individuals employed by the civil service or local governments, or whose work otherwise involves the exercise of public authority, comply with the law and "fulfil their obligations in other respects."[398]

7.3.1.3
Functions

The Ombudsmen carry out their mandate by investigating complaints, conducting self-initiated reviews, and initiating "other inquiries as [they] may find necessary."[399] They also "contribute to remedying deficiencies in legislation" by making representations to the legislative or executive branches of government when an issue arises during the course of their review activities.[400] The Ombudsmen may choose to refer complaints to another authority if they are of the view that the complaint can be more appropriately investigated and appraised by that authority.[401] Indeed, the Chief Ombudsman advised that in most instances his Office is a complaint institution of complementary recourse.[402]

The Chief Ombudsman also noted that even though primary complaint investigation is frequently undertaken by other accountability bodies, the complaint-processing function consumes the majority of the Ombudsmen's resources.[403] As a result, the Office has little time for self-initiated reviews of the

public authorities within its purview. For example, it normally visits only three police locations each year, which means that there can be up to 25 years between self-initiated reviews of a particular public authority. In addition, in the last 15 years, the Office has conducted only two "own initiative" investigations into the police Security Service,[404] and in the last 20 years, no such investigations of Sweden's other intelligence agencies.

7.3.1.4
Powers

Under the Swedish constitution, the Ombudsmen have access to the minutes and documents of any public authority; and these institutions, as well as government officials, must provide Ombudsmen with the information requested.[405] This provision is interpreted as allowing the Ombudsmen to access any information or data, whether classified or not. The Ombudsmen choose which investigations and reviews they will undertake,[406] and may impose fines to secure information.[407]

The Parliamentary Ombudsmen have various remedial powers. For example, they can offer "opinions" about whether an action by a public official complied with the law,[408] or was otherwise erroneous or improper; offer "advisory statements"; act as special prosecutors and lay criminal charges against public officials;[409] and invoke disciplinary measures, such as salary deductions, suspensions and dismissals.[410]

7.3.1.5
Reporting

The Ombudmen's Office submits annual reports to the Parliamentary Committee on the Constitution, which then files its own written report and notifies the Parliament.[411] The Ombudsmen may also submit special reports to the Committee, but this power is generally used only to recommend changes to existing legislation. Reports and decisions on the merits of individual cases are immediately made public.

7.3.1.6
Appointment and Composition

The Ombudsmen are elected by the Parliament for renewable, four-year terms.[412] No prerequisite qualifications are set out in statute for election to the position of Ombudsman, but by tradition, Ombudsmen must be acceptable to all political parties in Parliament. Almost without exception, the Ombudsmen have formerly held high judicial offices, a practice that is intended to secure their in-

dependence and their competence to supervise the legality of the activities of public authorities.

7.3.2 Other Forms of Review

The National Defence Radio Centre is also subject to review and oversight by the Defence Intelligence Commission. The Commission consists of six persons, most of whom are or have been members of Parliament. It reports directly to the Swedish government. No corresponding review body exists on the civilian side, notably for the Security Service. There is currently a proposal to appoint a similar standing commission to supervise the use of secret coercive measures such as wire tapping by all relevant bodies, thus including the Security Service.

8. UNITED KINGDOM

8.1 OVERVIEW

The law enforcement and security intelligence landscape in the United Kingdom (U.K.) has undergone considerable change in recent years. A number of statutes have created new terrorism offences and given national security actors enhanced powers to investigate terrorism.[413] Many covert intelligence-collection activities have been placed under statutory regulation;[414] many police structures have been reformed;[415] an independent body has been established to investigate the police in Northern Ireland,[416] and a new review body for the police has been established for England and Wales.[417] The government has increased its national security funding, including its allotment to law enforcement and intelligence agencies engaged in counter-terrorism activities.[418] It is also monitoring the operation of certain of its counter-terrorism measures through "independent review,"[419] and promoting public discussion about the proper balance between national security and rights and freedoms.[420]

The United Kingdom does not have a national police force for general law enforcement.[421] Policing is generally carried out by local and specialized police forces in England, Wales, Scotland and Northern Ireland,[422] all of which have a Special Branch that focuses on covert intelligence work related to national security.[423] The U.K. has three principal security intelligence agencies: the Security Service (known as MI-5), the Secret Intelligence Service (known as MI-6) and the Government Communications Headquarters.

Notably, U.K. police forces are subject not only to complaint-based review bodies, but also to bodies with complaint-based and review jurisdiction over a set of covert investigative activities, no matter which public sector actor carries them out.[424] Thus, certain U.K. policing activities such as wiretaps and other surveillance activities are subject to review and complaint-based review because of their covert nature, regardless of the type of investigation.

8.2 LAW ENFORCEMENT AND INTELLIGENCE

As I stated above, the U.K. does not have a national police force for general law enforcement. In England and Wales, there are 43 local police forces;[425] in Northern Ireland, there is one general police agency, the Police Service for Northern Ireland, and several specialized or local police agencies;[426] and in Scotland, there are eight police forces.[427] The U.K. also has several national forces with specific mandates.[428] The mandate of the U.K.'s local forces therefore necessarily includes national security law enforcement, although the scope and structure of their national security activities varies depending on the local circumstance.[429]

8.2.1 Metropolitan Police Service

The Metropolitan Police Service, which polices the greater London area, plays the leading role in counter-terrorism investigation by U.K. police. The Commander of the Metropolitan's Anti-Terrorist Branch is the national coordinator for the investigation of acts of terrorism. The Branch investigates acts of terrorism both within its defined policing area and, in conjunction with local forces, throughout the U.K.[430]

8.2.2 Special Branch

The Metropolitan Police Service includes a section — comprised of several hundred members — known as the Special Branch.[431] Other police forces in the U.K. also have their own Special Branches.[432] According to March 2004 Guidelines issued by the Home Office, the "primary function" of Special Branch is "covert intelligence work in relation to national security."[433] The Special Branch is also "available" to local police forces to deploy on duties that include "the prevention and detection of crime and the ensuring of public safety," but the Special Branch "should not be diverted" from its primary function "unless absolutely necessary."[434] "[C]ounter terrorist work . . . is currently the main focus

of their activity."[435] The Special Branch "assist[s]" and "supports" the intelligence-collection efforts of the U.K.'s security intelligence agencies, in particular the Security Service (described below) with which it often works in "close co-operation."[436] The Special Branch is staffed by police officers and by civilians.[437]

8.2.3 Police Service of Northern Ireland

The Police Service of Northern Ireland, formerly the Royal Ulster Constabulary (RUC), was created in 2001 as a result of recommendations by the Independent Commission on Policing in Northern Ireland.[438] For many years the PSNI/RUC Special Branch carried out anti-terrorism investigations in policing the conflict between unionist (Protestant) and republican (Catholic) paramilitaries in Ireland.[439] The Special Branch has now been restructured within PSNI Crime Operations Department as an intelligence-gathering group.

8.2.4 Serious Organised Crime Agency

The Serious Organised Crime Agency (SOCA) is "an intelligence-led agency with law enforcement powers."[440] It was created by statute in 2005 and began operating on April 1, 2006.[441] SOCA merges the National Crime Squad (NCS), the National Criminal Intelligence Service (NCIS), the investigation branch of the U.K. Immigration Service that deals with organized immigration crime, and the investigative branch of HMRC that deals with drug trafficking and associated criminal finance.[442] It has a mandate to prevent and detect serious organized crime; to gather, analyze, store and disseminate information on crime; and to provide support to law enforcement partners, particularly U.K. police forces and Her Majesty's Revenue and Customs (HMRC).[443] SOCA has taken over the NCIS' role as the U.K.'s financial intelligence unit, and therefore works to combat terrorist financing and money laundering.[444]

The Agency is divided into four directorates: intelligence, which gathers and assesses information; enforcement, which builds criminal cases and provides operational responses to threats; intervention, which focuses on confiscating criminal assets and working with the private sector; and corporate services, which supports SOCA's other functions.[445] Although its agents have police-type powers,[446] including being able to covertly collect information, SOCA is a civilian agency.[447] It operates in close to fifty locations throughout the United Kingdom and maintains liaison officers in various foreign countries.[448] SOCA anticipates having approximately 4,200 full-time staff in 2006–2007.[449]

The U.K. has three principal intelligence agencies: the Security Service, the Secret Intelligence Service and the Government Communications Headquarters. The Defence Intelligence Staff, which is a part of the Ministry of Defence, also contributes security intelligence.

8.2.5 MI-5

The Security Service,[450] also known as MI-5, is responsible for domestic security intelligence. According to its governing statutes, the Security Service's functions are "the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means"; the safeguarding of "the [U.K.'s] economic well-being"; and "support of the activities of police forces and other law enforcement agencies in the prevention and detection of serious crime."[451] MI-5's principal means of gathering intelligence are covert human intelligence sources, directed surveillance, interception of communications and intrusive surveillance.[452] The governing statutes contain several limitations on MI-5's activities, such as the prohibition on its obtaining information that exceeds its mandate.[453] MI-5 has no police powers such as arrest or detention.[454]

8.2.6 MI-6

The Secret Intelligence Service,[455] also known as MI-6, is responsible for foreign intelligence. Specifically, its functions are to "obtain and provide information relating to the actions or intentions of persons outside the British Islands; and to perform other tasks relating to the actions or intentions of such persons," but only "in the interests of national security, with particular reference to the defence and foreign policies of [the government]; in the interests of the economic well-being of the [U.K.]; or in support of the prevention or detection of serious crime."[456] Like MI-5, the functions, powers and limitations on powers of MI-6 are set out in its governing statute.[457] Also like MI-5, MI-6 has no police powers.

8.2.7 Government Communications Headquarters and Defence Intelligence Staff

The Government Communications Headquarters (GCHQ)[458] carries out signals intelligence, in the same interests as MI-6 — national security, national

economic well-being, and prevention or detection of serious crime.[459] The GCHQ's activities and powers are governed by the same statute as those of MI-6.[460]

The Defence Intelligence Staff collect and analyze intelligence generally in support of the Ministry of Defence, military commands and deployed armed forces.[461]

8.3
REVIEW AND OVERSIGHT

The U.K. review landscape differs in England and Wales, Northern Ireland and Scotland. The 43 local police forces of England and Wales, as well as the U.K.'s specialized police services with national reach, are subject to the Independent Police Complaints Commission (IPCC). The Police Service of Northern Ireland is subject to the jurisdiction of the Police Ombudsman for Northern Ireland. Complaints against the eight Scottish police forces are currently handled by the police,[462] but a multi-agency and public study of the government's proposal to establish "an independent complaints body" is underway.[463] I give further details of my examination of the IPCC and the Office of the Police Ombudsman for Northern Ireland below.

Police services in the U.K. are also subject to the jurisdiction of Her Majesty's Inspectorates of Constabulary, inspection services that report to the responsible minister on the effectiveness and efficiency of the police forces. Since these inspectorates are a part of the executive branch, and not "independent arm's length" agencies, I have not discussed them in detail. However, they formed part of my examination largely because they appear to have a substantive role in scrutinizing police activities and policies, including counter-terrorism activities. I set out my observations of these inspectorates, as well as the sources I consulted, in the Commission's Background Paper and Supplementary Background Paper on International Models, and I would refer the reader to those papers for more information.

Police services in the U.K., as well as the intelligence services and numerous other public authorities, are also subject to review by the bodies created by the *Regulation of Investigatory Powers Act* [*RIPA*], a statute that regulates the use of certain covert investigative methods, no matter which public authority is carrying them out. I have discussed these review bodies in detail below.

Finally, the intelligence services are subject to the Intelligence Services Commissioner, a body that is dedicated to reviewing only certain of their activities. This body is also established by the *Regulation of Investigatory Powers Act*, and I also briefly discuss it below.

8.3.1 Independent Police Complaints Commission

8.3.1.1 Jurisdiction

All local police forces in England and Wales, as well as the specialized police forces with national scope, are subject to the jurisdiction of the new Independent Police Complaints Commission (IPCC) that was established on April 1, 2004.[464] The IPCC also has jurisdiction over the enforcement activities of the Customs service (HMRC)[465] as well as complaint-based jurisdiction over all aspects of SOCA's activities, including its role as the U.K.'s financial intelligence unit. A recent government bill will add immigration enforcement complaints to the IPCC's jurisdiction.[466]

The IPCC's jurisdiction is therefore quite broad, includes diverse law enforcement and accompanying intelligence activities, and comprises many forces whose activities are integrated. The IPCC advised that it is too early in its existence to comment on whether there are advantages to its ability to observe such integrated activities.

The IPCC's role includes reviewing complaints, but it has a broader scope as well. Law enforcement agencies have a duty to refer serious incidents, injuries and deaths to the IPCC, even where there is no complaint or indication of misconduct. Finally serious allegations of misconduct not involving complaints also have to be referred. It is then up to the IPCC to decide how these will be investigated, including the possibility that the IPCC will itself investigate.

With respect to immigration enforcement, the IPCC's jurisdiction will be directed primarily at reviewing complaints about arrest and detention in the context of arrest. The IPCC's terms of reference are also expected to extend to handling complaints concerning powers of entry, powers of search and seizure, powers to examine and otherwise obtain information or personal data, and powers related to removing persons from the United Kingdom.[467] Similarly, the IPCC has jurisdiction over the arrest and short-term detention powers of Customs officials. Again, the IPCC's jurisdiction is focused on the exercise of police-type powers; its terms of reference do not extend, for example, to taxpayer complaints about HMRC's Inland Revenue functions.[468] Both HMRC and the Immigration Service enforcement branch have intelligence capabilities, and the IPCC has the power to review intelligence activities in the context of an investigation into the use of enforcement powers. With respect to both agencies, the

IPCC will focus on investigations regarding potential incidents of gross or criminal misconduct.

The IPCC's jurisdiction over all police forces and other authorities in England and Wales is independent of whether or not such bodies are engaged in national security investigations.[469] Indeed, the police forces have agreed to refer to the IPCC any complaints they receive about the use of their counter-terrorism powers.[470] The IPCC has a number of people with the requisite security clearance to access and review national security information, and it has proper storage and viewing facilities.

Overlapping Jurisdiction: Co-operation With Other Accountability Bodies

The IPCC's jurisdiction overlaps with a number of other public authorities, including access-to-information and human rights authorities, and numerous commissions and ombudsmen. Where a matter or course of conduct that has been called into question has involved more than just police forces, the IPCC has sometimes engaged in joint investigations with other accountability bodies. For example, it has worked with the Prisons and Probation Ombudsman and the Healthcare Commission on certain matters. A "statutory gateway"[471] was also recently created to allow for information exchange and co-operation between the IPCC and the Parliamentary Ombudsman, both of which have review jurisdiction over certain aspects of the new Revenue and Customs department.[472] That is, the IPCC and the Parliamentary Ombudsman "may disclose information to each other for the purposes of the exercise of" their respective mandates, and "may jointly investigate" certain matters.[473] A similar statutory gateway has been proposed to allow the Parliamentary Ombudsman and the IPCC to disclose information to one another and where necessary conduct joint investigations related to immigration enforcement complaints.[474]

Statutory gateways have been devised in the U.K. to address overlapping jurisdiction, the potential for duplication and the diminished observation and accountability that can result when multiple review bodies have "silo" vision. Among other things, statutory gateways allow "data sharing" between public bodies, and the Department for Constitutional Affairs has published guidance on the applicable laws, and the protocols that various bodies can establish.[475] Data sharing can include national security information, provided applicable rules are respected.

8.3.1.2
Mandate

The IPCC is charged with securing and maintaining a "suitable" system for handling complaints made about police conduct. This mandate includes securing "public confidence" in the system.[476] The IPCC is also charged with making recommendations about "police practice" that appear "necessary or desirable," and with specifically "recording" (i.e., investigating) police conduct that may have involved committing a criminal offence or that may justify disciplinary proceedings.[477]

8.3.1.3
Functions

This mandate is carried out through the IPCC's complaint-handling and complaint-monitoring functions, as well as its authority to "record" or "call in" matters for investigation in certain circumstances.[478] The IPCC also has the authority to issue "guidance" to police forces regarding its handling of complaints and recordable conduct, and its detection or deterrence of misconduct by police persons.[479]

The IPCC advises that it does not investigate or review 95 percent of the complaints filed concerning police activity. Rather, these complaints are filed with, referred to and/or investigated by the police and/or the respective Police Authority.[480] However, the IPCC retains the right to supervise or manage an investigation, or to conduct the investigation itself. Complainants may also appeal investigation results to the IPCC.[481]

The IPCC's investigations often intersect with or parallel police investigations, including national security investigations. While there are practical issues to address, such as access to evidence that both bodies require, so far each body involved has been able to carry out its own mandate without interfering in the other's. Statutory guidance was recently issued to help determine when the IPCC or the police should suspend complaint-investigations because of a risk of prejudice to a proceeding.[482] Complaint investigations may be postponed, for example, when the issues at the centre of the complaint are similar or identical to the issues before a court in a criminal proceeding.[483]

The IPCC has a duty to disclose all relevant material to the Crown Prosecution Service,[484] which in turn must disclose the material to the defence if it proceeds with a prosecution.[485] Where the IPCC has not conducted an investigation leading to the criminal proceeding, however, it does not have any automatic disclosure obligations.[486] The Crown Prosecution Service may seek a

court order requiring the IPCC to produce documents[487] where the Crown reasonably believes that the material may undermine the prosecution case or assist the case for the accused.[488] The Crown may choose not to seek third-party disclosure of sensitive information, however, if the public interest would justify withholding the information.[489] To date, the IPCC has granted the Crown Prosecution Service access to such material, but the Crown has not sought court-ordered disclosure. To preserve its independent position, the IPCC likely would require a Court order before making disclosure and might resist on the basis of public interest principles.

8.3.1.4
Powers

The IPCC is entitled by statute to access any information in the possession of the police,[490] and has powers of entry, search and seizure in relation to police premises.[491] Once a complaint is made or a conduct matter comes to notice, the affected police authority has a legal duty to secure all relevant evidence.[492] Police authorities and forces must turn over documents to the IPCC at "the earliest time at which it is practicable," and they may decline to do so "at all in a case in which it never becomes practicable."[493] The IPCC advises that this provision has not yet been tested, and that it has thus far received all documentation that it has requested.

To date, the IPCC has not had difficulty accessing information that it required on national security files, including information subject to third-party caveat. However, in practice, it has yet to require access to information that a third party did not want released. The IPCC investigation has also conducted investigations into "highly sensitive" police corruption allegations in which the police expressed concern that the sensitive information and investigation be handled appropriately, but did not object to its disclosure or use. The IPCC can interview individuals and collect evidence from other government agencies and private individuals. While the IPCC can demand any information or documents from police and other agencies subject to its jurisdiction, it cannot compel documents from agencies outside of its jurisdiction. However, its investigators have all the powers of police officers. Therefore, if an IPCC investigation involves a criminal aspect, then those investigators could obtain search warrants to seek any necessary evidence.

The IPCC does not have the power to make binding conclusions; it can only recommend the appropriate discipline or other action that should be taken.[494] It is also obliged to notify the Director of Public Prosecutions when an investigation report indicates that a criminal offence may have been committed.[495]

8.3.1.5
Reporting

The IPCC files annual reports with the Secretary of State, as well as reports containing advice and recommendations, and such other reports as the IPCC considers appropriate on matters that it believes "should be drawn to [the Secretary of State's] attention by reason of their gravity or of other exceptional circumstances." Annual reports are laid before Parliament, and other reports are laid before Parliament if the Secretary of State "considers it appropriate to do so." Copies of annual reports are also provided to the police forces and police authorities; and copies of other reports are provided to relevant chiefs and authorities.[496]

Copies of complaint-investigation reports must be delivered to the relevant chief police officer and police authority.[497] The IPCC also has a duty to keep certain persons, including complainants, "properly informed" about the handling of a complaint or recordable conduct matter.[498] It has a duty to advise such persons about the findings of an investigation report, including any recommendations and any action taken by a police authority as a result.[499] These duties are subject to Secretary of State regulations precluding disclosure of information on various grounds, including national security, the prevention or detection of crime, the premature or inappropriate disclosure of information relevant to prospective criminal proceedings and public-interest necessity.[500]

8.3.1.6
Appointment and Composition

The IPCC consists of "a chairman appointed by Her Majesty," and not fewer than ten other members appointed by the Secretary of State[501] as either part-time or full-time members.[502] IPCC's members cannot be police officers or former officers.[503] The chair and the members are appointed for a term of up to five years, and are eligible for re-appointment.[504] There are no statutory prerequisite qualifications for appointment.

8.3.2
Police Ombudsman for Northern Ireland

8.3.2.1
Jurisdiction

The Police Ombudsman for Northern Ireland has jurisdiction over police forces in Northern Ireland, including the Police Service for Northern Ireland (PSNI)

and several other local or specialized police forces.[505] The Police Ombudsman will also shortly have jurisdiction in Northern Ireland over certain aspects of Her Majesty's Revenue and Customs department,[506] and the Serious Organised Crime Agency (SOCA — described above in section 8.2.4). The Ombudsman will also have jurisdiction over criminal and other serious allegations against the Immigration Service.

The Ombudsman's jurisdiction therefore includes the PSNI's counter-terrorism activities. The Ombudsman observed that in her experience, there is little distinction in Northern Ireland between national security law enforcement and other law enforcement, and suggested that it would be difficult to draw a line between them for review purposes. In the Northern Ireland experience, terrorist groups carry out all manner of ordinary crimes — fuel smuggling, bank robberies, cigarette smuggling, drug smuggling and petty crimes, for example — the proceeds of which are often used to fund terrorism. Investigations routinely involve several sections of the police force, including the counter-terrorism section. The counter-terrorism section (previously the Special Branch) had and continues to have no investigation function. Investigations are carried out by the PSNI's criminal investigations department.

8.3.2.2
Mandate

The Police Ombudsman for Northern Ireland is mandated to investigate matters of police conduct that are the subject of a public complaint, and/or that may have involved the commission of a criminal offence or may justify disciplinary proceedings, and/or may be in the public interest to investigate.[507] The Ombudsman is also required to investigate matters referred to her by the Secretary of State, the Northern Ireland Policing Board and the Director of the Public Prosecution Service. She can also investigate matters because she considers it in the public interest to do so. The Ombudsman is not permitted to investigate complaints relating to the "direction and control" of police forces,[508] but can investigate a "current practice or policy of the police" if she has reason to believe that it would be in the public interest to do so.[509]

8.3.2.3
Functions

Complaints

The Ombudsman's office carries out primarily a complaint-handling and criminal- and disciplinary-investigation function. The Ombudsman has the statutory

power to refer a complaint to the Chief Constable of the relevant police force.[510] If the Ombudsman refers a complaint to the police for investigation, she may supervise such investigation and approve the person charged with carrying it out.[511] However, the Ombudsman has made a policy decision that no complaints will be referred back to the police for investigation, and hence the Ombudsman's office, rather than the PSNI, investigates all complaints requiring investigation.

The Ombudsman's office advises that it frequently investigates PSNI conduct concurrently with the PSNI's criminal investigations, including terrorism investigations, into the same or related events. At times, the Ombudsman's office and the PSNI both require access to the same evidence, and must negotiate such access as the investigations run parallel. On occasion the Ombudsman has taken primacy of an alleged crime scene.[512] The Ombudsman also conducts independent investigations where there is an allegation of police officer involvement in terrorism.

While investigations may run parallel, the Ombudsman's office does not generally comment on the investigation while it is still active, but only after the fact. If a prosecution is ongoing during the Ombudsman's investigation, the Ombudsman's office will generally consult with the Director of Public Prosecutions regarding any potential impact, and where necessary, will delay publication of the investigation findings.

If the Ombudsman's office finds potentially exculpatory evidence during its investigation, its practice is to disclose it.[513] The question of whether the Ombudsman would disclose potentially exculpatory, but "classified" evidence recently arose. The Ombudsman dealt with the matter as required by law, which involved making a disclosure application to a judge separate from the judge who would preside over the criminal prosecution.

The Ombudsman's office also has a duty to provide the police with information it has that indicates that a person may have committed an arrestable offence, if the information is likely to secure the arrest or conviction of a person.[514] The Ombudsman's office interprets this obligation strictly; to do otherwise would undermine public confidence in the Office, since its role is not to assist the prosecution of its complainants.

Matters may also be referred to the Ombudsman by the Secretary of State, the Northern Ireland Policing Board (the equivalent of the police authorities in England and Wales) or the Chief Constable of the police, if any of these authorities believe it is in the public interest to do so.[515] Similarly, the Ombudsman may "of his own motion" investigate certain matters.[516]

The PSNI has consulted the Ombudsman on guidelines and policies, and the Ombudsman has provided advice in these circumstances. In the

Ombudsman's view, such measures can help avoid questionable activity or complaints later, and are thus worthwhile.

8.3.2.4
Powers

The governing statute for the Office of the Ombudsman does not restrict the Ombudsman's access to documents and information from the PSNI and the Policing Board. It states that they must provide "such information and documents as the Ombudsman may require."[517] The Ombudsman advised that she therefore has access to caveated information provided to the PSNI by third parties, including foreign agencies. However, the Ombudsman can not compel information agencies or persons other than the PSNI and the Policing Board. This issue has been raised in the context of PSNI activities integrated with other domestic agencies, including the armed forces. There has been some discussion of whether the Ombudsman should have access to information from those other bodies to fulfill its mandate.[518]

The Ombudsman also has all the powers of a police officer, including the powers of search, seizure and arrest,[519] and has used the arrest power on several occasions.

Following her investigations, the Ombudsman may refer a matter, with recommendations, to the Director of Public Prosecutions for Northern Ireland when she believes a criminal offence may have been committed. The Ombudsman may also refer a matter to the "appropriate disciplinary authority," with reasons and recommendations, when she believes that disciplinary proceedings should be brought. The Ombudsman may also direct the Chief Constable to bring disciplinary proceedings. This is the only binding remedial power of the Ombudsman's office.

8.3.2.5
Reporting

The Ombudsman submits annual and five-year reports to the Secretary of State, who lays such reports before both Houses of Parliament. The Ombudsman also reports to the Secretary of State on matters the Secretary of State may request or on matters the Ombudsman may determine to be of public interest. These reports must also be laid before both Houses of Parliament. Copies of all such reports are also provided to the Policing Board and the Chief of the PSNI.[520] The Ombudsman must report to the Secretary of State, the Northern Ireland Policing Board and the Chief Constable on any matter that those bodies have referred or that she has "called in" for investigation.

Although there is no statutory obligation to report on a matter to a complainant, the Ombudsman may publish statements on any actions or decisions her office has taken, including the reasons for such actions or decisions.[521] All complainants receive a reasoned letter explaining the outcome of any investigation of the complaint that the complainant has made.

The Ombudsman also must report to the Chief of the PSNI and to the Police Board, and in some circumstances to the Secretary of State for Northern Ireland, on any matters concerning police practices and policies that she has investigated.[522]

8.3.2.6
Appointment and Composition

The Ombudsman is "appointed by Her Majesty" to serve on a part-time or full-time basis for a period of seven years, or for a period ending on the date on which the person turns 70, whichever is shorter.[523] There are no statutory prerequisite qualifications for appointment and no eligibility for reappointment.[524]

8.3.3
RIPA Authorities

8.3.3.1
Jurisdiction

In 2000, the U.K. passed the *Regulation of Investigatory Powers Act* (*RIPA*). The Act sought to regulate and review the use by public authorities of certain covert investigative activities such as wiretaps, surveillance and use of human sources.[525] It allows for approval of such activities by persons other than judges, such as senior officials of the respective agencies or the Secretary of State, but requires review of certain aspects of the activities by a designated high court judge or former judge. It also provides a regime for handling public complaints about the prescribed activities.

The statute applies regardless of which public authority is carrying out the investigative activity, although it regulates certain authorities differently than others.[526] It applies no matter how the objective of the investigative activity is described, whether conventional law enforcement, national security law enforcement, criminal intelligence, security intelligence or regulatory enforcement, for example.

RIPA therefore establishes a function-based monitoring regime in which the use of certain investigative activities is variously regulated, depending on which agency carries out the activities; and in which investigative activities are

reviewed by corresponding review bodies. Generally stated, the review-body regime is as follows:

- Interceptions of communications are inspected by the Interception of Communications Commissioner (ICC), regardless of which of the approximately 100 authorized agencies conducted the actual interception.[527]
- Acquisitions and disclosures of data about the medium, location, time, etc. of communications — but not about the content — by more than 800 authorized agencies are reviewed by the ICC.[528]
- Covert-surveillance and human-source activities are inspected by the Chief Surveillance Commissioner. In some cases, these activities are approved prior to their use, either by the Surveillance Commissioners where law enforcement and other agencies carry them out, or by the Intelligence Services Commissioner (ISC) where the intelligence services carry them out.[529]
- Investigations of encrypted data will be inspected by the Office of Surveillance Commissioners (OSC), once that part of *RIPA* comes into force.[530]
- Complaints regarding any of these activities are investigated and adjudicated by the Investigatory Powers Tribunal (IPT).[531]

The Interception of Communications Commissioner stated that he saw an advantage in a function-based monitoring regime. It allowed him to develop an expertise in one particularized aspect of covert activity, and to avoid the risk of "capture" by any one agency because he inspected the activities of so many. He stated that this system worked largely because his review mandate was limited to a small number of activities, that is, he was not charged with comprehensive review of the numerous public agencies within his jurisdiction.[532]

8.3.3.2
Mandate and Functions

The *RIPA* authorities generally monitor compliance with the statute's conditions for authorization and use of the prescribed covert investigative activities, as they are expressly mandated to do by statute. That is, their respective mandates, with the exception of the Office of Surveillance Commissioners,[533] do not exceed the limited review activities — and in some cases approval activities — that are expressly set out in the statute.

For example, Part I, Chapter I of *RIPA* sets out, among other things, the conditions for authorizing a wiretap. Such conditions may include necessity and proportionality; the persons who may apply for and issue warrants authorizing the wiretap; the contents of an application for such a warrant; or restrictions on

the use of the information procured from the wiretap.[534] The Interception of Communications Commissioner is charged with limited review of these statutory requirements; for instance, he personally reviews intercept warrants to determine whether the authorization, warrant-content and warrant-renewal requirements were met. However, he does not have the authority to inspect a police or intelligence service's activities more generally to address questions such as whether an agency is undertaking prescribed activities without lawful authorization, whether the information-gathering that preceded the warrant application was undertaken lawfully, or whether the agency is complying with information-sharing rules or is undertaking activities that exceed its mandate.[535]

The Interception of Communications Commissioner has a small staff and a secretariat shared with other *RIPA* bodies. The Commissioner personally reviews intercept warrants through biannual reviews, spending approximately a half-day at each agency. A team of inspectors, consisting of one Chief Inspector and five inspectors, reviews the use of "communications data" (data about the medium, location, time, etc., rather than the content, of the communication) by over 800 public authorities.

The Office of Surveillance Commissioners, which has approximately 950 public authorities under its purview,[536] consists of the Chief Surveillance Commissioner, six part-time commissioners, three part-time assistant commissioners and seven full-time inspectors. The Office visits each of the law enforcement agencies within its purview once a year for a period of several days, and each of the other public authorities within its purview for approximately one day every two to three years.

As I noted above, *RIPA* established a separate body — the Investigatory Powers Tribunal — to address public complaints about the prescribed covert activities. While the review and complaint-processing functions are thereby separated by *RIPA*, the statute requires that the various review bodies give the Tribunal "all such assistance" as it may require in carrying out its mandate.[537] The Tribunal advises that it has not yet had recourse to this provision, though it has access to certain information by virtue of its shared secretariat with the ICC and the ISC.

The IPT has received hundreds of complaints since it was established. At the time of writing, no complaint had been upheld.

8.3.3.3
Powers

The public agencies that are subject to *RIPA* have an obligation to provide "all such documents and information as [the *RIPA* authorities] require for the purpose of enabling [them] to carry out [their] functions."[538]

In addition to its power to compel documents, the Investigatory Powers Tribunal may conduct proceedings related to the complaints it receives.[539] It has the power to make "any such award of compensation or other order as [it] think[s] fit," including the quashing of warrants or authorizations, and the destruction of records.[540] Appeals from orders of the Tribunal are available in certain circumstances.[541]

Unlike the IPT, the other *RIPA* authorities do not have the authority to issue binding orders.[542] Where they find a breach of the statute, they report it as described below.

8.3.3.4
Reporting

The Chief Surveillance Commissioner, the Interception of Communications Commissioner and the Intelligence Services Commissioner submit annual reports to the Prime Minister, who lays these reports before Parliament, with the exception of any information that the Prime Minister, in consultation with the ICC or Chief Commissioner, deems "prejudicial" to national security or other defined interests.[543]

The ICC and the ISC also submit reports to the Prime Minister on other matters as they see fit. The ICC submits reports to the Prime Minister on any breaches of the statutory provisions within his purview and on any inadequacy that he identifies in arrangements by public agencies for compliance with the statute.[544] The Chief Surveillance Commissioner is also charged with reporting on certain appeal determinations that he makes.[545]

The Investigatory Powers Tribunal submits reports to the Prime Minister only where it makes findings "in favour of" a complainant and any determinations relating to "any act or omission" or authorization by the responsible Minister.[546] The Tribunal does not file annual reports with the Prime Minister and is prohibited from reporting anything to a complainant other than "a statement" that a determination has been made in the complainant's favour.[547]

8.3.3.5
Appointment

The Interception of Communications Commissioner, the Intelligence Services Commissioner, and the Surveillance and Assistant Surveillance Commissioners are appointed by the Prime Minister, and must hold or have held high judicial office.[548] The Prime Minister announces these appointments in Parliament. Investigatory Powers Tribunal members each receive a Letter Patent signed by the Queen confirming their appointments.[549] The IPT President must hold or have held high judicial office; ordinary IPT members have the same prerequisite or can be lawyers with at least 10 years' experience.[550]

The Surveillance Commissioners are appointed for a term of three years,[551] and the IPT members for five years.[552] All are eligible for reappointment. There is no statutory restriction on the length of term for which the ICC and the ISC may be appointed.

9.
UNITED STATES

9.1
OVERVIEW

A number of agencies in the United States are involved in national security. The principal civilian agencies are the Central Intelligence Agency (CIA),[553] which is responsible for gathering foreign intelligence; the Federal Bureau of Investigation (FBI),[554] which handles domestic security; and the Department of Homeland Security (DHS),[555] which deals with immigration, border protection, customs and critical infrastructure. The State Department also has a Bureau of Intelligence and Research, which relies on all-source intelligence to create intelligence assessments, and generally analyzes and applies intelligence information to further U.S. diplomatic interests.[556] The Department of Defense (DoD) has its own large intelligence apparatus,[557] including responsibility for the National Security Agency (NSA),[558] which intercepts electronic and other signals.[559]

The principal accountability mechanisms for the FBI, the DHS, the CIA and the DoD are their respective offices of inspectors general and congressional oversight committees. By statute, Civil Liberties Protection officers have also been created within the DHS and the Office of the Director of National Intelligence. I have not set out information about the congressional committees in this chapter, but the reader may consult the Background Paper on International Models for more information.[560] I have discussed the offices of the

inspectors general at some length below, even though they are not formally at arm's length from the bodies over which they have jurisdiction, because I believe that they offer various features worthy of mention.[561]

At the time of writing, the national security landscape in the United States is in a state of flux. The FBI, the CIA and the DHS are reorganizing their intelligence capabilities in response to the final report of the 9/11 Commission,[562] the *Intelligence Reform and Terrorist Prevention Act of 2004*,[563] and the final report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction.[564] The military intelligence apparatus has also been affected by these initiatives. These changes follow a major bureaucratic reorganization effected by the *Homeland Security Act of 2002* and a significant expansion of government surveillance powers in the *USA PATRIOT Act of 2001*.[565] The U.S. president also authorized warrantless interceptions of communications to or from persons within the U.S., which has generated controversy.[566]

There is a strong movement at the federal level toward consolidating national security intelligence expertise and increasing information sharing between agencies. The newly created Office of the Director of National Intelligence has been mandated to lead this effort. The National Counterterrorism Center, created in 2004,[567] was recently transferred to the Director of National Intelligence to integrate the anti-terrorism capabilities of different agencies.[568]

9.2 LAW ENFORCEMENT AND SECURITY INTELLIGENCE

9.2.1 The Office of the Director of National Intelligence

In December 2004, American intelligence services were reorganized by the *National Security Intelligence Reform Act of 2004*.[569] Before this reform, the Director of Central Intelligence coordinated the American Intelligence Community[570] and served as the Director of the Central Intelligence Agency. Under the new act, primary responsibility for coordinating and managing national intelligence activities lies with the Director of National Intelligence (DNI), to whom the Director of the CIA reports. The DNI has also replaced the Director of the CIA as the chief intelligence advisor to the President and Congress on matters of national security.[571]

The DNI has direct authority over the CIA,[572] and must ensure that the Agency complies with law and the Constitution.[573] As a result of his or her role in determining the intelligence community's budget[574] and priorities,[575] the Director also has indirect oversight and tasking authority over the other

14 agencies. In addition, the DNI has some power over staffing arrangements[576] and training programs[577] for the intelligence community as a whole. Acting through the various host departments, the Director must ensure that these 14 agencies are acting legally.[578]

9.2.2 Federal Bureau of Investigation

The FBI is a branch of the Department of Justice and is established by statute.[579] It has over 30,000 employees,[580] and is responsible for regular policing of matters within federal jurisdiction, as well as internal national security matters.[581]

The FBI recently created a special National Security Branch, consolidating the Bureau's counter-terrorism, counter-intelligence and intelligence functions.[582] It has four sections: the Directorate of Intelligence, the Counterintelligence Division, the Counterterrorism Division and the Weapons of Mass Destruction Directorate.[583] One of the objects of the National Security Branch is to integrate the FBI's counter-terrorism and counter-intelligence investigative and operational capabilities with its intelligence capabilities.[584]

The Directorate of Intelligence is established under statute and has responsibility for supervising all domestic intelligence activities.[585] The Directorate collects intelligence information and receives information from the CIA and foreign partners. It then analyzes and distributes this information within the FBI, and in some circumstances to state and municipal law enforcement and other federal agencies.[586] The Counterintelligence Division is the principal counter-espionage agency within the United States. It aims to prevent penetration of U.S. intelligence services or government agencies by foreign powers; and stop the unauthorized acquisition of critical American classified information systems and technology.[587] The Counterterrorism Division focuses on preventing and disrupting terrorism. Within the Counterterrorism Division, the FBI operates a Terrorism Financing Operations section to combat terrorist financing networks. The Division participates in over 100 Joint Terrorism Task Forces, where local police, FBI, CIA and other government officials work in integrated teams.[588] Finally, the Weapons of Mass Destruction Directorate is a more recent addition to the National Security Branch, created in order to consolidate the FBI's Weapons of Mass Destruction components.[589]

9.2.3 Department of Homeland Security

The Department of Homeland Security was created by the *Homeland Security Act of 2002*.[590] The Act merged 22 separate agencies, including the law

enforcement divisions of the former immigration and customs services. The DHS has approximately 183,000 employees.[591]

The DHS is responsible for enforcing a wide range of U.S. laws and regulations. These law enforcement functions are divided among several DHS agencies, including U.S. Customs and Border Protection, which is responsible for enforcing immigration and customs laws at and between U.S. ports of entry; the U.S. Immigration and Customs Enforcement, which enforces U.S. immigration and customs laws relating to the movement of people and goods, including those that threaten national security; the Transportation Security Administration, which protects U.S. transportation systems, including airports; the U.S. Coast Guard, which is a military maritime service that protects U.S. interests in ports, waterways, coastal and international waters, and maritime regions; and the U.S. Secret Service, which protects senior government officials, including the President, and investigates threats against such persons.

Most DHS agencies have an internal intelligence organization that supports their specialized operational and investigative needs. However, two elements within the DHS are formally designated members of the U.S. intelligence community: the Office of Intelligence and Analysis (formerly part of the Information Analysis and Infrastructure Protection Directorate), which is the principal national security intelligence organization within the DHS;[592] and the National Intelligence Element of the U.S. Coast Guard.[593]

9.2.4 Central Intelligence Agency

The CIA, which was created by the *National Security Act of 1947*,[594] is the principal American foreign intelligence agency.[595] The number of employees of the CIA is not publicly disclosed.[596]

The CIA is responsible for:

- collecting intelligence through human sources and other appropriate means;
- correlating, evaluating and disseminating national security intelligence;
- providing overall direction and coordination of American foreign intelligence activities; and
- performing other duties or functions related to national security or intelligence, as directed by the President of the United States or the Director of National Intelligence.[597]

The CIA has no "police, subpoena, or law enforcement powers or internal security functions."[598] The recent creation of the National Clandestine Service within the CIA has expanded its human intelligence role. The National

Clandestine Service will be responsible for coordinating, integrating and evaluating human intelligence across the U.S. intelligence community.[599]

9.2.5 National Security Agency[600]

In the words of its official website, the mission of the National Security Agency "is to intercept and analyze foreign adversaries' communications signals."[601] The NSA is the U.S. cryptologic organization — the code-makers and code-breakers.[602] The Agency is the responsibility of the Department of Defense,[603] and forms part of the U.S. intelligence community. It was created by a presidential secret memorandum in 1952[604] and given a statutory basis in 1959.[605] The Agency's foreign intelligence collection mandate is regulated by the *Foreign Intelligence Surveillance Act* (*FISA*),[606] which deals with the interception of communications of persons with the United States, and by a 1981 presidential executive order that deals with intelligence collection of communications outside the United States.[607]

The NSA intercepts, decrypts and analyzes communications signals.[608] It may intercept only communications relating to foreign intelligence and counterintelligence.[609] To intercept the communications of persons within the United States who are believed to be agents of a foreign power — including terrorist suspects[610] — the NSA requires a judicial warrant issued by the Foreign Intelligence Surveillance Court.[611] Following the September 11, 2001 terrorist attacks, the U.S. president authorized the NSA to intercept without such a warrant certain communications involving U.S. persons.[612] Although the Inspector General of the NSA has reviewed the program,[613] the legality of the President's authorization remains unclear[614] and the Senate Judiciary Committee is currently investigating the program.[615] The House of Representatives Permanent Select Committee on Intelligence also recently announced its plan to increase oversight of the NSA program.[616]

The NSA's signals intelligence supports both civilian and military decision making within the United States government.[617] The Agency is also responsible for protecting U.S. government and other technological communications systems, including"reporting, and responding to cyber threats [and] making encryption codes to securely pass information between systems."[618] Finally, the NSA conducts a significant amount of technological research and development to protect American communications systems and enhance American technological communications abilities.[619] The number of employees of the NSA is not publicly disclosed,[620] but it is known to be one of the largest U.S. intelligence agencies.[621]

9.3 REVIEW AND OVERSIGHT

National security agencies in the United States are reviewed by congressional oversight committees, the statutory and non-statutory inspectors general of the various agencies, and in some cases by internal, but statutorily created, Civil Liberties Protection officers. Inspectors general are formally part of the respective departments or agencies in which they operate, and are subject to the general supervision of the head of that department or agency. However, the governing statute for inspectors general, the *Inspector General Act of 1978*,[622] contains many provisions that provide some independence for the IGs. These include requirements for selection without political affiliation; prerequisite criteria relating to fields of expertise; complete access to records and deliberations of the relevant department or agency; public reporting; and dismissal by the U.S. president only, who must report to Congress on the reasons for removal. On this basis, and since I believe several other features of the IGs' review tasks are relevant to my mandate, I have discussed the inspectors general in some detail below. I have also provided a brief description of the Civil Liberties Protection officers created in the Department of Homeland Security and the Office of the Director of National Intelligence.

9.3.1 Inspectors General

9.3.1.1 Jurisdiction

The *Inspector General Act*[623] and other statutes[624] establish inspector general offices for a number of federal public authorities. Each Office of the Inspector General has jurisdiction over a defined department or agency; the jurisdiction of each Inspector General is therefore agency-based.

Within each department or agency over which an IG has jurisdiction, there may be many well-established component organizations. For example, the jurisdiction of the Inspector General of the Department of Justice (IG DOJ) includes the FBI; the jurisdiction of the Inspector General of the Department of Homeland Security (IG DHS) includes American customs, immigration and transportation security authorities, along with a number of other constituent divisions;[625] and the jurisdiction of the Inspector General of the Department of Defense (IG DoD) covers all defence intelligence agencies, including the National Security Agency and its non-statutory Inspector General.[626] An IG's

jurisdiction can be vast. For instance, the purview of the IG DHS is 183,000 DHS employees; and the IG DHS has approximately 525 staff.

The Central Intelligence Agency has its own statutory IG (IG CIA).[627] The Director of National Intelligence has established a statutory inspector general for the Office of the Director of National Intelligence.[628] The U.S. State Department also has a statutory inspector general,[629] which recently reviewed the Department's Bureau of Intelligence and Research.[630]

The IG DOJ noted in discussion with Policy Review legal counsel that review jurisdiction over only one body — the DOJ — although internally varied, allows the development of critical institutional knowledge and expertise. In his view, U.S. government departments and agencies are too big and too complex to allow for a workable and effective inspector general model with jurisdiction over all government actors involved in national security and intelligence. The IG DHS and the IG CIA shared this view.[631]

Integrated Activities

The IG DHS stated that it was important to have other agencies with "cross-executive jurisdiction" over certain specialized matters, such as the Government Accounting Office, the Office of Management and Budget, and the Office of Information Security.

Under the *Inspector General Act*, inspectors general are specifically mandated to conduct, coordinate and supervise relationships with other government agencies in order to promote economy and efficiency, prevent fraud and abuse, and identify and prosecute participants in fraud or abuse.[632] The IG DOJ, IG DHS, IG DoD and the State Department IG may request information or assistance from any federal, state or local government agency or entity.[633] The IG CIA, with the approval of the Director of Central Intelligence, may request information or assistance from any federal government agency.[634] All statutory inspectors general are also members of the President's Council on Integrity and Efficiency,[635] while inspectors general appointed by the heads of various agencies are members of the Executive Council on Integrity and Efficiency.[636] These councils provide training and support to IGs, including in relation to issues that cut across different departments.[637] In the national security field, the IGs have also established an Intelligence Community Inspectors General Forum to bridge areas of responsibility and determine whether there are common themes or matters requiring joint investigative action.[638]

The IGs of the DOJ and the DHS noted that co-operation and information sharing between review bodies is necessary and desirable, in particular to address increasing integration. The IG DHS gave the example of the Homeland

Security Operations Center and the Joint Terrorism Task Forces, which are either under DHS auspices or include DHS elements. For these reasons, the inspectors general often jointly investigate matters that touch on two or more areas of responsibility, either at their own initiative or as directed by Congress.

The IG DOJ also emphasized that some form of comprehensive observation of the full picture of national security agency action and interaction is necessary. In the U.S., this role is played by congressional committees, which receive semi-annual reports and hear testimony from all statutory inspectors general. I have been told that the emerging role of the Inspector General for the Office of the Director of National Intelligence may also fill this need.

9.3.1.2
Mandate

The inspectors general review their respective agencies for economy, efficiency and propriety.[639] This includes review for compliance with the U.S. Constitution, statutes, executive orders, internal directives, policy and procedure.[640]

Since the passage of the *PATRIOT Act* in 2001,[641] the IG DOJ must also designate an official to "review information and receive complaints alleging abuses of civil rights and civil liberties by Department of Justice employees"; take measures to publicize this mandate; and submit semi-annual reports to Congress on its fulfillment of this mandate. The IG DHS also has a detailed civil rights and civil liberties accountability mandate,[642] but does not have an explicit mandate to handle civil liberties complaints.

9.3.1.3
Functions

To fulfill their mandates, the inspectors general conduct financial audits;[643] process complaints;[644] and carry out investigations[645] at their own initiative,[646] at the request of the head of their respective agencies or at the request of Congress.[647]

Other statutory functions of the IGs include reviewing relevant legislation to assess its impact on efficiency, and on the prevention and detection of abuse in programs and operations; and recommending policies, and conducting, supervising or coordinating other activities to improve efficiency and to prevent and detect abuse in programs and operations.[648]

Further, IGs often have functions that are specific to the agency under their purview.[649] For example, a core function of the IG DOJ is to investigate criminal wrongdoing by department employees, and complaints and other matters of "urgent concern" reported by FBI members or contractors.[650]

Investigations

Investigations can be carried out jointly with other IGs, and they can be complex and multidisciplinary. For example, the U.S. National Commission on Terrorist Attacks Upon the United States (9/11 Commission) requested that inspectors general of the relevant departments and agencies

> conduct investigations and reviews as necessary to determine whether and to what extent personnel at all levels should be held accountable for any omission, commission, or failure to meet professional standards in regard to the identification, prevention, or disruption of terrorist attacks, including the events of September 11, 2001.[651]

The Inspector General of the Department of Justice recently completed a report on the FBI's incorrect identification of an American citizen in connection with the Madrid bombings and the suspect's subsequent imprisonment.[652] The investigation included a detailed examination of the FBI's fingerprint identification processes, as well as the Bureau's interaction with Spanish National Police. The Mayfield report highlights the need for extensive law enforcement expertise in a body that reviews national security policing. Ultimately, many of the report's conclusions about the propriety of the investigation turned on the IG's evaluation of a bread-and-butter law enforcement activity: fingerprint identification.

The Inspector General of the DHS recently investigated two alleged incidents of criminal conduct by Border Patrol agents. The first investigation related to alleged sexual contact between a Border Patrol agent and two women detained for entering the United States illegally.[653] The second involved the shooting of an individual trying to flee across the U.S. border into Mexico.[654]

Complaint Handling

Complaint handling can require significant resources. Some IGs have therefore developed systems to reduce the administrative burden. For example, the Inspector General of the Department of Justice, which has about 400 staff and jurisdiction over 110,000 people, receives approximately 10,000 complaints per year. Since it has the right of first refusal for all non-frivolous allegations of misconduct, and since it lacks the resources to investigate such a high volume of complaints, the Office of the IG decides whether to investigate a complaint itself or refer the complaint to other internal or external bodies. The decisions are generally based on the seriousness of the allegation. In some cases of referral to another body, the IG will require that he or she be kept informed of

investigative results. The IG DOJ also monitors trends in complaints, sometimes aggregates them for systemic investigation, and periodically reviews the complaint-handling function of the bodies to which it refers complaints.

The Inspector General of the Department of Homeland Security carries out complaint processing in a similar manner. He refers the majority of complaints to other internal and external review bodies, largely based on an assessment of the seriousness of the complaint. The IG DHS has developed guidelines to manage complaint referrals and memoranda of understanding with various internal bodies.

The Department of Justice Inspector General has received thousands of complaints under its civil liberties complaint-handling mandate. Many of these have been used to carry out systemic investigations, such as the 2003 investigation of alleged misconduct and abuse of individuals held on immigration charges in connection with September 11 investigations.[655] The IG DOJ advises that while many of the complaints could not have been substantiated on their own, the fact and process of aggregating them allowed for conclusions of misconduct and systemic problems.

Both the IG DOJ and the IG DHS advise that their complaint investigations may overlap with or occur at the same time as criminal investigations or prosecutions. In such cases, they often proceed nonetheless, but with caution, so as to avoid interfering or prejudicing the criminal case. The IG DHS also advises that before he issues a report on a matter that may touch on an ongoing criminal investigation, he invites the relevant authorities to identify elements of information that could be prejudicial if disclosed. He may also delay publishing a report, or may redact sensitive portions, until after the criminal case is closed.

9.3.1.4
Powers

The statutory inspectors general have subpoena powers applicable to non-federal government actors, and are directed by statute to use methods other than subpoenas to obtain information from federal government actors.[656] In general, federal government actors co-operate in providing information. Information is often obtained through other inspectors general.

The inspectors general of the DOJ and the DHS advise that in practice they have access to information that is protected by a foreign third-party caveat only if the originating agency agrees. They will also comply with any conditions that the originating agency requires to allow access, including restrictions on further dissemination. The IG DHS advises that he has had no reason to disseminate such information.

The inspectors general of the DOJ, the DHS and the DoD have police powers that include the power to carry firearms, make arrests, and seek and execute search and seizure warrants.[657] Although the Inspector General of the CIA does not have police powers, the CIA is legally required to give the IG direct access to all employees, files and other materials within the Agency.[658]

Responsibility for imposing discipline in all cases rests outside the Office of the Inspector General, with bodies such as the Deputy Attorney General and the Office of Professional Responsibility.[659] The IG will make disciplinary recommendations to the appropriate department head.[660]

According to statute, when the IGs of the DoD, DOJ and DHS are pursuing investigations and other actions requiring access to information relating to intelligence, counter-intelligence, national security, ongoing criminal investigations, undercover operations or protected sources, they are under the "direction and control" of the applicable department head.[661] This direction and control formally includes the power to prevent an investigation being completed and sensitive information being disclosed.[662] However, the use of these provisions by a department head must be reported to Congress, along with reasons for doing so.[663] The IGs DOJ and DHS advised that this rule is commonly viewed as a deterrent to undue use of the power. For example, with respect to IG DOJ reports, the power has been invoked only once, in 1998.[664] Other agency heads also appear to have used the provisions rarely: neither the Secretary of National Security nor the Director of the CIA has yet used them.[665]

The inspectors general make findings and recommendations with respect to their investigative and monitoring activities, but do not have binding remedial or policy powers.[666] The IGs of the Department of Justice, Department of Homeland Security and Department of Defense can also conduct criminal investigations and make arrests.[667] The IG CIA conducts criminal investigations but does not make arrests. The inspectors general are also variously bound to report activity that alleges criminal activity or on which there are reasonable grounds to believe there was criminal activity.[668] While they have the power to make recommendations and to report on the department's response, inspectors general cannot make binding orders and have no power to order compensation.

9.3.1.5
Reporting

Inspectors general must file semi-annual reports with their respective congressional committees.[669] With the exception of the IG CIA reports, inspector general reports are generally public, although certain information or reports will sometimes remain classified. The reports may not publicly disclose confidential

national security information or confidential information relating to an ongoing criminal investigation.[670] The IG CIA reports are classified.[671] Reporting can be delayed if the head of a department exercises his or her power to prohibit disclosure of information relating to intelligence, counter-intelligence, national security, ongoing criminal investigations, undercover operations or protected sources, as described in the previous section. In the one instance of use of the power with respect to an IG DOJ report, noted above, the IG's report was delayed by six months.[672]

The non-statutory IG of the NSA and the other three intelligence sub-agencies within the Department of Defense[673] must submit annual reports to the congressional intelligence committees. These reports must include a plan showing the programs and activities scheduled for review by the relevant IG, as well as any other matters relating to the independence and effectiveness of the Office of the IG.[674]

9.3.1.6
Appointment and Composition

The President, subject to confirmation by the Senate, appoints statutory inspectors general.[675] The Director of the NSA appoints the Inspector General of the National Security Agency.[676] The IG of the Department of Defense cannot be in the military.[677] Inspectors general are appointed on the basis of integrity and a "demonstrated ability in accounting, auditing, financial analysis, law, management analysis, public administration, or investigations."[678] In addition, the IG CIA must comply with the CIA's security standards and have prior experience in the field of foreign intelligence.[679]

9.3.2
New Civil Liberties Protection Officers

The Inspector General of the Department of Homeland Security does not have the specific civil liberties complaint-handling function that the *PATRIOT Act* granted the IG DOJ. Instead, a new Officer for Civil Rights and Civil Liberties has been created within the DHS.[680] This officer has a mandate to assist in policy development with a view to protecting civil liberties; overseeing compliance with law and policy regarding civil rights and civil liberties; coordinating privacy protection with the DHS Privacy Officer; and investigating complaints regarding civil rights and civil liberties that the Inspector General of the DHS chooses not to investigate.[681] The Officer has entered into a MOU with the Inspector General's office to "prevent duplication of effort and ensure the most effective, efficient and appropriate deployment of resources."[682] Among other things, this

MOU sets out decision-making procedures on whether the Inspector General's office or the Officer for Civil Rights and Civil Liberties will carry out primary investigation of a complaint. Pursuant to his statutory responsibility, the DHS Officer for Civil Rights and Civil Liberties has produced semi-annual reports on the implementation of his mandate.

A Civil Liberties Protection Officer has also been created as part of the Office of the Director of National Intelligence.[683] This officer is responsible for ensuring that privacy and civil liberties protections are incorporated in policies developed and implemented by the Office of the Director of National Intelligence and by the different organizations within the intelligence community. The Officer also oversees compliance with the U.S. Constitution, and with domestic law and policy relating to civil liberties and privacy; takes complaints about abuses of civil liberties or privacy violations; and where appropriate, may refer complaints to the inspectors general of the intelligence communities' component agencies. The Officer also looks at the impact of technology on privacy and conducts privacy impact assessments.[684]

10.
LIST OF ACRONYMS USED IN THIS CHAPTER

ACC	Australian Crime Commission
AFP	Australian Federal Police
ASIO	Australian Security Intelligence Organisation
ASIS	Australian Secret Intelligence Service
BfV	Federal Office for the Protection of the Constitution (Germany)
BND	Federal Intelligence Service (Germany)
CIA	Central Intelligence Agency (U.S.)
Committee I	Standing Committee for the Monitoring of Intelligence Services (Belgium)
Committee P	Standing Committee for the Monitoring of Police Forces (Belgium)
DHS	Department of Homeland Security (U.S.)
DNI	Director of National Intelligence (U.S.)
DIO	Defence Intelligence Organisation (Australia)
DSD	Defence Signals Directorate (Australia)
EOS Committee	Committee for Oversight of the Intelligence, Surveillance and Security Services (Norway)

FBI	Federal Bureau of Investigation (U.S.)
FISA	*Foreign Intelligence Surveillance Act (FISA)* (U.S.)
GCHQ	Government Communications Headquarters (U.K.)
GCSB	Government Communications Security Bureau (New Zealand)
HMIC	Her Majesty's Inspectorate of Constabulary (U.K.)
HMRC	Her Majesty's Revenue and Customs (U.K.)
ICC	Interception of Communications Commissioner (U.K.)
IG	IGIS Inspector General (U.S.)
IGIS	Inspector-General of Intelligence and Security (Australia, New Zealand)
IPCC	Independent Police Complaints Commission (U.K.)
IPT	Investigatory Powers Tribunal (U.K.)
ISC	Intelligence Services Commissioner (U.K.)
MAD	Military Counterintelligence Service (Germany)
MI-5	Security Service (U.K.)
MI-6	Secret Intelligence Service (U.K.)
MOU	Memorandum of Understanding
NSA	National Security Authority (Norway)
NZSIS	New Zealand Security Intelligence Service
ONA	Office of National Assessments (Australia)
OSC	Office of the Surveillance Commissioners (U.K.)
PKGr	Parliamentary Control Panel (Germany)
PSNI	Police Service for Northern Ireland (U.K.)
RIPA	*Regulation of Investigatory Powers Act 2000* (U.K.)
SE	*Surêté de l'État* (Belgium)
SEFO	Special Investigating Body for Police Matters (Norway)
SGRS	*Service général du Renseignement et de la Sécurité des Forces armées* (Belgium)
SIRC	Security Intelligence Review Committee (Canada)
SOCA	Serious Organised Crime Agency (U.K.)

Notes

1 I refer the reader to Chapter XII, "Policy Review Process," for a discussion of my reasons for selecting these review models for detailed study, and the process I used to conduct this examination.

2 To avoid undue repetition of substantial amounts of information contained elsewhere in this chapter, I have excluded source citations and footnoted explanations to the information in the Introduction.

3 Except where otherwise noted, the information in this chapter is based on meetings and communications between Policy Review legal counsel and representatives of the entities described in this chapter.

4 This is in part due to a "referral" of legislative power from the states and territories to the federal government to allow the "Commonwealth," as the federal government is known in Australia, to counter terrorism through legislative change and enforcement. Such referrals of power are authorized by section 51(xxxvii) of the Australian Constitution. See the Commonwealth and States and Territories Agreement on Terrorism and Multi-jurisdictional Crime, 5 April 2002, online, http://www.coag.gov.au/meetings/050402/terrorism.pdf (accessed May 15, 2006); and related state, territory and Commonwealth legislation. See also the *Commonwealth of Australia Constitution Act, 1900* (U.K.), 63 & 64 Vict., c. 12, online, http://www.comlaw.gov.au/comlaw/comlaw.nsf/440c19285821b109ca256f3a001d59b7/57dea3835d797364ca256f9d0078c087/$FILE/ConstitutionAct.pdf (accessed May 15, 2006); and the Department of Prime Minister and Cabinet, *Protecting Australia Against Terrorism: Australia's National Counter-Terrorism Policy and Arrangements* (Canberra: Commonwealth of Australia, 2004), p. 18, online, http://www.dpmc.gov.au/publications/protecting_australia/docs/protecting_australia.pdf (accessed May 15, 2006).

5 *Australian Crime Commission Act, 2002* (Cth.) [*ACC Act*].

6 "Australian and International Law to Combat Terrorism," online, National Security Australia, http://www.nationalsecurity.gov.au/agd/www/nationalsecurity.nsf/Page/What_Governments_are_doingAustralian_and_International_Law_to_Combat_Terrorism (accessed May 15, 2006).

7 See discussion below.

8 The term "Australian Intelligence Community," or "AIC," is commonly used in Australia in reference to the Australian Security Intelligence Organisation (ASIO), the Australian Secret Intelligence Service (ASIS), the Defence Signals Directorate (DSD), the Office of National Assessments (ONA), the Defence Imagery and Geospatial Organisation (DIGO), and the Defence Intelligence Organisation (DIO).

9 *Inspector-General of Intelligence and Security Act, 1986* (Cth.), s. 16 [*IGIS Act*]. This obligation also extends to consultations with the Auditor-General.

10 *Australian Federal Police Act 1979* (Cth.), s. 8(1)(b)(i) [*Australian Federal Police Act*].

11 *Criminal Code Amendment (Terrorism) Act 2003 (Constitutional Reference of Powers)* (Cth.). There are now 26 post-9/11 laws.

12 *Australian Federal Police Act,* s. 8(1).

13 Ibid. The Australian Protective Service was incorporated into the Australian Federal Police (AFP) in July 2002.

14 Australian Federal Police, "A New Functional Structure for the AFP," 82 Platypus (March 2004), p. 41, online, http://www.afp.gov.au/__data/assets/pdf_file/3973/functional_model.pdf (accessed May 15, 2006).

15 Ibid., p. 44.

16 Australian Federal Police, *AFP Annual Report 2002–2003*, p. 47, online, http://www.afp.gov.au/about/publications/annual_reports/afp (accessed May 15, 2006).

17 Australian Federal Police, "Australian Federal Police Counter Terrorism Measures."

18 Australian Federal Police, "International: Law Enforcement Cooperation Program (LECP)," online, http://www.afp.gov.au/international/liaison/LECP (accessed May 15, 2006); *AFP Annual Report 2002–2003*, p. 15. Indonesia and Australia also have a memorandum of understanding regarding ongoing law enforcement collaboration to combat transnational crime and develop police co-operation: *AFP Annual Report 2002–2003,* pp. 30, 42.

19 *AFP Annual Report 2002–2003*, p. 15.

20 *ACC Act*.

21 Australian Crime Commission, *Annual Report 2003–04*, p. 1, online, http://www.crimecommission.gov.au/content/publications/annual_reports/2004/pub-ar-2004-1.pdf (accessed May 15, 2006). See also the *ACC Act*, ss. 49, 58.

22 *ACC Act*, ss. 7A, 7C.

23 Ibid., s. 7B.

24 Ibid., s. 7C.

25 Examiners are appointed by the Governor-General and must have been legal practitioners for at least five years: *ACC Act*, s. 46B.

26 *ACC Act*, Division 2.

27 Ibid., s. 20.

28 Ibid., s. 12.

29 Ibid., s. 59(7).

30 Ibid., s. 59(9). The information must be relevant to the performance of the department's or agency's functions, and the CEO may provide recommendations.

31 Ibid., s. 59(11). The information must be relevant to security.

32 *Australian Security Intelligence Organisation Act 1979* (Cth.), s. 17 [*ASIO Act*], online, http://www.asio.gov.au/About/comp.htm (accessed May 15, 2006); http://www.nationalsecurity.gov.au/agd/www/nationalsecurity.nsf/AllDocs/348468DF2890F6A0CA256FCC001222D0?OpenDocument (accessed May 15, 2006).

33 *ASIO Act*, s. 17.

34 Ibid., s. 17.

35 Ibid., ss. 17ff.

36 http://www.asio.gov.au/About/comp.htm (accessed May 15, 2006).

37 Media release 191/2005, issued on 15 October 2005 by the Australian Attorney-General, the Hon. Philip Ruddock, MP, online, http://www.ag.gov.au/agd/WWW/MinisterRuddockHome.nsf/Page/Media_Releases2005 (accessed May 15, 2006).

38 Inspector-General of Intelligence and Security, *Annual Report 2002–2003* (Canberra: Commonwealth of Australia, 2003), p. 27, online, http://www.igis.gov.au/annuals/02-03/con_table.cfm (accessed May 15, 2006) [IGIS *Annual Report 2002–2003*].

39 Australia, *Report of the Inquiry into Australian Intelligence Agencies* (Canberra: Commonwealth of Australia, 2004), p. 146 (Chair: Philip Flood, AO).

40 *Intelligence Services Act 2001* (Cth.).

41 Ibid., ss. 6, 8, 9, 11, 12.

42 The *Rules to Protect the Privacy of Australians* are issued pursuant to s. 15 of the *Intelligence Services Act 2001*. The current Rules are available online at http://www.asis.gov.au/rules_to_privacy.html (accessed May 15, 2006).

43 *Intelligence Services Act 2001*, s. 11(1).

44 *Report of the Inquiry into Australian Intelligence Agencies*, p. 147.

45 *Intelligence Services Act 2001*, s. 11(2).

46 Ibid.

47 IGIS *Annual Report 2002–2003*, p. 33.

48 *Intelligence Services Act 2001*, s. 11(1).

49 Ibid., s. 11(2).

50 *Office of National Assessments Act 1977* (Cth.), s. 5(1).

51 Office of National Assessments, *Corporate Plan for 2003–2006*, online, http://www.ona.gov.au/corporate.shtml (accessed May 15, 2006); IGIS *Annual Report 2002–2003*, p. 43.

52 *Intelligence Services Act 2001*, s. 6B. DIGO was only recently put on this statutory footing by the *Legislation Amendment Act 2005* (Cth.).

53 *Report of the Inquiry into Australian Intelligence Agencies*, pp. 142–143.

54 IGIS *Annual Report 2002–2003*, p. 120.

55 Jurisdiction over the AFP is established by the *Complaints (Australian Federal Police) Act 1981* (Cth.). Jurisdiction over the ACC, most intelligence agencies and other public authorities is established by the *Ombudsman Act 1976* (Cth.). Legislation is expected to be introduced into the Parliament in 2006 to repeal the *Complaints (Australian Federal Police) Act* and to place the AFP under the jurisdiction of the *Ombudsman Act*.

56 *Ombudsman Act 1976* (Cth.), s. 4(4); *Migration and Ombudsman Legislation Amendment Act 2005* (Cth.), Schedule 2. See also Australia, Office of the Commonwealth Ombudsman, Immigration Bulletin 6: "Progress on Immigration Matters," December 14, 2005, online, http://www.ombudsman.gov.au/commonwealth/publish.nsf/content/bulletin_2005_06 (accessed May 15, 2006).

57 *Migration Act 1958* (Cth.), Part 8C. See also Australia, Office of the Commonwealth Ombudsman, "Commonwealth Ombudsman review of circumstances of long-term immigration detainees," July 14, 2005, online, Commonwealth Ombudsman, http://www.comb.gov.au/commonwealth/publish.nsf/Content/mediarelease_2005_04 (accessed May 15, 2006).

58 *Ombudsman Act 1976*, s. 15.

59 *Ombudsman Act 1976*, s. 5(1)(b); *Complaints (Australian Federal Police) Act 1981* (Cth.), s. 21A [*Complaints (AFP) Act*].

60 *Telecommunications (Interception) Act 1979* (Cth.), s. 84**;** *Crimes Act 1914* (Cth.), Part 1A. See also the *Surveillance Devices Act 2004* (Cth.), ss. 54ff., and the Ombudsman's *Annual Report 2003–2004,* pp. 62ff.

61 *Complaints (AFP) Act*, s. 6.

62 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98, online, http://www.austlii.edu.au/au/other/alrc/publications/reports/98/Ch_02.html (accessed May 15, 2006).

63 *Complaints (AFP) Act*, s. 21A; *Ombudsman Act 1976,* s. 5(1)(b).

64 Commonwealth Ombudsman, *Annual Report 2003–2004* (Canberra: Commonwealth of Australia, 2004), p. 61, online, http://www.comb.gov.au/publications (accessed May 15, 2006). The Ombudsman's 2003–2004 annual report noted that "[o]nly six complaints were received in 2003–04 [regarding the ACC], largely reflecting the fact that the ACC's role does not bring its staff in close contact with members of the public." In 2004–05, the Ombudsman received 12 complaints regarding the ACC: Commonwealth Ombudsman, *Annual Report 2004–2005*, p. 55.

65 *Telecommunications (Interception) Act 1979*, s. 83.

66 *Crimes Act 1914*, Part IAB.

67 *Surveillance Devices Act 2004*, ss. 54ff.

68 Australia, Commonwealth Ombudsman, *Department of Immigration and Multicultural Affairs: Administration of s. 501 of the Migration Act as it Applies to Long-term Permanent Residents* (Canberra: Commonwealth Ombudsman, 2006), online, Commonwealth Ombudsman, http://www.comb.gov.au/commonwealth/publish.nsf/AttachmentsByTitle/reports_2006_01_pdf/$FILE/s501_immigration_feb-2006.pdf (accessed May 16, 2006).

69 On accountability gaps in Australia generally, see Claire Pitham and Prof. John McMillan, "Who's Got the Map? The Changing Landscape of National Law Enforcement, Homeland Security and the Role of Administrative Accountability Bodies," academic paper forwarded to Policy Review legal counsel by the Australian Commonwealth Ombudsman's Office; and the Commonwealth Ombudsman, *Annual Report 2003–2004*, p. 55.

70 *Ombudsman Act 1976*, s. 8B.

71 See *ACC Act*, s. 49. Such "cross-jurisdiction" and "integration" issues are increasingly common for the Ombudsman, and in Australia generally. For example, a recent review of the use and sharing of DNA material among law enforcement agencies (both at the federal and state/territory level) made several recommendations to address similar accountability gaps and overlaps. It proposed that review bodies coordinate to determine who should take the "lead role" when numerous agencies have jurisdiction, and to "cover any jurisdictional gaps" created by federalism considerations: *Report of Independent Review of Part ID of the Crimes Act 1914 – Forensic Procedures*, ch. 5, p. 77, online, http://www.ag.gov.au/agd/WWW/criminaljusticeHome.nsf/D2801B61EABE80A2CA256809001328BA/F974FEAA49CD7F32CA256D2500090F58 (accessed May 16, 2006). The Ombudsman also discussed the accountability gaps arising from increasing integration in his 2003–2004 annual report, p. 55. See also the Inspector-General's discussion below, which highlights a recommendation by a parliamentary joint committee for "greater liaison between" the Ombudsman, state ombudsmen and the Inspector-General.

72 Parliamentary Joint Committee on ASIO, ASIS and DSD, *Review of administration and expenditure for ASIO, ASIS and DSD* (Canberra: Commonwealth of Australia, 2005), tabled March 14, 2005, p. 22.

73 *Ombudsman Act 1976*, ss. 9, 13, 14.

74 *Complaints (AFP) Act*, ss. 27, 29, 30.

75 *Ombudsman Act 1976*, ss. 8(2A)–8(2E), 8(3).

76 *Complaints (AFP) Act*, ss. 27(4), 30(3).

77 *Ombudsman Act 1976*, s. 15.

78 Ibid.

79 Ibid., s. 16. Where the report relates to a parliamentary department or to a court or tribunal, provision is made for reporting to other individuals, such as the President of the Senate, etc.

80 Ibid., s. 17.

81 For example, actions that were contrary to law; unreasonable, unjust, oppressive or improperly discriminatory; in accordance with a law that fits one of the above descriptors; based on mistake; or otherwise wrong; or that constituted an exercise of discretion for an improper purpose or on irrelevant grounds, or followed by inadequate reasons to the complainant: *Complaints (AFP) Act*, s. 31(1). See also ss. 26(3), (3A), (3B), 36(1).

82 *Complaints (AFP) Act*, ss. 32, 33.

83 Ibid., s. 37.

84 *Ombudsman Act 1976*, s. 19; *Complaints (AFP) Act*, s. 38.

85 *Ombudsman Act 1976*, s. 19.

86 Ibid., ss. 21–22.

87 *IGIS Act*, ss. 8ff.

88 Ibid., s. 4.

89 Ibid., s. 8.

90 Ibid., s. 8(1).

91 Ibid., s. 8(2)(c).

92 Ibid., s. 8(1)(d).

93 Ibid., s. 8(8)(a).

94 Ibid.

95 Ibid., s. 9.
96 IGIS *Annual Report 2002–2003*, Annex 2 – Bali Inquiry Report.
97 *IGIS Act*, ss. 18, 19(1), 20.
98 Ibid., s. 18(6).
99 Ibid., s. 16.
100 Ibid.
101 See discussion above of Commonwealth Ombudsman.
102 *IGIS Act*, s. 21.
103 Ibid., s. 22.
104 Ibid, ss. 22(1), (2).
105 Ibid., s. 24.
106 Ibid., s. 23.
107 Ibid., s. 35(1), (2), (2B).
108 Ibid., s. 35.
109 Ibid., s. 6.
110 Ibid., s. 26.
111 For a summary, see http://www.belgium.be/eportal/application?origin=navigationBanner.jsp&event=bea.portal.framework.internal.refresh&pageid=indexPage&navId=2681 (accessed May 16, 2006).
112 For more information, see the Belgium government's portal, http://www.belgium.be/eportal/application?origin=hardcodedAboutBelgiumNavTeaser.jsp&event=bea.portal.framework.internal.refresh&pageid=indexPage&navId=2679 (accessed May 16, 2006).
113 For a summary, see the Belgium government's portal.
114 For a summary, see http://www.belgium.be/eportal/application?origin=navigationBanner.jsp&event=bea.portal.framework.internal.refresh&pageid=indexPage&navId=2696 (accessed May 16, 2006).
115 For a summary, see http://www.belgium.be/eportal/application?origin=navigationBanner.jsp&event=bea.portal.framework.internal.refresh&pageid=indexPage&navId=1301 (accessed May 16, 2006).
116 See parliamentary document 51K0258, online, http://www.lachambre.be/kvvcr/showpage.cfm?section=flwb&language=fr&rightmenu=right&cfm=flwb.cfm?lang=F&legislat=51&dossierID=0258 (accessed May 16, 2006). This legislation was passed following the European Council's Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA), online, http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_164/l_16420020622en00030007.pdf (accessed May 16, 2006).
117 See parliamentary document 51K0383, online, http://www.lachambre.be/kvvcr/showpage.cfm?section=flwb&language=fr&rightmenu=right&cfm=flwb.cfm?lang=F&legislat=51&dossierID=0383 (accessed May 16, 2006). This legislation was passed following the European Council's Directive of 4 December 2001 relating to terrorism financing (2001/97/EC).
118 See EU Network of Independent Experts in Fundamental Rights, "The Balance between Freedom and Security in the Response by the European Union and its Member States to the Terrorist Threats," pp. 27ff., online, http://www.statewatch.org/news/2003/apr/CFR-CDF.ThemComment1.pdf (accessed May 16, 2006).
119 *Loi organisant un service de police intégré, structuré à deux niveaux*, M.B., 5 January 1999, 132, as amended, online, http://www.juridat.be/cgi_loi/loi_F.pl?cn=1998120731 (accessed May 16, 2006).
120 All information in this paragraph is cited to http://www.polfed.be (accessed May 16, 2006). See also the principal statute governing Belgian police forces, *Loi organisant un service de police intégré structuré à deux niveaux*.

121 See press release of the Chancellerie du Premier Ministre – Conseil des Ministres, dated March 30, 2004, online, http://www.belgium.be/eportal/application?origin=searchResults.jsp&event=bea.portal.framework.internal.refresh&pageid=contentPage&docId=33881 (accessed May 16, 2006).

122 Ibid.

123 Belgium, Police fédérale, "La Police integrée. Qui fait quoi? – 'Police locale' and 'Police fédérale,'" online, Police fédérale, http://www.polfed.be/pol_int_fr.php (accessed May 16, 2006).

124 See text of speech by Prime Minister Guy Verhofstadt, Committee meeting 18 March 2004, debate on terrorism, p. 6, online, http://www.dekamer.be/doc/CCRI/pdf/51/ic202.pdf (accessed May 16, 2006). See also, online, http://www.belgium.be/eportal/application?languageParameter=fr&pageid=contentPage&docId=7849 (accessed May 16, 2006).

125 See the *Loi organique des services de renseignement et de sécurité*, M.B., 18 December 1998, 40312, as amended, online, http://www.juridat.be/cgi_loi/loi_F.pl?cn=1998113032 (accessed May 16, 2006) [*Loi organique des services*]. See also, online, http://www.belgium.be/eportal/application?origin=searchResults.jsp&event=bea.portal.framework.internal.refresh&pageid=contentPage&docId=7849 (accessed May 16, 2006).
The initialisms are based on the French names for these agencies: thus, "SE" for *Sûreté de l'État* and "SGRS" for *Service général du Renseignement et de la Sécurité*.

126 *Loi organique des services*, art. 2.

127 Ibid., art. 7. The ministerial committee is discussed in more detail under "Review and Oversight."

128 Ibid., art. 8.

129 Ibid., art. 11.

130 Ibid., art. 11, §§ 2, 3.

131 Ibid., arts. 12, 13.

132 Ibid., art. 14.

133 *Loi organique du contrôle des services de police et de renseignements*, M.B., 26 July 1991, 16576**,** arts. 3, 9, as amended, online, http://www.juridat.be/cgi_loi/loi_F.pl?cn=1991071853 (accessed May 16, 2006) [*Loi organique du contrôle*]. In French, Committee P is *Comité permanent de contrôle des services de police,* or *Comité P*.

134 Committee P translates the French word *contrôle* as "monitoring" in English. However, for consistency I have used the word "review" throughout this chapter.

135 *Loi organique du contrôle*, art. 1.

136 Ibid., art. 9.

137 Committee P's 2003 annual report, online, Comité P, *Rapport annuel 2003*, http://www.comitep.be/2003/Fr/RA_2003.pdf.

138 The governing statute expressly provides for the establishment of an investigations department within Committee P with the authority to conduct investigations either on its own initiative or at the request of Committee P. See *Loi organique du contrôle*, arts. 1, 15, 16.

139 *Loi organique du contrôle*, art. 8.

140 Ibid., art. 9.

141 Ibid., art. 24–art. 27 bis. Art. 24 states that this power is subject to certain forms of immunity and privilege.

142 Ibid., art. 24 § 2.

143 Ibid., art. 27 bis. This power may be exercised only in the presence of the police chief or the chief's designate.

144 Ibid., art. 27 bis.

145 Ibid., art. 24 § 3.

146 Ibid., arts. 9, 12.
147 Ibid., art. 16.
148 Ibid., arts. 52ff.
149 Ibid.
150 Ibid., arts. 8, 9, 11, 32, 33, 35.
151 *Loi portant création d'un organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité du 11 décembre 1998*, M.B., 7 May 1999, as amended, online, http://www.juridat.be/cgi_loi/loi_F.pl?cn=1998121162.
152 *Loi organique du contrôle*, arts. 9, 11.
153 Ibid., art. 11.
154 Ibid.
155 Ibid., art. 4.
156 Ibid.. See also http://www.comiteri.be (accessed May 17, 2006). In French, Committee I is *Comité permanent de contrôle des services de renseignements*, or *Comité R*.
157 *Loi du 1 avril 1999*, art. 4, amending art. 3 of the *Loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements*, M.B., 3 April 1999, 11161, online, http://www.juridat.be/cgi_loi/loi_F.pl?cn=1999040131.
158 *Loi organique du contrôle*, art. 1.
159 Ibid., art. 33.
160 *Comité R, Rapport d'activités 2003*, online, http://www.comiteri.be/index_fr.html (accessed May 17, 2006. The name *Comité R* is explained at note 156 of this report.
161 As with Committee P, the statute expressly provides for the establishment of an investigation department within Committee I, and provides it with the authority to begin investigations on its own initiative or at the Committee's request. See the *Loi organique du contrôle des services de police et de renseignements*, arts. 1, 39–40.
162 *Loi organique du contrôle*, arts. 32ff.
163 Ibid., art. 33 § 2.
164 Ibid., arts. 48ff. Art. 48 states that this power is subject to certain forms of immunity and privilege.
165 Ibid., art. 51 bis.
166 Ibid.
167 Ibid., art. 48, § 3.
168 Ibid., arts. 33, 35.
169 Ibid., arts. 52ff.
170 Ibid., arts. 33, 35.
171 Ibid., art. 35.
172 Ibid.
173 Ibid., arts. 28ff.
174 See *Grundgesetz (The Basic Law): The Constitution of the Federal Republic of Germany* (May 23, 1949), ed. Axel Tschentscher (Würzburg: Jurisprudentia Verlag Würzburg, 2002), online, http://jurisprudentia.de/jurisprudentia.html (accessed May 17, 2006).
175 See the Office for the Protection of the Constitution website at http://www.verfassungsschutz.de/en/about_us.html/bfv_engl.html (accessed May 17, 2006). Note that the website has been reorganized since this report was researched. See also Assembly of Western European Union, The interim European Security and Defence Assembly, "Parliamentary oversight of the intelligence services in the WEU countries – current situation and prospects for reform – Germany," online, http://www.assembly-weu.org/en/documents/sessions_ordinaires/rpt/2002/1801.html (accessed May 17, 2006) [Interim European Security and Defence Assembly, "Parliamentary oversight"]. See also "Internal Affairs Ministers

discuss security structures," *German News* – English Edition (July 7, 2004), online, http://www.germnews.de/cgi-bin/show/dn/2004/07/07.html/4 (accessed May 17, 2006).

176 See Oliver Lepsius, "Liberty, Security, and Terrorism: The Legal Position in Germany" (May 2004) 5 German L.J. 435, pp. 437, online, German Law Journal, http://www.germanlawjournal.com/pdf/Vol05No05/PDF_Vol_05_No_05_435-460_special_issue_Lepsius.pdf (accessed May 17, 2006); Erik van de Linde, Kevin O'Brien, Gustav Lindstrom et al., "Quick Scan of Post 9/11 National Counter-Terrorism Policymaking and Implementation in Selected European Countries," Research Project for the Netherlands Ministry of Justice (Leiden: Rand Europe, May 2002), pp. 61–75, online, Rand Europe, http://www.rand.org/randeurope/review/1.4-obrien.html (accessed May 17, 2006); German Foreign Office, Report to the Security Council Committee established pursuant to Resolution 1373 (2001) concerning Counter-Terrorism, online, http://www.auswaertiges-amt.de/www/de/infoservice/download/pdf/vn/ctc_bericht.pdf (accessed May 17, 2006); Markus Rau, "Country Report: Germany," in *Terrorism as a Challenge for National and International Law – Security versus Liberty*, Christian Walter, Silja Vöneky, Volker Röben et al., eds., Max Planck Institute for Comparative Public Law and International Law (Heidelberg: Springer, 2003), online, http://www.mpil.de/ww/en/pub/research/details/publications/staff/pub03.cfm (accessed May 17, 2006) [Rau report].

177 See Lepsius, p. 441. See also *Gesetz zur Bekämpfung des internationalen Terrorismus* (TerrorBekämpfG), 9 January 2002 (BGB1 I 2002, pp. 361, 3142) *(Counter-Terrorism Act)*, Abs. 1, § 6. German legislation can be found online at http://bundesrecht.juris.de/.

178 See van de Linde, O'Brien, Lindstrom et al., pp. 64–65.

179 For comments, see, for example, Amnesty International, "Back in the Spotlight: Allegations of police ill-treatment and excessive use of force in Germany," EUR 23/001/2004 (January 14, 2004), online, http://web.amnesty.org/library/print/ENGEUR230012004 (accessed May 17, 2006); United Nations Committee against Torture, "Conclusions and recommendations of the Committee against Torture: Germany (Concluding Observations/Comments)," CAT/C/CR/32/7 (11/06/2004), online, http://www.unhchr.ch/tbs/doc.nsf/0/5d9c452885c30123c1256ebd00506b57?Opendocument (accessed May 17, 2006).

180 Christian Heyer, Secretariat of the Parliamentary Control Panel of the German Bundestag for the Oversight of the Intelligence Services, "Parliamentary Oversight of Intelligence: The German Approach" (Paper presented to The Changing Face of Intelligence: NATO Advanced Research Workshop, Pluscarden Programme for the Study of Global Terrorism and Intelligence, St. Anthony's College, Oxford, England, December 2005) [unpublished], p. 9 [Heyer, "Parliamentary Oversight"].

181 From the German *Bundesamt für Verfassungsschutz*.

182 Heyer, "Parliamentary Oversight," p. 10.

183 *Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz* (BverfSchG), 20 December 1990 (BGB1 I S p. 2954) (*Federal Act on the Protection of the Constitution)*, § 3, para. 1(1)–(3) [*Federal Constitution Protection Act*]. Cited in *2003 Annual Report of the Office for the Protection of the Constitution*, p. 13, online, http://www.verfassungsschutz.de/en/publications/annual_reports/vsbericht2003.engl.html/vsbericht_2003_engl.pdf (accessed May 17, 2006).

184 *Federal Constitution Protection Act*, § 3, para.1(4); *2003 Annual Report of the Office for the Protection of the Constitution*, p. 13; *Grundgesetz für die Bundesrepublik Deutschland* (GG), 23 May 1949 (BGB1 III p. 100-1) (*The Basic Law)*, most recently amended by the amending act dated 26 July 2002 (BGB1 I S, p. 2863), §§ 9(2) and 26(1), online, http://www.bundesregierung.de/en/Federal-Government/Function-and-constitutional-ba-,10206/Basic-Law.htm (accessed May 17, 2006).

185 See the *Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes (*Sicherheitsüberprüfungsgesetz – SÜG), 20 April 1994 (BGB1 I S, p. 867) (*Security Clearance Act)*; and the *2003 Annual Report of the Office for the Protection of the Constitution*, p. 14. See also the Rau report, p. 28. The definition of "security sensitive areas" was expanded by the second security package.

186 *2003 Annual Report of the Office for the Protection of the Constitution*, p. 14.

187 Office for the Protection of the Constitution website; *2003 Annual Report of the Office for the Protection of the Constitution*, p. 13.

188 *Federal Constitution Protection Act*, § 8, paras. 5–8; *Counter-Terrorism Act*, § 1. See also the Rau report, p. 21.

189 Lepsius, p. 14.

190 Office for the Protection of the Constitution website. The website has been reorganized since this report was researched, and the wording may have changed.

191 Heyer, "Parliamentary Oversight," p. 10.

192 Office for the Protection of the Constitution website. See also Interim European Security and Defence Assembly, "Parliamentary oversight."

193 Heyer, "Parliamentary Oversight," p. 10.

194 Office for the Protection of the Constitution website. See also Interim European Security and Defence Assembly, "Parliamentary oversight."

195 See, for example, "Internal Affairs Ministers discuss security structures."

196 From the German *Militärischer Abschirmdienst*.

197 Heyer, "Parliamentary Oversight," p. 11.

198 *Gesetz über den Militärischen Abschirmdienst* (MAD-Gesetz– MADG), 20 December 1990 (BGB1 I 1990, pp. 2954, 2977), as amended (*Military Counterintelligence Service Act*).

199 Rau report, p. 23, note 99.

200 *Military Counterintelligence Service Act*, § 1, para. 1(2). Cited in the Rau report, p. 23.

201 Ibid., § 1, para. 11.

202 Heyer, "Parliamentary Oversight," p. 11.

203 From the German *Bundesnachrichtendienst*.

204 Heyer, "Parliamentary Oversight," pp. 9, 27–28.

205 Ibid., p. 9.

206 *Gesetz über den Bundesnachrichtendienst* (BND-Gesetz), 20 December 1990 (BGB1 I S, pp. 2954, 2979) (*Federal Intelligence Service Act*).

207 See Lepsius, p. 451.

208 Heyer, "Parliamentary Oversight," p. 27.

209 *Counter-Terrorism Act*, §§ 1(3), 3. *Federal Intelligence Service Act*, § 3.

210 *Gesetz zur Beschränkung des Brief-, Post-, und Fernmeldegeheimnisses (G-10)*, 26 June 2001 (BGB1 I 2001, pp. 1254, 2298 (*The Act on Article 10 of the Basic Law*), Abs. 3 § 7 para. 2(1) [*G-10 Act*]. See the Rau report, p. 24.

211 Heyer, "Parliamentary Oversight," p. 10.

212 Ibid., p. 11.

213 *Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes* (Parlamentarisches Kontrollgremiumgesetz), 11 April 1978 (BGB1 I S 1978, p. 453) (*Parliamentary Control Panel Act*), as amended by the Act of 26 June 2001 (BGB1 I S 2001, p. 1254). For an overview of the rationale for creating a special panel of parliamentarians to review the activities of the intelligence services, see Heyer, "Parliamentary Oversight," pp. 12–13. The initialism "PKGr" is from the German *Parlamentarisches Kontrollgremium*.

214 *Parliamentary Control Panel Act*, § 1.

215 Heyer, "Parliamentary Oversight," p. 15.

216 *Parliamentary Control Panel Act*, § 2; Heyer, "Parliamentary Oversight".
217 Heyer, "Parliamentary Oversight," p. 16.
218 Ibid.
219 Ibid.
220 Heyer, "Parliamentary Oversight," p. 2; Lepsius, pp. 446–447.
221 Ibid.
222 Ibid.
223 For a detailed description of this process, see Heyer, "Parliamentary Oversight," p. 17.
224 German Bundestag, Secretariat of the Parliamentary Control Commission (PKGr), "Parliamentary Control of the Intelligence Services in Germany," pp. 17–19; Heyer, "Parliamentary Oversight," pp. 15–20.
225 *Infra* note 278.
226 Heyer, "Parliamentary Oversight," p. 28.
227 Ibid., p. 17.
228 Heyer, "Parliamentary Oversight," pp. 21–22; "Parliamentary Control of the Intelligence Services in Germany," pp. 17–19.
229 Ibid.
230 Interim European Security and Defence Assembly, "Parliamentary oversight."
231 Heyer, "Parliamentary Oversight," p. 17.
232 Ibid., pp. 7, 21.
233 Ibid., p. 16.
234 Ibid.
235 Ibid., p. 17.
236 Ibid., p. 18.
237 Interim European Security and Defence Assembly, "Parliamentary oversight"; *2003 Annual Report of the Office for the Protection of the Constitution*, p. 15.
238 "Parliamentary Control of the Intelligence Services in Germany", p. 22; Heyer, "Parliamentary Oversight," p. 18.
239 Heyer, "Parliamentary Oversight," p. 18.
240 Ibid., p. 22.
241 "Parliamentary Control of the Intelligence Services in Germany," p. 2706.
242 Act of 9 January 2002 (Federal Law Gazette 1, p. 361).
243 Heyer, "Parliamentary Oversight," p. 20.
244 Lepsius, p. 448.
245 See note 242.
246 *Parliamentary Control Panel Act*, § 4; Heyer, "Parliamentary Oversight," p. 14.
247 *Parliamentary Control Panel Act*, § 4; Heyer, "Parliamentary Oversight," pp. 13–14. See also Interim European Security and Defence Assembly, "Parliamentary oversight."
248 Heyer, "Parliamentary Oversight," p. 14.
249 Ibid., p. 17.
250 *G-10 Act*.
251 Heyer, "Parliamentary Oversight," p. 27.
252 Heyer, "Parliamentary Oversight," p. 22. The statute is cited in "Parliamentary Control of the Intelligence Services in Germany," pp. 28–31. See also Interim European Security and Defence Assembly, "Parliamentary oversight"; and *Article 10 Law*, paras. 14–15, cited in Lepsius, "Liberty, Security, and Terrorism," p. 448. See also *The Basic Law*, art. 10(2).
253 Heyer, "Parliamentary Oversight," p. 29.
254 Lepsius, p. 448; Heyer, "Parliamentary Oversight," p. 29.
255 Heyer, "Parliamentary Oversight," p. 29.

256 Ibid., p. 28.

257 Ibid., p. 29.

258 Ibid., p. 30.

259 Ibid., p. 29.

260 Ibid., pp. 22, 28.

261 Ibid., p. 29. Note that in Germany, a student pursuing legal training will choose whether to train for judicial office or legal practice. Therefore, unlike common law nations, the judiciary is a separate stream of legal specialization in Germany.

262 See http://www.police.govt.nz/about/structure.php (accessed May 23, 2006). For an organizational chart of the New Zealand Police, see http://www.police.govt.nz/about/management-structure-2004.gif (accessed May 23, 2006).

263 *Police Act 1958* (N.Z.), 1958/109, 17 RS. See also Ministry of Justice, *Directory of Official Information 2003–2005 Published by the Ministry of Justice Pursuant to Part III, Section 20 of the Official Information Act 1982* (Wellington: Ministry of Justice, 2003), pp. 429–447, online, http://www.justice.govt.nz/pubs/reports/2003/DOI-03-05/directory-03-05.pdf (accessed May 23, 2006). New Zealand statutes are available online through the New Zealand Parliamentary Council Office at http://www.legislation.govt.nz/ (accessed May 23, 2006).

264 See http://www.police.govt.nz/service/counterterrorism (accessed May 23, 2006).

265 Ibid.

266 House of Representatives Foreign Affairs, Defence and Trade Committee, *Report on International Treaty Examination of the United Nations Convention Against Transnational Organised Crime, the Protocol to Prevent, Suppress and Punish Trafficking of Persons, Especially Women and Children, Supplementing the United Nations Convention Against Transnational Organised Crime and the Protocol Against the Smuggling of Migrants by Land, Sea and Air, Supplementing the United Nations Convention Against Transnational Organised Crime* (22 February 2002), para. 23(c), online, http://www.clerk.parliament.govt.nz/content/631/fdtetoctpsm.pdf (accessed May 23, 2006).

267 *New Zealand Security Intelligence Service Act 1969* (N.Z.), 1989/119, 21 RS [*NZSIS Act*].

268 *NZSIS Act*, s. 4(1).

269 New Zealand Security Intelligence Service, *Report of the New Zealand Security Intelligence Service: Report to the House of Representatives for the year ended 30 June 2003*, p. 6, online, http://www.nzsis.govt.nz/publications/ar03/nzsis-ar03.pdf (accessed May 23, 2006).

270 *NZSIS Act*, ss. 4(2)ff.

271 *Government Communications Security Bureau Act 2003*, (N.Z.) 2003/009, s. 3(a) [*GCSB Act*].

272 *GCSB Act*, s. 8(1)(a)–(d).

273 The Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet, "Securing Our Nation's Safety: How New Zealand manages its security and intelligence agencies" (Wellington: The Domestic and External Security Secretariat, December 2000), p. 27.

274 Inspector-General of Intelligence and Security, *Annual Report of the Inspector-General of Intelligence and Security for the year ending June 1999*, pp. 9–10, cited in The Domestic and External Security Secretariat, "Securing Our Nation's Safety: How New Zealand manages its security and intelligence agencies," pp. 27–28.

275 *GCSB Act*, ss. 11, 14–17, 19, 22–25.

276 Complaints regarding the Immigration and Customs services are handled by New Zealand's Parliamentary Ombudsman: *Ombudsmen Act 1975*, Schedule I. For more information on the New Zealand Parliamentary Ombudsman, see the Ombudsman's website at http://www.ombudsmen.govt.nz (accessed May 23, 2006).

277 *Police Complaints Authority Act 1988* (N.Z.), 1988/002, s. 12(1)(a)(ii).

278 Ibid., ss. 27(1), 28(1).

279 Ibid., s. 12(1)(b).

280 Ibid., ss. 17, 18, 19. The Authority appears to have had the Police investigate complaints in the past, having hired its own investigators late in 2003: Louisa Cleave, "Workload surge taxes watchdog," *The New Zealand Herald*, October 1, 2004, online, http://www.nzherald.co.nz/storyprint.cfm?storyID=3594659 (accessed May 23, 2006).

281 *Police Complaints Authority Act 1988*, s. 21(1).

282 Ibid., ss. 24(1), (2).

283 Ibid., ss. 26(1).

284 Ibid., ss. 27(2), 28(2).

285 Ibid., ss. 29(1).

286 Ibid., ss. 30.

287 Ibid., ss. 29(2), (3).

288 bid., ss. 35(1), (2).

289 *Police Complaints Authority Act 1988*, ss. 34(1), (2). The public release of decisions is "relatively rare": Law and Order Select Committee, "Independent Police Complaints Authority Amendment Bill: Commentary," Presented to the House of Representatives on 17 November 2003, Office of the Clerk of the House of Representatives, p. 8, online, http://www.clerk.parliament.govt.nz/Content/SelectCommitteeReports/18bar2.pdf (accessed May 23, 2006).

290 *Police Complaints Authority Act 1988*, s. 5(1).

291 Ibid., s. 4(2).

292 Ibid., s. 4(3).

293 The Honourable Sir Rodney Gallen, *Review of the Police Complaints Authority* (Wellington: Ministry of Justice, October 2000), online, http://www.justice.govt.nz/pubs/reports/2001/police_complaints/review_of_pca.doc (accessed May 23, 2006).

294 Law and Order Select Committee, "Independent Police Complaints Authority Amendment: Commentary," p. 2.

295 Ibid.

296 Ibid., pp. 8–9.

297 See "Related information and links: Police under Investigation," *The New Zealand Herald* (February 3, 2004), online, http://www.nzherald.co.nz/storyprint.cfm?storyID=3547492 (accessed May 23, 2006); Cleave, "Workload surge taxes watchdog"; *Police Complaints Authority (Commission of Inquiry into Police Conduct) Act 2004*.

298 *Inspector-General of Intelligence and Security Act 1996* (N.Z.), 1996/47, s. 4.

299 Ibid., ss. 11, 19.

300 Ibid., s. 11(3).

301 Ibid., s. 11(4).

302 Ibid., ss. 19(3), 23(2).

303 Ibid., s. 19(5).

304 Ibid., s. 21.

305 Ibid., s. 20(1).

306 Ibid., s. 26(3).

307 Ibid., s. 25(1).

308 Ibid., s. 25(2).

309 Ibid., s. 25(5).

310 Ibid., s. 27(1).

311 Ibid., ss. 27(3), (4).

312 Ibid., s. 5(2).

313 Ibid., s. 5(3).

314 Ibid., s. 6(1).

315 Norway, Official Site in the U.K., "General info," online, http://www.norway.org.uk/facts/political/general/general.htm (accessed May 23, 2006). See also the Norway government's information site in English, online, http://www.odin.dep.no/odin/english/bn.html (accessed May 23, 2006); Statewatch, "Norway: police and security agencies," online, http://www.poptel.org.uk/cgi-bin/dbs2/statewatch?query=Norway&mode=records&row_id=18406 (accessed May 23, 2006); and U.S. Department of State, Background Note: Norway, online, http://www.state.gov/r/pa/ei/bgn/3421.htm (accessed May 23, 2006).

316 Fredrik Sejersted, "Intelligence and Accountability in a State without Enemies: The Case of Norway," in Hans Born, Loch Johnson and Ian Leigh, eds., *Who's Watching the Spies? Establishing Intelligence Service Accountability* (Washington, DC: Potomac Books, Inc., 2005), pp. 121–122 [Sejersted, "Intelligence and Accountability"].

317 Translation of the Norwegian name *Utvalget for kontroll med etterretnings-, overvåknings- og sikkerhetstjeneste*, provided by the Committee. The Committee advises that it uses the word "Parliamentary" to clarify that the committee is a parliament-appointed review body for the legislative branch. Note that the use of this name in this report differs from the names used in previous Policy Review publications. The abbreviated English name of the Committee remains the same, however: the EOS Committee, an acronym for the words in its Norwegian title, *etterretnings-, overvåknings- og sikkerhetstjeneste*.

318 Ministry of Justice and the Police, "Statement on Safety and Security of Society," Report no. 17 to the Storting (2001–2002), p. 2, online, http://www.odin.dep.no/jd/english/doc/white_paper/012101-040002/dok-bn.html (accessed May 23, 2006).

319 Ibid., p. 3.

320 Lillian Røstad and Maria Bartnes Dahl, Centre for Information Security, "Experiences from establishing a national Centre for Information Security in Norway," online, http://www.terena.nl/conferences/tnc2003/programme/papers/p1c1.pdf (accessed May 23, 2006).

321 National Police Directorate, "The National Police Directorate — and a Short Introduction to the Police in Norway," online, http://www.straffet.com/eng/eng_pdf/NPD.pdf (accessed May 23, 2006) [National Police Directorate, "Introduction"].

322 *Police Act*, no. 53 of 4 August 1995. English version, without subsequent amendments, online, http://www.ub.uio.no/ujur/ulov/english.html (accessed May 23, 2006).

323 National Police Directorate, "Introduction."

324 *Police Act*, para. 17b, no. 5.

325 This was done by an amendment to the *Police Act*, no. 53 of 4 August 1995, adding ss. 17a, 17b and 17c. See Fredrik Sejersted, "Intelligence Oversight in Norway" (Geneva Centre for the Democratic Control of Armed Forces: 2003), p. 7 [Sejersted, "Intelligence Oversight"].

326 Sejersted, "Intelligence and Accountability" p. 123.

327 National Police Directorate, "Introduction."

328 See Leif Mevik, Chair of the Intelligence Oversight Committee, "Parliamentary Oversight of the Intelligence Services: The Norwegian Experience" (Paper presented at the Workshop on the Handbook on "Parliamentary Oversight of the Security Sector," Bucharest, Romania, March 29–30, 2004, organized by the Geneva Centre for the Democratic Control of Armed Forces, and the Romanian Parliament), p. 3, online, http://www.dcaf.ch/oversight/ev_bucharest_040329Mevik.pdf), in which it is noted that the Security Service receives the greatest number of inspections (per the *Instructions for Monitoring of Intelligence, Surveillance and Security Services*) (accessed May 23, 2006) [Mevik, "Parliamentary Oversight"]; and Sejersted, "Intelligence and Accountability," p. 134, in which the author notes that the Police Security Service generates the most complaints.

329 Sejersted, "Intelligence and Accountability, p. 121.

330 *Act relating to the Norwegian Intelligence Service*, 20 March 1998, s. 3, online, http://www.ub.uio.no/ujur/ulovdata/lov-19980320-011-eng.pdf (accessed May 24, 2006) [*Intelligence Service Act*].

331 Ibid.

332 Ibid., s. 4.

333 Sejersted, "Intelligence and Accountability," p. 121; *Intelligence Service Act*, s. 2.

334 Sejersted, "Intelligence and Accountability," p. 121.

335 *Act relating to Protective Security Services*, no. 10 of 20 March 1998, s. 8 [*Security Act*].

336 See http://www.nationmaster.com/encyclopedia/Nasjonal-Sikkerhetsmyndighet (accessed May 24, 2006).

337 Sejersted, "Intelligence and Accountability," p. 122.

338 Ibid.

339 *Security Act*, s. 10.

340 *Security Act*, which came into force in 2001. See Sejersted, "Intelligence Oversight," p. 7.

341 Sejersted, "Intelligence and Accountability," p. 122.

342 Sejersted, "Intelligence Oversight," p. 46. See also Ministry of Justice and the Police, "Statement on Safety and Security of Society," (2001–2002), p. 4.

343 Sejersted, "Intelligence Oversight," p. 46.

344 *Act concerning the Storting's Ombudsman for Public Administration*, no. 8 of 22 June 1962, s. 4; *Directive to the Storting's Ombudsman for Public Administration*, 19 February 1980, s. 2; Office of the Parliamentary Ombudsman for Public Administration, *The Parliamentary Ombudsman for Public Administration — Norway, Annual Report 2004*, *Summary in English*, Appendix 1, online, The Parliamentary Ombudsman, http://www.sivilombudsmannen.no/eng/index.php?12 (accessed May 24, 2006).

345 *Directive to the Storting's Ombudsman for Public Administration* (1980), s. 2. For more information on the Norwegian Parliamentary Ombudsman, see the Ombudsman's website, online, http://www.sivilombudsmannen.no/eng/index.php?32 (accessed May 24, 2006).

346 *Act relating to the Monitoring of Intelligence, Surveillance and Security Services*, no. 7 of 3 February 1995, ss. 1, 3 [*Intelligence Monitoring Act*]. See also Sejersted, "Intelligence and Accountability," pp. 124–125.

347 Sejersted, "Intelligence and Accountability," pp. 124–25.

348 Fredrik Sejersted has noted that the issue is "growing" as co-operation among domestic agencies increases. He notes that the EOS Committee is "keeping its eye on" the coordinated efforts of the Police Security Service and the economic crimes unit of the ordinary police, as well as the coordination between the Police Security Service and immigration authorities. See Sejersted, "Intelligence Oversight," p. 13, note 12.

349 In Norway, this issue is complicated by the fact that the economic crimes unit forms part of the superior prosecution body, which is exempt from oversight by the EOS Committee. The discussion is at section 2 of the Committee's 2003 annual report, but the report is available in Norwegian only.

350 *Intelligence Monitoring Act*, s. 3, para. 3.

351 Until January 1, 2005, this body was SEFO (the Norwegian acronym for the Special Investigating Body for Police Matters). As of January 1, 2005, complaints against the police are handled by a new agency called the *Spesilaenheten for politisaker* — the Special Unit for Police Matters. In contrast to SEFO, this new body is external to the police.

352 See discussion above.

353 *Intelligence Monitoring Act*, s. 2.

354 *Instructions for Monitoring of Intelligence, Surveillance and Security Services (EOS)*, issued pursuant to s. 1 of Act No. 7 of 3 February 1995 relating to the Monitoring of Intelligence, Surveillance and Security Services, s. 11 [*Instructions*].

355 *Intelligence Monitoring Act*, s. 2.
356 Ibid., s. 3.
357 Ibid., s. 2.
358 Sejersted, "Intelligence and Accountability," p. 133. Sejersted also discusses the "grey zone between consultations and discussions" and the fact that "the principle of retrospective oversight is difficult to maintain fully when it comes to operations that run for some period of time." See also Sejersted, "Intelligence Oversight," pp. 30ff.
359 *Intelligence Monitoring Act*, ss. 4, 5; *Instructions*, s. 6.
360 *Intelligence Monitoring Act*, s. 3.
361 *Instructions*, s. 10.
362 Mevik, "Parliamentary Oversight," p. 4.
363 *Intelligence Monitoring Act*, s. 2.
364 According to the EOS Committee, the *Intelligence Monitoring Act*, s. 2, presupposes that the Committee cannot make binding decisions. See also the *Instructions*, s. 7.
365 *Instructions*, s. 8.
366 *Intelligence Monitoring Act*, s. 8.
367 Ibid.
368 *Instructions*, s. 13.
369 *Intelligence Monitoring Act*, s. 8.
370 *Instructions*, s. 1.
371 Sejersted, "Intelligence and Accountability," p. 127.
372 *Intelligence Monitoring Act*, s. 9.
373 See http://www.sweden.se/templates/cs/CommonPage___3752.aspx (accessed May 24, 2006).
374 Ordinance (2003:148).
375 Ordinance (2003:1156).
376 Swedish Helsinki Committee for Human Rights, *Annual Report 2003*, p. 9.
377 Swedish Security Service, *Annual Report 2003*, p. 2, online, http://www.securityservice.se/Publikationer/annual03.pdf (accessed May 24, 2006).
378 Ann-Louise Eksborg, Director-General, Swedish Emergency Management Agency, "The Swedish Emergency Management Agency: Experiences and Conclusions after Two Years," p. 1, online, http://www.krisberedskapsmyndigheten.se/3673.epibrw (accessed May 24, 2006) [Eksborg, "Swedish Emergency Management Agency"].
379 Ibid., p. 2.
380 See National Police Board, "Polis: A presentation of The Swedish Police Service," online, http://www.polisen.se/inter/mediacache//4347/4637/Polis_05_eng.pdf (accessed May 24, 2006) [National Police Board, "Polis"]. For more information on the national police service, see National Police Board, "The Police Act with commentary" (Stockholm: Swedish National Police Board, 1999), online, http://www.polisen.se/inter/mediacache//4347/4734/2671/policeact_pdf.pdf (accessed May 24, 2006) [National Police Board, "Police Act"].
381 See National Police Board, "Police Act."
382 See http://www.polisen.se/inter/nodeid=10232&pageversion=1.html; and National Police Board, "Polis."
383 Ordinances (1989:773) containing instructions to the National Police Board; and (2002:1050) containing instructions to the Security Service. See also Swedish Security Service, *Annual Report 2002*, p. 5, online, Swedish Security Service, http://www.securityservice.se/Publikationer/annual02.pdf (accessed May 24, 2006).
384 National Police Board, "Polis," p. 23.
385 Ibid.

386 Swedish Security Service, *Annual Report 2003*, p. 6. See also Swedish Security Service, *Annual Report 2002*, online, http://www.securityservice.se/ (accessed May 25, 2006).

387 Swedish Security Service, *Annual Report 2003*, p. 3.

388 *Defence Intelligence Activity Act* (2000:131); Related ordinance (2000:131).

389 Translation of the Swedish *Försvarets Radioanstalt*, on which the initialism is based.

390 *Edict with Instructions for the National Defence Radio Centre* (1994:714) (*Förordning (1994:714) med instruktion för Försvarets radioanstalt*). The statute is available online in Swedish only on the National Defence Radio Centre website at http://www.fra.se/rixlex/1994-714.htm (accessed May 25, 2006).

391 Eksborg, "Swedish Emergency Management Agency," p. 3.

392 *The Act with Instructions for the Parliamentary Ombudsmen* (1986:765), art. 2, online, http://www.jo.se/Page.asp?MenuId=37&MainMenuId=12&ObjectClass=DynamX_Document&Id=575&Language=en (accessed May 25, 2006) [*Act with Instructions*]. See also the summary in English at the end of the Parliamentary Ombudsmen's *Report for the period 1 July 2000 to 30 June 2001*, online, http://www.riksdagen.se/debatt/0001/forslag/jo1/jo1.pdf (accessed May 25, 2006). Note that jurisdiction over "the armed forces . . . extends only to commissioned officers with the rank of second lieutenant or above, and to those of corresponding rank": *Act with Instructions*, art. 2.

393 National Police Board, "Polis," p. 5.

394 The Ombudsmen do not have jurisdiction over elected officials or members of policy-making municipal bodies, the parliamentary administration, or the governing board of the National Bank of Sweden: *Act with Instructions*, art. 2.

395 The reason for this division is largely historic. There used to be one ombudsman for all public authorities except the military, and another ombudsman for the military. The functions of the Military Ombudsman have now been incorporated into the Parliamentary Ombudsmen's office, but a separation of responsibilities has been maintained. See The Swedish Parliamentary Ombudsmen, *Report for the Period 1 July 2003 to 30 June 2004* (Stockholm: Elanders Gotab, 2004), p. 483, online, The Swedish Parliamentary Ombudsmen, http://www.riksdagen.se/srvfunc/dokarkiv/0405/bet/JO1.PDF (accessed May 25, 2006).

396 Swedish Parliamentary Ombudsmen, *Report for the Period 1 July 2003 to 30 June 2004*, p. 483.

397 Ibid., p. 516. A fourth Ombudsman is responsible for the fields of social welfare, public health, and medical care and education.

398 Parliamentary Ombudsmen, "General Information," online, http://www.jo.se/Page.aspx?MenuId=12&ObjectClass=DynamX_Documents&Language+en (accessed May 25, 2006). See the *Act with Instructions*, ss. 1, 3.

399 *Act with Instructions*, s. 5.

400 Ibid., s. 4.

401 Ibid., s. 18.

402 Due to the generalist nature, supervisory structure and small size of the Office of the Ombudsmen, individuals often use other complaints or resolution mechanisms before approaching it. In addition, the Ombudsmen have the power to refer complaints to other "appropriate" authorities for resolution: *Act with Instructions*, s. 18. In some cases the Ombudsmen's office asks to be informed of the outcome of such referrals.

403 The Ombudsmen's office has 55 employees, 30 of whom are lawyers. The office received approximately 5,100 complaints last year. For a discussion of the volume of complaints in the Ombudsmen's office, see B. Wieslander, *The Parliamentary Ombudsman in Sweden,* 2nd revised ed. (The Bank of Sweden Tercentenary Foundation: 1999), pp. 49–59.

404 The most recent of these was an investigation into the execution by the Security Police of an order by the Swedish government to deport two Egyptian citizens. The investigation was

completed in March, 2005. See http://www.jo.se/Page.aspx?MenuId=106&MainMenuId=106&Language=en&ObjectClass=DynamX_DocumentSFS_Decision&Id=16251662 (accessed May 25, 2006).

405 *The Instrument of Government* (1974:152), ch. 12, art. 6, online, http://www.jo.se/Page.asp?MenuId=37&MainMenuId=12&Language=en&ObjectClass=DynamX_Documents&Id=571 (accessed May 25, 2006).

406 *Act with Instructions*, art. 6.

407 Ibid., s. 21. The Office of the Parliamentary Ombudsmen advises that this power has never been used.

408 For example, in its 2000–2001 annual report, the Parliamentary Ombudsmen found that a police official had had "no basis in law" for issuing a warrant for a vehicle search. See Parliamentary Ombudsmen's Report for the period 1 July 2000 to 30 June 2001, pp. 546–47.

409 *The Instrument of Government*, ch. 12, art. 6. Any public prosecutor shall assist the Ombudsman upon request. According to the Ombudsmen's website, this power is rarely used.

410 Parliamentary Ombudsmen, "Powers and Sanctions," online, http://www.jo.se/Page.aspx?MenuId=23&MainMenuId=12&ObjectClass=DynamX_Documents&SetLanguage=en (accessed May 25, 2006). See also *Act with Instructions*, arts. 3ff.

411 Parliamentary Ombudsmen, "General Information."

412 *Riksdag Act*, ch. 8, art. 11, online, http://www.jo.se/Page.asp?MenuId=37&MainMenuId=12&ObjectClass=DynamX_Document&Id=573 (accessed May 25, 2006).

413 *Terrorism Act 2000* (U.K.), 2000, c. 11; *Anti-terrorism, Crime and Security Act 2001* (U.K), 2001, c. 24; *Prevention of Terrorism Act 2005* (U.K.), 2005, c. 2; *Serious Organised Crime and Police Act 2005* (U.K.), 2005, c. 15; *Terrorism Act 2006* (U.K.), 2006, c. 11.

414 *Regulation of Investigatory Powers Act 2000* (U.K.), 2000, c. 23 [*RIPA*].

415 *Police Reform Act 2002* (U.K.), 2002, c. 30. See also the website of the Secretary of State for the Home Department [the Home Office], online, http://www.homeoffice.gov.uk (accessed May 25, 2006); and the *Serious Organised Crime and Police Act 2005*. The Serious Organised Crime Agency (SOCA) established by this Act assumed its duties on April 1, 2006: *Serious Organised Crime and Police Act 2005*, ss. 1–59.

416 *Police (Northern Ireland) Act 1998* (U.K.), 1998, c. 32.

417 The *Police Reform Act 2002*, created the Independent Police Complaints Commission for England and Wales. See also http://www.ipcc.gov.uk/ (accessed May 25, 2006).

418 See the Home Office, "Counter-Terrorism & Resilience: Key Facts," September 2004, online, http://www.homeoffice.gov.uk/docs3/terrorism_keyfacts.pdf (accessed May 25, 2006).

419 See for example Lord Carlile of Berriew Q.C. (independent reviewer of the *Terrorism Act 2000*), "Report on the Operation in 2002 and 2003 of the Terrorism Act 2000"), online, http://security.homeoffice.gov.uk/news-and-publications1/publication-search/independent-reviews/TerrorismAct_ rpt1.pdf?view=Binary (accessed May 25, 2006); and Lord Carlile of Berriew Q.C, "Anti-terrorism, Crime and Security Act 2001, Part IV, Section 28: Review 2003," online, http://security.homeoffice.gov.uk/news-and-publications1/publication-search/independent-reviews/atcsa-review-part7.pdf?view=Binary (accessed May 25, 2006). For a listing of independent reviews of terrorism legislation, see online, http://security.homeoffice.gov.uk/news-and-publications1/publication-search/independent-reviews/ (accessed May 25, 2006).

420 See for example the Home Office, "Counter-Terrorism Powers: Reconciling Security and Liberty in an Open Society: A Discussion Paper," presented to the U.K. Parliament February 2004, online, http://security.homeoffice.gov.uk/news-and-publications1/publication-search/general/ct-discussion?view=Binary (accessed May 25, 2006).

421 The U.K. does, however, have certain national forces with specific mandates. For example, the National Crime Squad (NCS) and the National Criminal Intelligence Service (NCIS) focus on law enforcement and intelligence collection, respectively, in the area of organized crime. See *Police Act 1997* (U.K.), 1997, c. 50. See also http://www.nationalcrimesquad.police.uk/ (accessed May 25, 2006) and http://www.ncis.co.uk/ (accessed May 25, 2006). As I describe in Section 8.2.4 of this chapter, on April 1, 2006, the U.K. government merged the NCS and the NCIS, together with certain governmental investigative and intelligence sections, in the new Serious Organised Crime Agency. See also the Home Office, "One Step Ahead: A 21st Century Strategy to Defeat Organised Crime" (Crown: March 2004), also known as the "Organised Crime White Paper." Available online at http://www.homeoffice.gov.uk/documents/cons-organised-crime-300704/organised-crime-300704?view=Binary (accessed May 25, 2006). Other examples include the British Transport Police, the U.K. Atomic Energy Authority Constabulary and the Royal Parks Constabulary.

422 For a list of U.K. local police forces, non-geographic police forces, and related agencies and links, see http://www.police.uk/ (accessed May 25, 2006).

423 Note that the Metropolitan Police Special Branch will soon be amalgamated with its Anti-Terrorist Branch. See note 431 below.

424 See *RIPA* and discussion below.

425 See http://www.police.uk/ (accessed May 25, 2006).

426 See http://www.psni.police.uk/ (accessed May 25, 2006).

427 See http://www.scotland.gov.uk/library/documents/police.htm (accessed May 25, 2006).

428 See note 421.

429 See the Policing Plans and other publications of the various forces, which can be accessed via the http://www.police.uk/ portal (accessed May 25, 2006).

430 See the Metropolitan Police Service's website, Anti-Terrorist Branch, online, http://www.met.police.uk/terrorism/index.htm (accessed May 25, 2006). The Metropolitan also appears to receive the bulk of the government's funding to police for counter-terrorism. See for example the Home Office press release, "Government Steps up its Fight Against Terrorism . . . ," dated March 19, 2004, online, http://press.homeoffice.gov.uk/press-releases/Government_Steps_Up_Its_Fight_Ag?version=1 (accessed May 25, 2006) and "Budget Boost to Regions for Street Crime, Counter-terrorism . . . ," dated May 1, 2002, online, http://www.policesupers.com/police-supers-news.asp?news_id=94 (accessed May 25, 2006). See also "Terrorism – Policing the Unknown," a speech by Home Office representative Leigh Lewis to the Police Federation Annual Conference, May 20, 2004, online, http://security.homeoffice.gov.uk/news-and-publications1/speeches-statement/Speech_policing_the_unknown1.pdf?view=Binary (accessed May 25, 2006).

431 Her Majesty's Inspector of Constabulary, "A Need to Know: HMIC Thematic Inspection of Special Branch and Ports Policing" (Home Office Communications Directorate: January 2003), p. 10. It appears that the Metropolitan Police Special Branch will be amalgamated with the Anti-Terrorist Branch to form a single anti-terrorism directorate: see the Statement by Sir Ian Blair, Metropolitan Police Commissioner, reported at "End for Special Branch After 122 Years," *The Daily Telegraph* (September 9, 2005), online, Telegraph.co.uk, http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2005/09/09/nspecials09.xml&sSheet=/news/2005/09/09/ixhome.html (accessed May 25, 2006); "End of the Road for Special Branch," *The Guardian* (September 9, 2005), online, *The Guardian,* http://www.guardian.co.uk/crime/article/0,2763,1566085,00.html (accessed May 25, 2006); "Special Branch to Close in Merger," *BBC News* (September 9, 2005), online, BBC News, http://news.bbc.co.uk/2/hi/uk_news/4227476.stm (accessed May 25, 2006).

[432] Home Office, Scottish Executive and Northern Ireland Office, "Guidelines on Special Branch Work in the United Kingdom" (Home Office, Communications Directorate: March 2004), p. 6, online, http://www.scotland.gov.uk/Resource/Doc/47171/0025036.pdf (accessed May 25, 2006) [Home Office, "Guidelines"].

[433] Ibid., p. 2. This statement of the Special Branch's function appears to differ from the statement set out in the 1994 Guidelines, which provided that the role of Special Branch was "to gather intelligence to meet national security requirements as well as to support other policing priorities such as the prevention of disorder." See Her Majesty's Inspector of Constabulary, "A Need to Know: HMIC Thematic Inspection of Special Branch and Ports Policing" (Home Office Communications Directorate: January 2003), p. 10. It may be relevant that in this report, the HMIC found that "the role and responsibilities of Special Branch are unclear; the 1994 guidelines do not reflect the changed environment . . . . HMIC recommends that the Home Office review and update the current Guidelines in order to clarify the role of Special Branch thereby formalising its remit and priorities within the national security arena" (p. 13). More research will be required on the precise nature of the Special Branch activities.

[434] Home Office, "Guidelines," p. 2.

[435] Ibid., Foreword.

[436] Ibid., p. 6 and Foreword.

[437] Ibid., Foreword.

[438] "About PSNI," Police Service of Northern Ireland, online, http://www.psni.police.uk/index/about_psni.htm (accessed May 25, 2006). Independent Commission on Policing in Northern Ireland, *A New Beginning: Policing in Northern Ireland, The Report of the Independent Commission on Policing for Northern Ireland* (Norwich: The Copyright Unit, 1999), online, Independent Commission on Policing for Northern Ireland, http://www.belfast.org.uk/report/fullreport.pdf (accessed May 25, 2006) [Report of the Independent Commission on Policing for Northern Ireland].

[439] The RUC's involvement in anti-terrorism policing is reviewed and analyzed in the Report of the Independent Commission on Policing for Northern Ireland, esp. Ch. 1.

[440] U.K., Home Office, Serious Organised Crime Agency, *SOCA Annual Plan, 2006/7*, p. 6, online, Serious Organised Crime Agency, http://www.soca.gov.uk/downloads/annualPlan.pdf (accessed May 25, 2006) [*SOCA Annual Plan*].

[441] *Serious Organised Crime and Police Act 2005*.

[442] *SOCA Annual Plan*, p. 6.

[443] Ibid., p. 7.

[444] For more information on this aspect of SOCA's activities, see the SOCA website at http://www.soca.gov.uk/financialIntel/index.html (accessed May 25, 2006). See also Sir Stephen Lander, SOCA, *Review of the Suspicious Activity Reports Regime (SAR Review)*, March 2006, online, SOCA, http://www.soca.gov.uk/downloads/SOCAtheSARsReview_FINAL_Web.pdf (accessed May 25, 2006). In Canada, this role is filled by the Financial Transactions and Reports Analysis Centre (FINTRAC), which I discuss in Chapter V.

[445] *SOCA Annual Plan*, pp. 7–8

[446] *Serious Organised Crime and Police Act 2005*, s. 5.

[447] See, for example, U.K., Home Office, "The introduction of oversight by the Independent Police Complaints Commission (IPCC) of certain functions of Immigration Officers (IOs), in England and Wales Regulatory Impact Assessment," (2006), p. 5, online, Home Office Police, http://police.homeoffice.gov.uk/news-and-publications/publication/police-reform/RIA-IPCC_v5.pdf?view=Binary (accessed May 25, 2006) [Home Office, "Introduction of oversight"].

448 *SOCA Annual Plan*, p. 8. See also SOCA FAQs, online, SOCA http://www.soca.gov.uk/faqs/index.html (accessed May 25, 2006).

449 *SOCA Annual Plan*, p. 7.

450 See the *Security Service Act 1989* (U.K.), 1989, c. 5; http://www.mi5.gov.uk/ (accessed May 25, 2006); and U.K., "National Intelligence Machinery" (Crown: September 2001), online, http://www.archive.official documents.co.uk/document/caboff/nim/0114301808.pdf (accessed May 25, 2006).

451 *Security Service Act 1989*, s. 1; *Security Service Act 1996* (U.K.), 1996, c. 35, s. 1.

452 http://www.mi5.gov.uk/output/Page77.html (accessed May 25, 2006).

453 *Security Service Act 1989*, s. 2.

454 *Security Service Act 1989*.

455 See the *Intelligence Services Act 1994* (U.K.), 1994, c. 13, online, http://www.opsi.gov.uk/acts/acts1994/Ukpga_19940013_en_1.htm (accessed May 25, 2006); and U.K., "National Intelligence Machinery" (Crown: September 2001), online, http://www.archive.official-documents.co.uk/document/caboff/nim/0114301808.pdf (accessed May 25, 2006).

456 *Intelligence Services Act 1994*, s. 1.

457 *Intelligence Services Act 1994*.

458 See the *Intelligence Services Act 1994*; http://www.gchq.gov.uk/ (accessed May 25, 2006); and U.K., "National Intelligence Machinery" (Crown: September 2001), online, http://www.archive.official-documents.co.uk/document/caboff/nim/0114301808.pdf (accessed May 25, 2006).

459 *Intelligence Services Act 1994*, s. 3.

460 *Intelligence Services Act 1994*.

461 U.K., "National Intelligence Machinery."

462 However, a complainant who is dissatisfied with the results of an investigation can write to Her Majesty's Inspectorate of Constabulary for Scotland (discussed below), which reviews the investigation and may request a reconsideration by the police. See Her Majesty's Inspectorate of Constabulary for Scotland, "The Role of HMIC in Police Complaints," online, http://www.scotland.gov.uk/Topics/Justice/Police/15403/2065 (accessed May 25, 2006).

463 See Scottish Executive, News Release, "Next steps on police complaints" (June 24, 2004), online, http://www.scotland.gov.uk/News/Releases/2004/06/5702 (accessed May 25, 2006); and Scottish Executive, "Complaints Against the Police in Scotland: A Consultation Paper," online, http://www.scotland.gov.uk/consultations/justice/caps.pdf (accessed May 25, 2006).

464 The Independent Police Complaints Commission replaced the Police Complaints Authority on April 1, 2004. See the *Police Reform Act 2002*, ss. 9ff.; and http://www.ipcc.gov.uk (accessed May 25, 2006).

465 The *Commissioners for Revenue and Customs Act 2005* (U.K.), 2005, c. 11 [*Revenue and Customs Act*] combines the Inland Revenue, and Customs and Excise departments into a single department called Her Majesty's Revenue and Customs [HMRC]. Pursuant to the *Revenue and Customs (Complaints and Misconduct) Regulations 2005*, (U.K.) S.I. 2005/331, published under s. 28 of the *Commissioners for Revenue and Customs Act*, the IPCC has jurisdiction over certain aspects of the HMRC's activities.

466 Bill 119, Police and Justice Bill (U.K.), 2006–2007 Sess., 2006, s. 38 (1st reading 25 January 2006), online, http://www.publications.parliament.uk/pa/cm200506/cmbills/119/2006119.htm (accessed May 26, 2006) [Bill 119, 2006]. More information on the proposal is available in Bill 119-EN, "Explanatory Notes" (U.K.), 2006, online, http://www.publications.parliament.uk/pa/cm200506/cmbills/119/en/06119x--.htm (accessed May 26, 2006); and in the Home Office Regulatory Impact Assessment" Introduction of oversight."

467 Bill 119, 2006, s. 38(2). The Prisons and Probation Ombudsman, not the IPCC, has jurisdiction over conditions of detention in immigration holding facilities: Bill 119, 2006, s. 38(3).

468 Her Majesty's Customs and Revenue Department has both Customs and Inland Revenue functions. The IPCC's jurisdiction does not extend, for example, to taxpayer complaints.

469 This jurisdiction includes the Special Branches, though as noted above, this proposition has not been tested yet, and much of their work would be subject to *RIPA* scrutiny.

470 There is statutory authority behind this agreement, insomuch as the IPCC can "call in" complaints or other matters for investigation by the IPCC: *Police Reform Act 2002*, Schedule 3, s. 4(1)(c). Rather than the IPCC calling in all such complaints individually, the police forces have agreed to simply refer all complaints regarding the use of anti-terrorism powers.

471 The Department for Constitutional Affairs defines a "statutory gateway" as an "express statutory power to share personal data whether permissive or mandatory." See "Public Sector Data Sharing – A guide to Data Sharing Protocols," November 2003, online, http://www.dca.gov.uk/foi/sharing/toolkit/infosharing.htm (accessed May 25, 2006).

472 See note 465.

473 *Revenue and Customs Act*, ss. 28(3)–(4). The Regulations are available online at http://www.opsi.gov.uk/si/si2005/20053311.htm (accessed May 26, 2006).

474 Bill 119, 2006, ss. 38(5), 38(6). The official name of the Parliamentary Ombudsman is the Parliamentary Commissioner for Administration. The Commissioner has a statutory basis under the *Parliamentary Commissioner Act 1967* (U.K.), 1967, c. 13, and the *Parliamentary Commissioner Act 1994* (U.K.), 1994, c. 14.

475 See http://www.dca.gov.uk/foi/sharing/toolkit/infosharing.htm (accessed May 26, 2006); and http://www.dca.gov.uk/foi/sharing/toolkit/lawguide.htm#part3 (accessed May 26, 2006).

476 *Police Reform Act 2002*, s. 10.

477 Ibid., s. 10(2)(b), Schedule 3, Parts 2, 3.

478 Ibid., s. 10, Schedule 3, Parts 2, 3.

479 Ibid., s. 22.

480 *Police Reform Act 2002*, Schedule 3, ss. 6ff. See generally, Independent Police Complaints Commission (U.K.), *Making the New Police Complaints System Work Better: Statutory Guidance*, 2005, para. 5.4.13, online, http://www.ipcc.gov.uk/ (accessed May 26, 2006) [IPCC Statutory Guidance]. This statutory guidance was issued pursuant to the *Police Reform Act*, s. 22. The U.K.'s police forces are each subject to a Police Authority, which is charged with maintaining efficient and effective police forces for its respective policing area. See *Police Act* (U.K.), 1996, c. 16, ss. 3-0, 26.

481 *Police Reform Act 2002*, Schedule 3, s. 25. See generally, IPCC Statutory Guidance.

482 *The Police (Complaints and Misconduct) Regulations 2004* (U.K.), S.I. 2004/643, s. 16, online, http://www.opsi.gov.uk/si/si2004/20040643.htm#16 (accessed May 26, 2006); IPCC Statutory Guidance, para. 5.4.13.

483 IPCC Statutory Guidance, para. 5.4.13.

484 *Criminal Procedure and Investigations Act 1996* (U.K.), 1996, c. 25, s. 3; *Criminal Justice Act 2003* (U.K.), 2003, c. 44, s. 32.

485 *Criminal Procedure and Investigations Act 1996*.

486 U.K., Attorney General, *Attorney General's Guidelines on Disclosure*, para. 48, online, The Legal Secretariat to the Law Officers, http://www.lslo.gov.uk/pdf/disclosure.doc (accessed May 26, 2006) [Attorney General's Guidelines]; U.K., Crown Prosecution Service, *Crown Prosecution Service Disclosure Manual* (2005), Ch. 4, para. 27, online, The Crown Prosecution Service, http://www.cps.gov.uk/legal/section20/chapter_a.html#001 (accessed May 26, 2006) [Crown Prosecution Manual].

487 The Crown may apply to the Court for a witness summons under s. 97 of the *Magistrate's Court Act 1980* or in the *Crown court, section 2 Criminal Procedure (Attendance of Witnesses) Act 1965* as amended: Crown Prosecution Service Disclosure Manual, Ch. 4, para. 16; Attorney General's Guidelines on Disclosure, para. 52.

488 Attorney General's Guidelines, paras. 51–54; Crown Prosecution Manual, Ch. 4.

489 Crown Prosecution Manual, Ch. 4, para. 23.

490 *Police Reform Act 2002*, s.17.

491 Ibid., s. 18.

492 Ibid., Schedule 3, ss. 1, 12.

493 Ibid., s. 17.

494 *Police Reform Act 2002*, Schedule 3, Part 3; s. 10.

495 Ibid., ss. 23(2)(b)–(c).

496 Ibid., s. 11.

497 Ibid., Schedule 3, s. 22; s. 29.

498 Ibid., ss. 20, 21.

499 Ibid., Schedule 3, ss. 23, 25–28.

500 *Police Reform Act 2002*, s. 20(6); *The Police (Complaints and Misconduct) Regulations 2004* (U.K.), S.I. 2004/643, s. 12.

501 *Police Reform Act 2002*, s. 9.

502 Ibid., Schedule 2, s. 2.

503 Ibid., s. 9.

504 Ibid., Schedule 2, s. 2.

505 See *Police (Northern Ireland) Act 1998*, amended by the *Police (Northern Ireland) Act 2000* (U.K.), 2000, c. 32, and the *Police (Northern Ireland) Act 2003* (U.K.), 2003, c. 6.

506 *Revenue and Customs Act 2005*.

507 *Police (Northern Ireland) Act 1998*, ss. 50–56.

508 Ibid., s. 52(5).

509 *Police (Northern Ireland) Act 2003* (U.K.), s. 13.

510 *Police (Northern Ireland) Act 1998*, ss. 53–54.

511 Ibid., s. 57.

512 Ibid.

513 This practice is consistent with the *Criminal Procedure and Investigations Act 1996*. The Ombudsman's office is not formally bound by this statute, but states that it regards itself as being bound.

514 *Criminal Law Act (Northern Ireland) 1967* (U.K.), 1967, c. 18, s. 5.

515 *Police (Northern Ireland) Act 1998*, s. 55.

516 Ibid.

517 *Police (Northern Ireland) Act 2000*, s. 66.

518 See for example House of Commons Northern Ireland Affairs Committee, "The Functions of the Office of the Police Ombudsman for Northern Ireland," 23 February 2005, pp. 22–23.

519 *Police (Northern Ireland) Act 1998*, s. 56.

520 Ibid., s. 61.

521 Ibid., s. 62.

522 *Police (Northern Ireland) Act 2003*, s. 13.

523 *Police (Northern Ireland) Act 1998*, Schedule 3, s. 1.

524 Ibid.

525 *RIPA*. This *Act* applies to Northern Ireland as well, and includes the establishment of a Northern-Ireland-specific review body, the Investigatory Powers Commissioner for Northern Ireland. The Scottish Parliament passed its own similar law, the *Regulation of Investigatory Powers (Scotland) Act 2000*, A.S.P. 2000, c. 11.

526 For example, the use of certain "intrusive surveillance" methods are subject to different authorization regimes, depending on whether a police agency or an intelligence agency wishes to use the method: *RIPA*, ss. 32, 36, 41, 42.

527 See *RIPA*, Part I, Chapter I.

528 See *RIPA*, Part I, Chapter II.

529 See *RIPA*, parts II and IV. Note that the Office of the Surveillance Commissioners was created by the *Police Act 1997* rather than by *RIPA*, although *RIPA* effected some changes to its powers. For example, complaints are now handled by the IPT: *RIPA*, Part IV, ss. 65ff.

530 *RIPA*, Part III.

531 *RIPA*, Part IV, ss. 65ff.

532 A complete list of the public authorities that may seek covert surveillance authorizations is found in Schedule 1 of the *Regulation of Investigatory Powers Act 2000* (U.K.), and *The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003*, S.I. 2003/3171. The various acts and regulations governing covert surveillance activity in Great Britain are available online, Office of Surveillance Commissioners, http://www.surveillancecommissioners.gov.uk/index.html (accessed May 26, 2006).

533 The OSC advises that although it is empowered to carry out general inspection activity, it does not, as it asks all public authorities under its purview to provide detailed reports of any breaches in procedures.

534 *RIPA*, ss. 5ff.

535 For a detailed listing of the Interception of Communication Commissioner's mandate, see *RIPA*, ss. 57–58. See also the ICC's annual reports, found online at http://www.official-documents.co.uk/ (accessed May 26, 2006).

536 Annual Report of the Chief Surveillance Commissioner, 2000–2001, p. 5.

537 *RIPA*, ss. 57(3), 59(3), 68(2), 68(8).

538 *RIPA*, ss. 40, 58, 60, 61, 68.

539 Ibid., s. 68.

540 Ibid., s. 67.

541 Ibid., s. 67.

542 Note that as described above, the OSC plays the additional role of authorization of certain surveillance activities, including certain activities undertaken by police forces, as well as determination of appeals of authorization refusals. See Part II, ss. 36ff. In this respect, the OSC does have "binding" powers.

543 *RIPA*, ss. 58–60, 39; *Police Act 1997*, s. 107.

544 *RIPA*, ss. 58–60.

545 *Police Act 1997*, s. 107.

546 *RIPA*, s. 68.

547 Ibid., s. 68.

548 *RIPA*, ss. 57, 59, 63; *Police Act 1997*, s. 91.

549 *RIPA*, s. 65(1).

550 Ibid., Schedule 3, s. 1.

551 *Police Act 1997*, s. 91.

552 *RIPA*, Schedule 3, s. 1.

553 *National Security Act of 1947*, Pub. L. No. 80-253, 61 Stat. 495 (codified as amended at 50 U.S.C. § 401 note). An unofficial version of the U.S. Code can be found online at Cornell Law School Legal Information Institute, http://www.law.cornell.edu/uscode (accessed May 26, 2006).

554 Exec. Order No.12,333, Part 1.14, 3 C.F.R. 200 (1981 Comp.), online, http://www.fas.org/irp/offdocs/eo12333.htm (accessed May 26, 2006), as amended by Exec.

Order No. 13,284 (January 23, 2003), online, http://www.fas.org/irp/offdocs/eo/eo-13284.htm (accessed May 26, 2006).

555 *Homeland Security Act of 2002*, 6 U.S.C. §§ 101ff.

556 U.S., Department of State, "Bureau of Intelligence and Research," online, U.S. Department of State, http://www.state.gov/s/inr/ (accessed May 26, 2006).

557 See 50 U.S.C. §§ 403–5.

558 *National Security Agency Act of 1959*, Pub. L. 86-36, 73 Stat. 63 (codified as amended at 50 U.S.C. § 402 note).

559 Two core documents that outline federal department responsibilities for U.S. national security, offered as general reference materials to the reader, are the Homeland Security Presidential Directive/HSPD-5, February 28, 2003, online, http://www.fas.org/irp/offdocs/nspd/hspd-5.html (accessed May 26, 2006), and the National Response Plan, December 2004, online, http://www.fas.org/irp/agency/dhs/nrp.pdf (accessed May 26, 2006).

560 The Background Paper is available on the Commission website, www.ararcommission.ca. Two civil liberties boards have also been established at the executive level, but they are beyond the scope of this chapter: the President's Board on Safeguarding Americans' Civil Liberties was established by Exec. Order No. 13,353, 69 Fed. Reg. 53 (Sept. 1, 2004); a Privacy and Civil Liberties Oversight Board within the Executive Office of the President was established by the *Intelligence Reform Act of 2004*, being Title I of the *Intelligence Reform and Terrorism Prevention Act of 2004*, Pub. L. No. 108-458, 118 Stat. 3638 § 1061 (codified at 5 U.S.C. § 601 note). The relationship between these two entities, and whether they will both continue to exist, is unclear at the time of writing.

561 See discussion under "Review and Oversight" below.

562 *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York: W.W. Norton, 2004), online, GPO Access, http://www.gpoaccess.gov/911/index.html (accessed May 26, 2006).

563 *Intelligence Reform and Terrorism Prevention Act of 2004*.

564 Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States* (Washington, D.C.: U.S. Government Printing Office, 2005), online, GPO Access, http://www.gpoaccess.gov/wmd/ (accessed May 26, 2006).

565 *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001*, Pub. L. No. 107-56, 115 Stat. 272. See also Stephen J. Schulhofer, *The Enemy Within: Intelligence Gathering, Law Enforcement, and Civil Liberties in the Wake of September 11* (New York: The Century Foundation Press, 2002), p. 1.

566 See James Risen and Eric Litchtblau, "Bush Lets U.S. Spy on Callers Without Courts," *The New York Times* (December 16, 2005), A1 [Risen and Litchtblau article]; White House, Radio Address, "President's Radio Address" (December 17, 2005), online, White House, http://www.whitehouse.gov/news/releases/2005/12/20051217.html (accessed May 26, 2006) [Radio Address by President George W. Bush]; U.S., Congressional Research Service, *Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information*, Memorandum by Elizabeth B. Bazan and Jennifer K. Elsea (Washington D.C.: Library of Congress, January 5, 2006), online, Federation of American Scientists Intelligence Resource Program, http://www.fas.org/sgp/crs/intel/m010506.pdf (accessed May 26, 2006) [CRS report on NSA Intercepts]; U.S., Department of Justice, White Paper, *Legal Authorities Supporting the Activities of the National Security Agency Described by the President* (January 19, 2006) [U.S. Justice Department White Paper].

567 Exec. Order No.13,354 (August 27, 2004) establishing the National Counterterrorism Center, online, Federation of American Scientists, http://www.fas.org/irp/offdocs/eo/eo-13354.htm (accessed May 26, 2006).

568 *Intelligence Reform and Terrorism Prevention Act of 2004* §1021. For an overview of this centre and the challenges involved in creating it, see U.S., Congressional Research Service, *The National Counterterrorism Center: Implementation Challenges and Issues for Congress*, by Todd M. Masse (RL 32816) (Washington, D.C.: Library of Congress, March 24, 2005), p. 16, online, Federation of American Scientists Intelligence Resource Program, http://www.fas.org/sgp/crs/intel/RL32816.pdf (accessed May 26, 2006).

569 Codified at 50 U.S.C. § 401 note, being Title I of the *Intelligence Reform and Terrorism Prevention Act of 2004*.

570 The American Intelligence Community was established formally by President Gerald Ford in Exec. Order No. 11, 905, 41 Fed. Reg. 7703 (February 19, 1976), online, Gerald R. Ford Presidential Library and Museum, http://www.ford.utexas.edu/library/speeches/760110e.htm (accessed May 26, 2006). The American Intelligence Community consists of 16 different organizations. For a list and a description of each agency, see "Members of the Intelligence Community," online, United States Intelligence Community, http://www.intelligence.gov/1-members.shtml (accessed May 26, 2006).

571 50 U.S.C. § 403.

572 Ibid. § 403-4a.

573 Ibid. § 403-1(f)(4).

574 Ibid. § 403-1(c).

575 Ibid. §§ 403-1(f), 403-1(c)(5)(C).

576 Ibid. § 403-1(e).

577 Ibid. § 403-1(f)(3)(A).

578 Ibid. § 403-1(f)(4).

579 28 U.S.C. §§ 531-540C.

580 "FBI History," online, Federal Bureau of Investigation, http://www.fbi.gov/fbihistory.htm (accessed May 26, 2006).

581 U.S., National Commission on Terrorist Attacks upon the United States, *Staff Statement No. 9: Law Enforcement, Counterterrorism, and Intelligence Collection in the United States Prior to 9/11* (April 13, 2004), p. 1. The investigatory authority of the FBI is found at 28 U.S.C. § 533. Specific authority to investigate crimes against the United States is provided for at 28 U.S.C. § 533(1).

582 U.S., *FBI Transformation Efforts: Hearing Before the Subcommittee on Science, State, Justice and Commerce, and Related Agencies of the House Committee on Appropriations*, 109th Cong. (2005), pp. 2–3 (Robert S. Mueller, III, Director, Federal Bureau of Investigation). The National Security Branch represents the FBI's response to the *Intelligence Reform and Terrorism Prevention Act of 2004* § 2001(c)(2), codified at 28 U.S.C. 532 note. The statute requires the FBI to "develop and maintain a specialized and integrated national intelligence workforce."

583 "National Security Branch Overview", online, Federal Bureau of Investigation, htttp://www.fbi.gov/hq/nsb/whitepaper.htm (accessed October 19, 2006) ["National Security Branch Overview"]. The FBI has stated that it intends to continuously incorporate structural changes across the National Security Branch in order to create efficiencies and promote integration.

584 Ibid.

585 *Intelligence Reform and Terrorism Prevention Act of 2004,* § 2002.

586 "Facts and Figures," online, Federal Bureau of Investigation, http://www.fbi.gov/priorities/priorities.htm (accessed May 26, 2006).

587 "Investigative Programs, Counter Intelligence Division," online, Federal Bureau of Investigation, http://www.fbi.gov/hq/ci/cointell.htm (accessed May 26, 2006); "Focus on Counter Intelligence, Part 1 of an Interview with FBI Assistant Director Dave Szady," online, Federal

Bureau of Investigation, http://www.fbi.gov/page2/july04/szady072004.htm (accessed May 26, 2006).

588 "Protecting America Against Terrorist Attack: A Closer Look at the FBI's Joint Terrorism Task Forces," online, Federal Bureau of Investigation, http://www.fbi.gov/page2/dec04/jttf120114.htm (accessed May 26, 2006).

589 "National Security Branch Overview."

590 6 U.S.C. §§ 101ff.

591 "Department of Homeland Security," online, The Executive Office of the President, Office of Management and Budget, http://www.whitehouse.gov/omb/budget/fy2005/homeland.html (accessed May 26, 2006).

592 6 U.S.C. § 121

593 For more information on the Coast Guard intelligence capability, see "US Coastguard Intelligence," online, United States Intelligence Community, http://www.intelligence.gov/1-members_coastguard.shtml (accessed May 26, 2006).

594 *National Security Act of 1947*. The *Central Intelligence Agency Act of 1949*, ch. 412 § 2, 63 Stat. 579 (codified at 50 U.S.C. § 401 note) supplemented the *National Security Act of 1947*. It provided a statutory basis for the Agency's budgetary secrecy and exempted it from disclosing the "organization, functions, names, official titles, salaries, or numbers of personnel employed by the Agency." See 50 U.S.C. § 403g.

595 See "CIA Frequently Asked Questions," online, Central Intelligence Agency, http://www.cia.gov/cia/public_affairs/faq.html#3 (accessed May 26, 2006) [CIA FAQ].

596 CIA FAQ.

597 50 U.S.C. § 403-4a(d)(1)–(4).

598 Ibid. § 403-3(d)(1).

599 Office of the Director of National Intelligence, News Release, "Establishment of the National Clandestine Service" (October 13, 2005), online, Office of the Director of National Intelligence, http://www.dni.gov/press_releases/20051013_release.htm (accessed May 26, 2006). See also U.S., *Oversight Subcommittee Hearing on the Status of Implementation of the Intelligence Reform and Terrorism Prevention Act of 2004, and the Stand-Up of the Office of the Director of National Intelligence: Hearing before the Permanent Select Committee on Intelligence, Subcommittee on Oversight*, 109th Cong. (2005), p. 11 (General Michael V. Hayden, Principal Deputy Director of National Intelligence), online, House of Representatives Permanent Select Committee on Intelligence, http://intelligence.house.gov/Media/PDFS/Transcript072805.pdf (accessed May 26, 2006); "General Michael V. Hayden Before House Permanent Select Committee, Subcommittee on Oversight, July 28, 2005," online, Office of the Director of National Intelligence, http://www.dni.gov/testimonies/20050728_testimony.htm (accessed May 26, 2006).

600 The NSA is sometimes referred to as the NSA/CSS. A presidential directive established the Central Security Service (CSS) in 1972 to integrate the military cryptological capability into the NSA. The CSS is still responsible for military cryptological elements. The Director of the CSS is also the Director of the NSA: "About NSA," online, National Security Agency, http://www.nsa.gov/about/about00018.cfm#5 (accessed May 26, 2006). A brief history of the NSA is given in Joel F. Brenner, "Information Oversight: Practical Lessons from Foreign Intelligence," Heritage Lectures No. 851, delivered June 25, 2004, and available online, The Heritage Foundation, www.heritage.org/research/nationalsecurity/hl851.cfm (accessed May 26, 2006) [Brenner].

601 National Security Agency, "Frequently Asked Questions," p. 1, online, National Security Agency, www.nsa.gov/about/about00020.cfm (accessed May 29, 2006).

602 For more information about Signals Intelligence generally, see "Signals Intelligence," online, National Security Agency, http://www.nsa.gov/sigint/index.cfm (accessed May 29, 2006).

603 50 U.S.C. § 403-5(b)(1); Exec. Order No. 12,333 §§ 1.11(j), 1.12(b), online, Ronald Reagan Presidential Library Archives, http://www.reagan.utexas.edu/archives/speeches/1981/120481d.htm (accessed May 29, 2006).

604 U.S., Congressional Research Service, *The National Security Agency: Issues for Congress*, by Richard A. Best (RL 30740) (Washington, D.C.: Library of Congress, January 16, 2001), p. 16, online, Federation of American Scientists Intelligence Resource Program, http://www.fas.org/irp/crs/RL30740.pdf (accessed May 29, 2006).

605 *National Security Agency Act of 1959* § 402 note. The responsibilities of the NSA are set out in Exec. Order No. 12,333 § 1.12(b).

606 Pub. L. 95-511, Title I, 92 Stat. 1796 (October 25, 1978) (codified as amended at 50 U.S.C. §§ 1801ff.) [*FISA*].

607 Exec. Order No. 12,333.

608 50 U.S.C. § 403-5(b)(1). Exec. Order No. 12,333 authorizes the NSA to collect foreign intelligence.

609 Exec. Order No. 12,333. For more information on what signals intelligence involves, see "SIGINT Frequently Asked Questions," online, National Security Agency, http://www.nsa.gov/sigint/sigin00003.cfm (accessed May 29, 2006).

610 An agent of a foreign power includes an individual engaged in international terrorist activities: *FISA*, 50 U.S.C. § 1801(a)(4).

611 *FISA*, 50 U.S.C. § 1804.

612 Risen and Litchtblau article; Radio Address by President George W. Bush.

613 Office of the Director of National Intelligence, "Remarks by General Michael V. Hayden, Address to the National Press Club: What American Intelligence & Especially the NSA Have Been Doing to Defend the Nation," January 23, 2006, Washington, D.C., online, Office of the Director of National Intelligence, http://www.dni.gov/speeches/20060123_speech.htm (accessed May 29, 2006).

614 See Risen and Litchtblau article; Radio Address by President George W. Bush; Letter from William E. Moschella, Assistant Attorney General, to The Hon. Pat Roberts, Chairman, Senate Select Committee on Intelligence, The Hon. John D. Rockefeller, IV, Vice Chairman, Senate Select Committee on Intelligence, The Hon. Peter Hoekstra, Chairman, Permanent Select Committee on Intelligence, U.S. House of Representatives, The Hon. Jane Harman, Ranking Minority Member, Permanent Select Committee on Intelligence, U.S. House of Representatives (December 22, 2005), online, Findlaw, www.findlaw.com (accessed May 29, 2006); CRS report on NSA Intercepts; U.S. Justice Department White Paper; Letter from Arlen Specter, U. S. Senate Judiciary Committee Chairman to U.S. Attorney General Alberto Gonzales (January 24, 2006), online, Findlaw, www.findlaw.com (accessed May 29, 2006). See also Beth Nolan, Curtis Bradley, David Cole et al., "On NSA Spying: A Letter to Congress," *New York Review of Books* 53:2 (February 9, 2006), online, http://www.nybooks.com/articles/18650 (accessed May 29, 2006). Written by a number of leading American constitutional scholars and former government officials, the letter questions the legality of the program. The essence of the debate turns around whether the President had the authority to authorize the NSA program, or whether that power lies with Congress.

615 U.S., Senate Committee on the Judiciary, Hearing on "Wartime Executive Power and the NSA's Surveillance Authority" (February 6, 2006), The Hon. Alberto Gonzales, Attorney General of the United States appearing as witness.

616 U.S., House of Representatives Permanent Select Committee on Intelligence, Press Release, "House Intelligence Agrees to Work Plan on NSA, FISA Oversight," online, House of Representatives Permanent Select Committee on Intelligence, http://www.fas.org/irp/news/2006/03/hpsci030206.pdf (accessed May 29, 2006).

617 Exec. Order No.12,333 § 1.12(b)(5).

618 "Information Assurance," online, National Security Agency, http://www.nsa.gov/ia/index.cfm (accessed May 29, 2006). The legal basis for this part of the NSA's mandate is found in Exec. Order No.12,333 § 1.12(b)(9).

619 Exec. Order No. 12,333 § 1.12(b)(9). See also *National Security Agency Act of 1959* § 13; "Research," online, National Security Agency, http://www.nsa.gov/research/ (accessed May 29, 2006).

620 *National Security Agency Act of 1959* § 6(a).

621 Best, p. 1. One recent press estimate has placed the number of employees at about 38,000: Barton Gellman, Dafna Linzer and Carol D. Leonnig, "Surveillance Net Yields Few Suspects," *Washington Post* (February 5, 2006) A01, online, Washington Post, www.washingtonpost.com (accessed May 29, 2006).

622 5 U.S.C. app.

623 5 U.S.C. app. §§ 1–12 (1978) § 11(2).

624 See for example, 50 U.S.C. § 403q, which creates and regulates the Office of the Inspector General of the CIA.

625 The jurisdiction of the IG DHS over certain immigration and customs bureaus is explicitly set out at 5 U.S.C. app. § 8I(e).

626 5 U.S.C. app. § 8H(a)(1)(A) and (g)(i). See also Department of Defense Directive 5106.1, "Inspector General of the Department of Defense" (January 4, 2001), online, Washington Headquarters Services, Executive Services Directorate, Directives and Records Division, http://www.dtic.mil/whs/directives/corres/html/510601.htm (accessed May 29, 2006). While the Inspector General for the Department of Defense was created by statute, the IG of the NSA was created by a regulation of the Agency: NSA/CSS Directive 10-4, November 26, 1997, cited in Brenner. Appointment of the NSA Inspector General is made by the NSA itself and so lacks the independence of an outside appointment. See "Office of the Deputy Inspector General for Intelligence," online, United States Department of Defense, Office of the Inspector General, http://www.dodig.osd.mil/Ir/index.html (accessed May 29, 2006).

627 50 U.S.C. § 403q (IG CIA).

628 The *Intelligence Reform and Terrorism Prevention Act of 2004* §1078 gives the DNI the power to establish an inspector general. This provision modifies the *Inspector General Act of 1978* and is codified at 5 U.S.C. app. § 8K.

629 5 U.S.C. app. § 2(1). See also the website of the U.S. Federal Inspectors General, IGNet at http://www.ignet.gov/pande/pmembers1.html (accessed May 29, 2006).

630 U.S., United States Department of State and the Broadcasting Board of Governors, Office of Inspector General, "Inspection of the Bureau of Intelligence and Research," November 28, 2005, online, U.S. Department of State, http://oig.state.gov/documents/organization/58019.pdf (accessed May 29, 2006).

631 5 U.S.C. app. § 5.

632 5 U.S.C. app. § 4(4).

633 5 U.S.C. app. § 6(a)(3). Note that when conducting certain sensitive investigations, including investigations that may touch on matters of national security, the inspectors general of the DHS, DOJ and DoD are under the control and direction of the head of their respective agencies: 5 U.S.C. app. §§ 8I(a)(1), 8E(a)(1) and 8(b)(1), respectively.

634 50 U.S.C. § 403q(e)(8). The agencies from which the IG CIA may request assistance are defined in 50 U.S.C. § 403a(c).

635 Exec. Order No. 12,301 (March 26, 1981), Integrity and Efficiency in Federal Programs, online, The American Presidency Project, http://www.presidency.ucsb.edu/ws/index.php?pid=43593&st=&st1=; Exec. Order No. 12,805 (May 11, 1992), *Integrity and*

Efficiency in Federal Programs, online, IG Net, http://www.ignet.gov/randp/igbrochure04.pdf (accessed May 29, 2006); U.S., Inspector General Community, "An Introduction to the Inspector General Community," December 14, 2004, online, IG Net, http://www.ignet.gov/randp/igbrochure04.pdf (accessed May 29, 2006) [Inspector General Community, "An Introduction"].

636 Exec. Order No. 12,805.

637 Inspector General Community, "An Introduction." See generally the Inspector General Community website at http://www.ignet.gov (accessed May 29, 2006).

638 For more information on the forum, see "Office of Deputy Inspector General for Intelligence —Coordination," online, Department of Defense, http://www.dodig.osd.mil/Ir/coordination.htm (accessed May 29, 2006). See also the House of Representatives report on a bill to enact the Intelligence Community, Rept. 104-620, June 13, 1996, § 132 and accompanying analysis, online, U.S. Government Printing Office, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_reports&docid=f:hr620p1.104.pdf (accessed May 29, 2006).

639 5 U.S.C. app. § 4; for the IG CIA, 50 U.S.C. 403q(a).

640 5 U.S.C. app. § 4; for the IG CIA, 50 U.S.C. 403q(c)(1).

641 *PATRIOT Act*.

642 *Intelligence Reform and Terrorism Prevention Act of 2004* § 8304, amending the *Inspector General Act of 1978* app. § 8I. See also *Intelligence Reform and Terrorist Prevention Act of 2004* § 8302, amending the *Homeland Security Act of 2002*, 6 U.S.C. § 111(b)(1). The new section (G) states that a principal mission of the Department of Homeland Security is to "ensure that the civil rights and civil liberties of persons are not diminished by efforts, activities, and programs aimed at securing the homeland."

643 5 U.S.C. app. § 4(a)(1); for the IG CIA, 50 U.S.C. § 403q(c)(1).

644 5 U.S.C. app. § 7; for the IG CIA, 50 U.S.C. § 403q(e)(3).

645 5 U.S.C. app. § 4(a)(1); for the IG CIA, 50 U.S.C. § 403q(c)(1).

646 5 U.S.C. app. § 6(a)(2); for the IG CIA, 50 U.S.C. § 403q(a)(1).

647 50 U.S.C. §403q(d)(4).

648 5 U.S.C. app. § 4(a). The IG CIA's mandate is similar but is set out in a separate statute. See 50 U.S.C. § 403q(a).

649 See for example 5 U.S.C. app. §§ 8, 8E and 8I, respectively. Specific provisions regarding the Inspectors General of the Intelligence Communities, which include the IG of the NSA, are found at 5 U.S.C. app. § 8H.

650 5 U.S.C. app. §§ 8E(b)(1), (2), (4) and 8H(a)(1)(B).

651 U.S., Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001, *Report of the U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence*, S. Rep. No. 107-351; and H.R. Rep. No. 107-792, (2002), pp. 15–16. For further examples of investigations, see the special reports published by the IG DOJ in relation to the FBI, online, http://www.usdoj.gov/oig/ (accessed May 29, 2006).

652 U.S., Department of Justice, Office of the Inspector General, *A Review of the FBI's Handling of the Brandon Mayfield Case: Unclassified Executive Summary* (January 2006), online, U.S. Department of Justice, Office of the Inspector General, http://www.usdoj.gov/oig/special/index.htm (accessed May 29, 2006).

653 U.S., Department of Justice, FBI Media Release, "Border Patrol Agent Arrested for Civil Rights Violation" (January 20, 2006), online, Department of Homeland Security, http://www.dhs.gov/interweb/assetlibrary/BPagent_Arrested.pdf (accessed May 29, 2006).

654 U.S., Department of Justice, "Two U.S. Border Patrol Agents Charged by Federal Grand Jury Indictment with Assault Charges" (April 13, 2005), online, Department of Homeland Security,

http://www.dhs.gov/interweb/assetlibrary/OIG_BPShooting_Apr05.pdf (accessed May 29, 2006).

655 See Inspector General of the Department of Justice, "The September 11 Detainees: A Review of the Treatment of Aliens Held on Immigration Charges in Connection with the Investigation of the September 11 Attacks" (June 2003); and the "Supplemental Report on September 11 Detainees' Allegations of Abuse at the Metropolitan Detention Center in Brooklyn, New York" (December 2003).

656 5 U.S.C. app. § 6(a); 50 U.S.C. §403q(e)(5).

657 5 U.S.C. app. § 6(e)(1).

658 50 U.S.C. § 403q(e)(2). CIA employees also have an obligation to co-operate with the IG.

659 5 U.S.C. app. §§12–13.

660 50 U.S.C. § 403q(a) and (c) (IG CIA); 5 U.S.C. app. §§ 4(4)(B)–(5); Meetings with IGs DoD, DOJ and DHS.

661 5 U.S.C. app. §§ 8(b)(1), 8E(a)(1), 8I(a)(1). The relevant department head may also prohibit the IG from carrying out or completing an inspection or investigation (see 5 U.S.C. app. §§ 8(b)(2), 8E(a)(2) and 8I(a)(2)), and in the case of the DOJ and DHS, may prevent disclosure of sensitive information or harm to U.S. national interests (see 5 U.S.C. app. §§ 8E(a)(2) and 8I(a)(2)). See also 5 U.S.C. app. §§ 8(b)(2), 8I(a)(2) and 50 U.S.C. § 403q(b).

662 Ibid.

663 50 U.S.C. § 403(q)(b)(4) (IG CIA); 5 U.S.C. app. §§ 8(b)(3)–(4), 8E(a)(3), 8I(a)(3).

664 U.S., Office of the Inspector General of the Department of Justice, *Epilogue* (July 1998) to *CIA-Contra-Crack Cocaine Controversy: A Review of the Justice Department's Investigations and Prosecutions* (December 1997), online, U.S. Department of Justice, Office of the Inspector General, http://www.usdoj.gov/oig/special/9712/epilogue.htm (accessed May 29, 2006) [IG DOJ, *Epilogue*].

665 L. Britt Snider, "Creating a Statutory Inspector General at the CIA" (2001) 10 *Studies in Intelligence* 15, p. 20.

666 5 U.S.C. app. § 4(a).

667 5 U.S.C. app. § 6(e)(1), subject to guidelines issued by the Attorney General (§ 6(e)(4)).

668 50 U.S.C. § 403(q)(b)(5) (IG CIA); 5 U.S.C. app. § 4(d).

669 See 5 U.S.C. app. §§ 5 and 8H(g)(1); 50 U.S.C. § 403q(d).

670 5 U.S.C. app. § 5(e).

671 50 U.S.C. § 403q(d)(1).

672 IG DOJ, *Epilogue*.

673 The Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office.

674 5 U.S.C. app. § 8H(g).

675 5 U.S.C. app. § 3(a); 50 U.S.C. § 403q(b)(1).

676 Brenner.

677 5 U.S.C. app. § 8(a).

678 Ibid., § 3(a).

679 50 U.S.C. § 403q(b)(1).

680 6 U.S.C. § 345 (2002).

681 *Intelligence Reform and Terrorism Prevention Act of 2004*, § 8303(4), amending the *Homeland Security Act of 2002*, 6 U.S.C. § 345(a).

682 *Memorandum of Understanding between the Officer for Civil Rights and Civil Liberties and the Inspector General*, September 4, 2003.

683 50 U.S.C. § 403-3c. The Director of the CIA reports to the Director of National Intelligence, as discussed above.

684 Ibid. § 403-3d.

VIII

Characteristics of National Security Activities Requiring Enhanced Review

1. INTRODUCTION

National security activities aimed at maintaining the safety and security of our country can affect rights and freedoms valued by Canadians and protected by the Constitution. The challenge in a liberal democracy such as Canada is to keep the country and its people secure from external and internal threats, including threats of terrorist violence, while preserving the rights and freedoms essential to democracy.[1] The Supreme Court of Canada has observed:

> On the one hand stands the manifest evil of terrorism and the random and arbitrary taking of innocent lives, rippling out in an ever-widening spiral of loss and fear. Governments . . . need the legal tools to effectively meet this challenge.
>
> On the other hand stands the need to ensure that those legal tools do not undermine values that are fundamental to our democratic society — liberty, the rule of law, and the principles of fundamental justice — values that lie at the heart of the Canadian constitutional order and the international instruments that Canada has signed. In the end it would be a Pyrrhic victory if terrorism were defeated at the cost of sacrificing our commitment to those values.[2]

In this chapter, I draw attention to issues that should be considered in designing a review mechanism for the RCMP's national security activities. In particular, I identify characteristics of national security investigations that are different, in kind or at least in degree, from those of other criminal investigations and that call for enhanced review.

National security activities involve the most intrusive powers of the state: electronic surveillance; search, seizure and forfeiture of property; information collection and exchange with domestic and foreign security intelligence and law

enforcement agencies; and, potentially, the detention and prosecution of individuals. The use of such powers may adversely affect individual rights and freedoms.

The threat to rights and freedoms posed by national security activities is of particular concern in the post-9/11 era. Understandably, terrorism has affected the approaches of security intelligence and law enforcement agencies. Many Western nations have made significant amendments to their legislation to create extraordinary powers of investigation, detention and prosecution in the terrorism context.[3] Since September 11, 2001, there has been greater domestic and international information sharing and co-operation with respect to terrorist threats,[4] as well as a significant shift in resources toward the prevention of terrorist activities.

Counter-terrorism national security investigations pose a greater potential risk to rights and freedoms than most, if not all, traditional criminal investigations, particularly in the post-9/11 environment.[5] In the discussion that follows, I examine some of the distinguishing characteristics of national security investigations, their potential for adversely affecting rights and freedoms, and the implications for review mechanisms. The point is to highlight what impact different characteristics of national security investigations could have on rights and freedoms, with a view to assisting with the design of an appropriate review mechanism.

2. SECRECY

The most compelling reason for developing a robust review mechanism for the RCMP's national security activities is the lack of transparency that necessarily accompanies all national security investigations.

Such investigations inevitably involve surreptitious or covert activities by law enforcement or security intelligence services, often including the use of human sources, information obtained from foreign or international agencies, and electronic and physical surveillance. To function effectively, Canada's national security agencies must be able to protect their sources and investigative methods, as well as information that could compromise ongoing investigations. Classified information, information from human sources and certain information provided by foreign governments must also be kept secret.[6] Subjects of national security investigations therefore may never know that they have been under investigation and thus are unlikely to be in a position to lay a complaint if anything improper occurred.

Moreover, the *Criminal Code*,[7] *Immigration and Refugee Protection Act*,[8] *Charities Registration (Security Information) Act*[9] and *Canada Evidence Act*[10] make provision for *in camera* and *ex parte* hearings in order to protect confidential or classified information. As a result, some information that would otherwise be made public in judicial or administrative hearings is kept confidential and may not be disclosed to the affected parties.[11]

Some degree of secrecy may also be necessary to protect the privacy and reputations of those investigated. While being identified as a suspect in any criminal investigation is hard, being linked to a terrorism investigation is particularly difficult. Openly identifying individuals as terrorism suspects can have serious ramifications for the individuals themselves, their families and any organizations that are identified.[12]

The extraordinary powers introduced by Canada's anti-terrorism legislation, which I discuss in Chapter III, include discretionary ministerial powers to maintain the confidentiality of information related to national security in legal and administrative proceedings. Under the *Canada Evidence Act*, the Attorney General of Canada has broad discretion to protect the disclosure of "potentially injurious" and "sensitive" information.[13] Persons who anticipate the disclosure of such information in the course of court proceedings must notify the Attorney General, who may apply to the Federal Court for an order respecting disclosure. If a disclosure order is made, whether by the Federal Court or, on appeal, by the Federal Court of Appeal or Supreme Court of Canada, the Attorney General has the discretion to issue a certificate prohibiting disclosure in order to protect information obtained in confidence from or in relation to a foreign entity[14] or to protect national defence or national security.[15] Such a certificate is binding even during criminal proceedings. Although there are provisions for judicial review of the certificate and for the stay of criminal trials when necessary to ensure fairness to an accused,[16] the grounds upon which the Attorney General exercises his or her discretion may be difficult to review for compliance with constitutional values because of the secrecy involved.[17]

Expert groups and commentators have voiced concern over the scope of protected information under section 38 of the *Canada Evidence Act*, citing the open court principle and the ability of the executive branch of government to override a judicial decision authorizing disclosure.[18] Others, however, note that the courts have protected the open court principle even in the context of investigation of terrorism offences and that "[b]ecause the secrecy requirement often cannot be avoided, it is the presiding judge who must serve as the bulwark and the screen, safeguarding the public interest and protecting the integrity of the process."[19]

Section 38 also affects the operation of the federal *Access to Information Act* and provincial equivalents. These statutes generally provide a right of access to information in the control of government institutions, based in part on the principle that government information should be available to the public, subject to limited and specific exceptions. Access to information is one aspect of individual rights and freedoms in Canada. The Supreme Court of Canada has recognized that the overarching purpose of access to information legislation is to facilitate democracy.[20] Such legislation helps ensure that citizens have the information needed to participate meaningfully in the democratic process and that politicians and bureaucrats remain accountable to the public.

Nevertheless, the federal *Access to Information Act* contains exemptions to the right of access to information in the national security context, including access to information obtained in confidence from a foreign government, a foreign institution or an international organization of states; information the disclosure of which could be injurious to international affairs or defence; information pertaining to law enforcement and investigations; and personal information.[21] The Information Commissioner of Canada, who is responsible for administering the *Access to Information Act*, may access all documents, except those protected by Cabinet privilege, for the purpose of ascertaining whether a government institution is properly claiming these exemptions. The Information Commissioner's decisions in this regard are subject to review by the Federal Court. If, ultimately, information is found to come within one of the Act's exemptions, then the public has no right of access.

It is thus essential that the design of a review mechanism for the RCMP's national security activities take account of the fact that a great deal of what needs to be reviewed may not be disclosed publicly. The significant challenge is therefore to come up with a process that, while not fully transparent, still engenders public confidence and trust.

3. POLICE POWERS AND TERRORISM OFFENCES

Following the events of 9/11, the Canadian government passed the *Anti-terrorism Act* and other statutes that created new terrorism offences and established new powers in respect of those offences. I discuss both in greater detail in Chapter III. Extraordinary powers include investigative hearing, preventive detention and enhanced electronic surveillance powers.

As a law enforcement agency, the RCMP also has police powers not provided to either CSIS or the Communications Security Establishment (CSE), Canada's main security intelligence agencies. The authority to use the broad

range of powers conferred on the RCMP in the national security context may affect the rights and freedoms of individuals and thus must be considered when designing a review mechanism.

3.1
POWERS UNDER *ANTI-TERRORISM ACT*

One of the newly created special investigative powers in relation to terrorist activity is the investigative hearing power. A person with information about a past or future terrorist act may be compelled to take part in a judicial investigative hearing to answer investigators' questions put to him or her by a Crown attorney.[22] The Supreme Court of Canada has upheld the constitutionality of judicial investigative hearings.[23] In *Application under s. 83.28 of the Criminal Code (Re)*, the majority of the Court concluded that the role of the judge presiding over the hearing was not simply to ensure that the witness answered questions, but also to ensure that the proceeding adhered to constitutional protections, including the protection of individual rights and freedoms. It should be noted, however, that only one application to conduct an investigative hearing has been made, retrospectively, with respect to the Air India matter,[24] and the investigative hearing has not actually been held.

Another new power is that of preventive arrest where a police officer has reasonable and probable grounds to believe that the arrest or detention of a person is necessary to prevent the carrying out of a terrorist activity.[25] This power has never been invoked. In addition, the *Anti-terrorism Act*[26] created enhanced electronic surveillance powers that may be exercised when terrorist activity is being targeted. These powers are in addition to regular police powers, which may also be directed towards the investigation and prevention of terrorist activity.

Other extraordinary investigative powers in the national security context have yet to be reviewed by the courts. Commentators have varying views about the outcome of legal challenges. On the one hand, concern has been expressed that the judiciary may have difficulty avoiding "the temptation of being just a little more deferential towards the government and of leaning towards the state and away from rights in the post-September 11 world."[27] On the other, arguments have been made that "[t]he procedural provisions confer power while at the same time constraining resort to it" and "[r]estricting the reach or ambit of the legislation in this manner to matters and concerns affecting the national security constitutes a restraining or minimally-impairing feature of this initiative for purposes of constitutional analysis."[28]

3.2 POLICE POWERS

The design of a review mechanism for the RCMP's national security activities must take account of the fact that the RCMP has certain police powers that the security intelligence agencies, CSIS and the CSE, do not possess. The use of coercive police powers can result in significant curtailment of rights and freedoms.[29]

The RCMP possesses significant coercive powers, including powers to arrest individuals (with or without warrants), detain individuals, conduct warrantless searches incidental to arrests, execute search warrants / entry into premises (both overt and covert), seize evidence, draw and use firearms, use non-lethal force (choke-hold, Taser, baton or pepper spray, for example), use police dogs and lay charges. CSIS has only one of these powers: the power of covert entry into premises pursuant to judicial authorization. Other intrusive powers, including electronic surveillance, may be conducted by both police and security intelligence agencies.

Police powers may be exercised in both national security investigations and more traditional policing situations. However, the use of these powers in a national security context bears particular risks that may require a different form of review. Most importantly, it is far less likely to be transparent or known to those affected. The secret use of coercive powers calls for increased vigilance and enhanced methods of accountability.

It is also more likely that the exercise of police powers in a national security context will be based on information provided from foreign or other sources that may not be disclosed publicly. As discussed below, there is also a concern in the post-9/11 environment that the use of these powers in a national security investigation may be discriminatory because of the types of offences involved and the communities investigated.

If charges are not laid, or if a decision is made not to proceed with a prosecution after charges are laid, there may be very limited or no review of the exercise of these powers. For example, where an individual is arrested pursuant to a warrant, the decision to issue the arrest warrant is made by a justice of the peace or a judge based on evidence provided by police officers. If charges are not proceeded with and no civil suit is pursued, the nature, quality and reliability of the information used to obtain the arrest warrant will likely not be subject to judicial review.

It is consequently important that a review mechanism for the RCMP's national security activities take account of the fact that the RCMP has the authority to employ a wide range of intrusive and coercive investigative techniques.

4. INTERNATIONAL CO-OPERATION

International co-operation during national security investigations is clearly important and nothing I say here should be interpreted as indicating that such co-operation should not take place or continue to expand as necessary to address global threats to our security. However, international co-operation during national security investigations has the potential to significantly affect rights and freedoms. As countries coordinate their law enforcement and security intelligence activities, the effects of practices such as information sharing are increasing exponentially, in both positive and potentially negative ways. My report on the Factual Inquiry demonstrated that sharing information from investigations in Canada with other countries can have a "ripple effect" beyond Canada's borders, with consequences that may not be controllable from within Canada. The legal power of Canadian courts and governments to require respect of constitutional rights and freedoms is exercised within Canada's territorial borders. Once a person or information moves outside of Canada, it becomes difficult to ensure treatment of that person or information in accordance with Canadian constitutional rights and values.

The Supreme Court of Canada has recognized this problem in the context of extradition and deportation proceedings in Canada, particularly where the affected person could face torture or the death penalty in the destination country. It has ruled that extradition to face the death penalty violates section 7 of the *Canadian Charter of Rights and Freedoms* (the Charter)[30] and that deportation to face torture is impermissible,[31] though noting that there may be extraordinary exceptions. What is important for this discussion is that the Court has stated that Canadian decision makers must consider the potential consequences of their actions on rights and freedoms beyond Canadian borders. Where there is a sufficient connection between Canadian government actions and a subsequent deprivation of liberty outside Canada in violation of the principles of fundamental justice, section 7 of the Charter may be unjustifiably infringed. The Canadian government thus may bear responsibility within Canada for deprivations of liberty outside Canada that result from its actions.

Addressing issues beyond the direct risk of torture or death, the Supreme Court recently held that compelled testimony from investigative hearings may not be used against the witness in extradition or deportation proceedings and

may not subsequently be passed on to other governments for prosecution purposes. The Court indicated that such a situation would violate the right against self-incrimination and that judges presiding over investigative hearings should set conditions to prevent such use of testimony.[32]

Canadian investigators may receive and act upon information from other countries. Use of this information may have significant personal consequences for individuals in Canada and their associates, such as investigation, surveillance, arrest or prosecution. In some instances, such information may have been acquired in ways inconsistent with rights and freedoms protected here. For example, it may have been obtained through torture or other unacceptable investigation techniques, or in the absence of checks and balances to ensure reliability.[33] While it is often important that Canadian investigators receive information from other countries, special care needs to be taken to ensure that the use of such information does not unfairly affect individuals in an investigation. As one American commentator has noted, "the most serious questions of human rights will arise not here, but abroad" if countries try to "reap the benefits" of activities forbidden by international human rights conventions by attempting to obtain information about the plans of terrorists in countries that do not have similar standards in regard to issues such as interrogation, detention or surveillance.[34]

My concern about the potential unreliability of such information is heightened by the fact that the person to whom the information applies will have no way to determine whether or not the investigators' information is correct until that information is divulged to him or her. In the meantime, investigators acting on incorrect or unreliable information may proceed with a vast array of intrusive actions, from interviews of friends, employers and family to applications for electronic surveillance or, potentially, investigative detention. Below, I refer to personal information contained in RCMP and CSIS data banks that are exempt from the *Privacy Act* and to exemptions in the *Privacy Act* that allow governments to deny access to personal information or the right to correct such information on grounds, for example, of law enforcement.

A mechanism for reviewing the RCMP's national security activities must be able to examine RCMP information-sharing practices, particularly practices for sharing information with other countries, as well as the use made in Canada of foreign-source information.

5.
PRIVACY AND THE COLLECTION, USE AND SHARING OF INFORMATION

5.1
PRIVACY

An important aspect of personal freedom that may be affected by national security activities is privacy. As the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (McDonald Commission) noted in its report:

> In a liberal society, which as a matter of principle wishes to minimize the intrusion of secret state agencies into the private lives of its citizens and into the affairs of its political organizations and private institutions, techniques of investigation that penetrate areas of privacy should be used only when justified by the severity and imminence of the threat to national security. This principle is particularly important when groups may be subjected to security intelligence investigations although there is no evidence that they are about to commit, or have committed, a criminal offence.[35]

Section 7 of the Charter guarantees the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice. This broadly framed section encompasses aspects of decisional, informational and personal privacy interests, such as rights related to physical or psychological integrity or the right to space within which to make basic personal choices.[36] Specific protection for informational, territorial, spatial and personal privacy is also found in sections 8 and 9 of the Charter, which recognize the right to be free from unreasonable search and seizure and from arbitrary detention. Finally, international instruments such as the *International Covenant on Civil and Political Rights*[37] explicitly protect the right to be free from arbitrary interference with privacy.

The informational privacy interest also receives some legislative protection at both the federal and provincial levels through statutes such as the federal *Privacy Act*, which protects individual privacy with respect to information held by government institutions. That act also provides individuals with a right of access to personal information about themselves held by government institutions and a right to request correction of erroneous or incomplete personal information.[38] However, a number of statutory exemptions allow government institutions to deny individuals access to personal information about themselves, including

access for the purpose of correcting erroneous information. In the national security context, the most relevant exemptions relate to personal information obtained in confidence from governments of foreign states or foreign institutions; information the disclosure of which could be injurious to international affairs, the defence of Canada or allied states or "the efforts of Canada toward detecting, preventing or suppressing subversive or hostile activities;" information pertaining to law enforcement or investigations; and information related to security clearances.[39] The "investigations" referred to here include those pertaining to activities suspected of constituting threats to the security of Canada within the meaning of the *Canadian Security Intelligence Service Act*. In *Ruby v. Canada,* the Supreme Court of Canada upheld the ability of government to make *ex parte* and *in camera* submissions to the court when exemptions from disclosure on the ground of national security or protection of foreign confidences are claimed.[40]

There are also a number of "exempt banks," that is, whole collections of information exempt from the *Privacy Act*. Of particular significance to any examination of the impact of national security activities on rights and freedoms is the fact that, by executive order, the following personal information banks are designated exempt: (a) Criminal Operations Intelligence Records, under the control of the RCMP;[41] (b) Canadian Security Intelligence Service Investigational Records, under the control of CSIS;[42] and (c) National Security Investigations Records, under the control of the RCMP.[43] These exemptions, combined with the Attorney General's power to issue certificates under section 38 of the *Canada Evidence Act*, as discussed above, have caused the Privacy Commissioner, among others, to raise concerns about the extent, propriety and accuracy of information sharing among government agencies in the national security context.[44] Moreover, the lack of a review mechanism leaves individuals with no way to correct inaccurate or false information or to have information removed from the system.[45]

5.2
USE OF PERSONAL INFORMATION IN NATIONAL SECURITY INVESTIGATIONS

Almost all national security activities will affect privacy interests, given the nature of national security investigations, where information about groups and individuals is collected and analyzed. The RCMP may collect, use and disclose personal information about individuals in the course of investigations in the following ways:

- individuals may be identified as suspects or persons of interest;

- individuals may be placed under physical or electronic surveillance and their contacts may be traced;
- individuals may be questioned;
- human sources may be identified and solicited to provide information about an individual;
- information about individuals may be entered on computer databases;
- information may be provided to other government, police and security intelligence agencies, both domestically and internationally; and
- personal information may be contained in affidavits used to obtain search or arrest warrants.

Whenever an investigator takes one of these steps, the broadly defined privacy interest of the individual is affected. The degree of intrusiveness varies. For example, the interception of private communications pursuant to a warrant is a significant intrusion, subject to external judicial scrutiny, whereas the decision to undertake physical surveillance to identify a pattern of behaviour is much less intrusive and does not require a warrant or judicial approval.

It is also important to recognize that the RCMP may collect information from a wide variety of sources, including internal sources, provincial and municipal police forces, the Canada Border Services Agency (CBSA), Citizenship and Immigration Canada, CSIS, the CSE, Transport Canada, foreign police agencies, and foreign security intelligence agencies. The RCMP must assess the reliability of information, decide whether to enter it in a national security data bank such as the Secure Criminal Information System (SCIS) and determine how long the information should be retained.

The individual affected may never know the nature, content or accuracy of the information collected or the identity of persons to whom the information has been disseminated. In *R. v. Dyment*, Justice La Forest commented specifically on the importance of informational privacy, stating:

> This too is based on the notion of the dignity and integrity of the individual. As the Task Force put it: "This notion of privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit." In modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected.[46]

If charges are laid and a prosecution proceeds to trial, the individual will have the benefit of external scrutiny, including judicial scrutiny for compliance with the Charter. If not, the individual may never learn to what extent the state has delved into his or her private life or what information may remain on computer databases.[47] Here again, the need for a credible, robust review mechanism is clear.

6. SCOPE AND EXERCISE OF DISCRETIONARY POWERS

Many of the decisions made in the context of national security, including decisions by the police, are discretionary. They may include decisions to input information into national security databases, ask questions of individuals, select suspects for investigation, recruit and use a human source, and act upon information supplied by a foreign government. Such decisions affect the privacy rights and interests of individuals and, potentially, other rights such as the right to freedom from adverse treatment on discriminatory grounds.[48] Unless charges are laid, there will likely be no external scrutiny of these discretionary decisions.

Another example of the use of discretion in the national security context relates to cases involving non-citizens of Canada. In these cases, when the government has sufficient evidence, it may opt to lay charges under the criminal law or to use immigration proceedings. Immigration law, including the security certificate process, provides for broader grounds of culpability and lower standards of proof than criminal law.[49] It also allows for some proceedings to be conducted in private, in the absence of the person arrested.[50] The Supreme Court of Canada has recognized that non-citizens may be subject to impermissible discrimination,[51] and the "non-citizen" category often overlaps with those groups that may be vulnerable to racial, ethnic and religious profiling, which I discuss below.

Many aspects of the national security activities of the RCMP are not directly subject to legislation or regulation, but involve discretionary decisions about what activities or persons will be investigated and how this will be done.[52] Even where policies or ministerial directives exist, they sometimes contain general language and undefined terms, the application of which also necessarily involves the exercise of discretion.

The nature of intelligence-led policing and security intelligence poses particular challenges for ensuring the protection of fundamental rights and freedoms. Clearly, discretionary decisions by officials applying a law must be made in compliance with the Charter.[53] However, in the absence of specifically legislated measures to guide or review protection of rights and freedoms during

national security investigations, complying with the values of the Charter is a challenge.

The substantial discretion exercised by investigators on an operational level in many national security activities is often not subject to external scrutiny. This makes it difficult to assess or object to the impact of decisions on rights and freedoms. An effective review mechanism can play an important role in ensuring that discretionary decisions are made in conformity with legal and policy requirements and with fundamental values considered important in Canada.

7.
POTENTIAL FOR DISCRIMINATION

7.1
RACIAL, ETHNIC AND RELIGIOUS PROFILING

The nature of national security investigations, particularly terrorism investigations in the post-9/11 environment, and the new terrorism offences that have been created have increased the potential for discriminatory action by investigators. A properly empowered review mechanism can do much to address perceptions and provide assurance that the RCMP does not engage in such practices.

A number of the participants in this Inquiry raised concerns about the targeting of Arab and Muslim communities through racial, ethnic and religious profiling in the wake of the attacks of September 11, 2001.[54] Profiling can be defined broadly as the use of race, religion or ethnicity as the sole reason for or a factor in a decision to detain or arrest an individual or subject him or her to further investigation.[55] It may stigmatize and place some groups in Canadian society at risk.[56] As the Canadian Bar Association has pointed out, compromises between security and civil liberties are "not demanded equally of all who are theoretically made more secure."[57] Certain ethnic and religious groups have been targeted since 9/11. Intervenors and academic commentators have expressed concern that such profiling undermines the liberty, privacy and equality of innocent Canadians. It may thus be found to be discriminatory under section 15 of the Charter.

A further issue is the fact that any profiling that may take place is the result of a discretionary operational decision, removed from public debate or legislative scrutiny.[58] Racial, ethnic and religious profiling practices emerge not from a legislative direction, but from administrative discretion and investigative practice. This has prompted concerns that such discretion may be exercised without

a thorough understanding of the cultural and religious milieu in which an investigation is being conducted.

7.2 INQUIRY INTO RELIGIOUS OR POLITICAL BELIEFS

National security activities raise a question regarding the protection of rights and freedoms because they may lead to a considerable degree of state inquiry into religious and political beliefs. A distinctive characteristic of some of the terrorism offences in the *Criminal Code* is that motivation is an element of the offence; prohibited activity must be undertaken "in whole or in part for a political, religious or ideological purpose, objective or cause."[59] This requirement marks a shift away from the traditional proposition in criminal law that motive is not a necessary element of a crime, but, rather, may be a factor in determining a proper sentence. The shift towards motive as an essential element in a crime provides increased reason for national security investigations to involve inquiry into a subject's personal religious or political beliefs, or for investigation to stem from suspicions aroused by a subject's personal beliefs.[60]

The requirement for proof of political or religious motive must be linked to an intent to cause serious harm. It is designed to impose "an extra burden of proof upon the state."[61] Investigators may nonetheless lean toward increased inquiry and investigation based on religious and personal beliefs.[62] This could raise concerns about profiling in addition to the concerns about privacy and freedom of religion and expression.

7.3 EXPRESSION AND ASSOCIATION

Freedom of thought, belief, opinion, expression and association, which is essential to democracy, is protected under section 2 of the Charter. However, it has long been recognized that one of the greatest concerns regarding national security investigations is their potentially chilling effect on legitimate dissent. Indeed, one of the major issues raised by the McDonald Commission was the improper targeting of legitimate dissent.[63] Those who exercise freedoms to challenge our social, economic and political structures should not "have their activities noted in secret security dossiers to be used against them by the state."[64]

The breadth of the new terrorism offences, which include financing and facilitating, also increases the potential for state scrutiny of a wide range of associational and expressive activities, as well as invasions of privacy.[65]

The "participating, facilitating, instructing and harbouring" provisions of the Code make it an offence, for example, to knowingly participate in or contribute

to, directly or indirectly, any activity of a terrorist group, including knowingly recruiting new individuals for the purpose of enhancing the ability of a terrorist group to facilitate or commit terrorist activities.[66] These provisions have been criticized as overly broad and vague, leaving the door open for officials to exercise their discretion improperly.[67]

Even where an organization is not proscribed as a terrorist organization, the perception that it may be under scrutiny by the RCMP or CSIS may have a chilling effect on both the associational and expressive activities of individuals and organizations in its respect.[68] It can be difficult to discern the appropriate limits between gathering information needed to identify terrorist activities and limiting legitimate political dissent. Thus, this issue is relevant in designing a review mechanism.

8.
ROLE OF COURTS

Because of the nature of most national security investigations, the courts provide less oversight in their regard than they do for other criminal investigations. This reduced level of judicial oversight is a further reason for independent review.[69]

Few national security investigations receive the degree of external scrutiny found in the investigative hearing process or in criminal prosecutions. The goal of preventing terrorism in the national security context may lead to the collection of a diverse range of information by both domestic and foreign police and security intelligence agencies. Moreover, where national security is involved, a decision may be made not to lay charges when a crime has been committed, so as to protect Canada's foreign relations, the security of sources or information-sharing protocols with other countries. Unless charges are laid, however, the choice of investigative targets, methods of information collection and exchange, and means of investigation generally will not be subject to judicial scrutiny, media coverage or public debate.

The courts have an attenuated role in national security investigations and prosecutions as a result of amendments to the *Criminal Code* made by the *Anti-terrorism Act*, which significantly reduced the extent of judicial oversight of the activities of law enforcement and security intelligence actors, especially in the area of surveillance.[70] The RCMP's national security investigations are frequently aimed primarily at preventing and disrupting terrorist activity, rather than prosecuting individuals after terrorist offences have been committed. The information and intelligence that enables law enforcement and security intelligence services to perform this function may be of such a nature that it would not be admissible as evidence in a criminal prosecution. Furthermore, the RCMP may

receive information in national security investigations that was originally collected by CSIS or the CSE, which are bound by different and, in many respects, less onerous legal standards regarding the use of electronic surveillance. In other areas, such as international information sharing, there is no judicial oversight whatsoever. As a result, in national security investigations, court scrutiny of government action against individuals for compliance with the Charter is less frequent. Rights and freedoms consequently may be eroded more easily.[71] The Canadian Bar Association has noted:

> [I]f an investigative agency gathers information knowing that there will not be a criminal charge, there may be even less incentive to respect guaranteed rights and freedoms.[72]

Below, I discuss statutory limits on judicial oversight of national security activities in relation to authorizations for the interception of private communications, the detention of terrorist suspects, and criminal prosecutions. Judicial oversight may also be restricted in the national security context by section 38 of the *Canada Evidence Act*, which I discuss earlier in this chapter. Moreover, under the *Immigration and Refugee Protection Act*, the courts are limited to the judicial review of executive decisions regarding security certificates.[73] No judicial determination on the merits is available. The limits on judicial scrutiny of the RCMP's national security activities should be a consideration in the design of a review body.

8.1 AUTHORIZATIONS

8.1.1 *Criminal Code*

The *Anti-terrorism Act* made significant changes to the judicial authorization procedure for communication surveillance warrants and the threshold for arrest of a suspect under the preventive detention powers.

Unlike the situation for other offences in the *Criminal Code*, communications intercept authorizations may be granted in terrorism investigations even where the same information could be obtained in a less invasive manner.[74] In addition to providing the police with easier access to intrusive surveillance methods, the *Criminal Code* allows a judge to authorize interceptions for longer periods of time and provides a relaxed test for delaying notification of surveillance subjects. The chart below summarizes the differences between the provisions

regarding interception of private communications in relation to terrorism offences[75] and in relation to regular criminal offences.

DIFFERENCES IN JUDICIAL AUTHORIZATIONS FOR INTERCEPTION OF COMMUNICATIONS

	Terrorism Offences	Regular Criminal Offences
Test to obtain	No requirement for investigative necessity. Interception would be in the best interests of justice.[76]	Proof of investigative necessity required, i.e., other methods have been tried and have failed, are unlikely to succeed or are impractical. Interception would be in the best interests of justice.[77]
Initial length of time	Up to one year.[78]	Up to 60 days.[79]
Renewals	Up to one year.[80]	Up to 60 days.[81]
Notification of suspect	Same as for regular offences.	Within 90 days of end of surveillance period.[82]
Extension of notification period	Up to three years.[83]	Up to three years.[84]
Criteria for granting extension	No continuing investigation requirement. Extension must be in the interests of justice.[85]	Investigation must be continuing.[86] Extension must be in the interests of justice.[87]

As may be seen from the chart, the *Criminal Code* amendments allow the police to use invasive methods of surveillance without demonstrating the actual or likely failure of other methods, continue surveillance for quadruple the usual length of time with no judicial review, and delay notification of the subject of the surveillance for three years after the investigation has been completed.[88] Without debating the merits of these provisions here, I note that the decreased judicial oversight for electronic surveillance is an issue that has implications for the design of an appropriate review mechanism for the RCMP's national security activities.

One of the new powers that the *Criminal Code* gives law enforcement authorities to deal with the threat of terrorism is that of preventive arrest,[89] for

which it sets a lower threshold than for the normal power of arrest. A terrorist suspect may be arrested and subjected to restrictive, court-ordered conditions without being charged with a criminal offence. While the requirement for the Attorney General's consent provides some balance, law enforcement agencies have greater discretion and are subject to less judicial scrutiny when they employ this extraordinary power. Where a warrant is obtained or an individual is held until he or she appears before a judge, the use of the preventive arrest power is subject to judicial oversight. However, where an individual is detained based on an officer's suspicion and then released before the detention is reviewed, there is no provision for judicial oversight regarding the propriety of the detention.

The Attorney General is required to make annual reports to Parliament on the use of the investigative hearing and preventive arrest powers. However, these reports may not disclose any confidential national security information[90] and there is no requirement to report the number of warrantless arrests made under section 83.3(4) of the *Criminal Code* where the individual was released prior to appearing before a judge. The reports provide very little information. For instance, the summary on the use of the investigative hearing and preventive detention powers in the 2004–2005 report states only that no applications were initiated and that there are no data to report.[91]

There is no question about the legitimate need for confidentiality in national security matters. However, the lack of detailed information in these reports does little to allay public concerns regarding the use and potential abuse of powers.[92] An independent review agency could review the use of the preventive arrest power in detail. As the Canadian Arab Federation and Canadian Council on American–Islamic Relations emphasized in their oral presentation to the Inquiry, an independent review body will help ensure that these extraordinary provisions are being used appropriately and in accordance with Charter values, thereby increasing the confidence of all Canadians in the RCMP.[93]

My final comment on the attenuation of judicial oversight in respect of the investigation of terrorist offences relates to the prospect that search warrants may be sealed under section 38 of the *Canada Evidence Act*. Sealing a warrant prevents public scrutiny at this stage of the investigation, creating an additional need for effective review in a context where many investigations may never reach the prosecution stage.[94]

8.1.2
Communications Security Establishment

There are many players in national security investigations. The reduction or lack of judicial oversight in relation to the interception of private communications is not confined to the actions of law enforcement officials. Under the *National Defence Act*, the Communications Security Establishment (CSE) may intercept the private communications of Canadians and persons within Canada when targeting communications originating outside Canada,[95] subject to ministerial authorization. Thus, when the RCMP receives information from the CSE, it may come into possession of information that was not collected pursuant to a judicial authorization.

Canadian courts have no jurisdiction to issue warrants with respect to persons outside Canada.[96] The *National Defence Act* substitutes executive authorization for judicial authorization in relation to the interception of private communications of Canadian citizens or permanent residents, so long as the interception is directed at a foreign entity and satisfactory measures are in place to protect the privacy of Canadians.[97] *Criminal Code* requirements relating to wiretap authorizations do not apply to the CSE insofar as it operates under ministerial authorizations.[98] Information obtained by the CSE may be shared, subject to strict conditions, with other Canadian or foreign law enforcement or security services.[99]

Under the *National Defence Act*, ministerial authorization may be granted where the Minister of National Defence is satisfied of the following:

(a) the interception will be directed at foreign entities located outside Canada;
(b) the information to be obtained could not reasonably be obtained by other means;
(c) the expected foreign intelligence value of the information that would be derived from the interception justifies it; and
(d) satisfactory measures are in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security.[100]

The CSE Commissioner scrutinizes the legality of the CSE's interception of communications pursuant to ministerial authorizations, ensuring that the intercepts comply with the terms of the authorizations. However, the Commissioner does not review the Minister's decision to authorize interception. Thus, the authorization is not reviewed for compliance with the criteria set out in section 273.65(2) of the *National Defence Act* or in the Charter.[101]

8.2 PROSECUTIONS

In Canada, the rights of the accused in a criminal proceeding are safeguarded by an independent judiciary in the context of an adversarial trial. However, *Criminal Code* prosecutions for terrorist offences have been rare, and this will likely continue to be the case in the future. To date, there have been only two cases where charges have been laid under the Code's anti-terrorism provisions. In the event of criminal prosecutions for national security offences, both the *Criminal Code* and the *Canada Evidence Act* provide for procedures that may involve *in camera* proceedings. The *Criminal Code* allows both secret evidence and *in camera* proceedings in relation to the listing of terrorist entities, as well as the use of evidence received in confidence from foreign sources.[102] In addition, section 38 of the *Canada Evidence Act* may require secret proceedings and evidence.[103] Taken as a whole, these provisions mandate secrecy in some situations and therefore may intrude upon the ability of the accused to know the case to be met and may fetter the open court principle.[104] Judicial oversight may consequently be less complete and less effective than would otherwise be the case. Another important consideration is that public scrutiny and accountability are diminished.

The infrequent use of criminal prosecutions contrasts with the more common recourse to administrative detention under the *Immigration and Refugee Protection Act*.[105] Five men are currently subject to security certificates under the Act and three are in detention. Procedural safeguards available in the immigration context are inferior to those available to criminal defendants. The standards intended to ensure reliability of evidence in criminal trials do not apply.[106] When a section 38 certificate is issued under the *Canada Evidence Act* in a criminal proceeding, the information subject to the certificate may not be disclosed or introduced into evidence. Section 38.14 of the Act nevertheless does provide that a criminal trial judge may make any order that is necessary to protect the accused's right to a fair trial, including a stay of the criminal proceedings, provided it respects section 38. While both section 78 of the *Immigration and Refugee Protection Act* and section 38 of the *Canada Evidence Act* provide for *in camera* and *ex parte* hearings, section 78 of the *Immigration and Refugee Protection Act* allows a federal court judge to rely on information that may never be disclosed to the detainee, even in summary form, when reviewing the reasonableness of the Minister's decision to deport the individual. Moreover, as I mention above, judges of the Federal Court conducting a hearing under

section 78 may not evaluate security certificates on the merits[107] and the judge's decision on the reasonableness of a certificate may not be appealed.[108]

9. CONCLUSION

There are a number of common investigative activities relating to national security that, in the absence of criminal prosecutions, will probably not be subject to external judicial review. As well, those who are directly affected will probably never know about many of these actions, including decisions in regard to the following:

- selecting a subject for investigation;
- selecting associates of targets and initiating or extending investigations;
- initiating physical surveillance of individuals;
- interviewing individuals;
- designing questions to be asked of individuals;
- recruiting and using human sources to obtain information;
- inputting information into national security databases;
- receiving information from and imparting information to other Canadian institutions (federal and provincial police, security intelligence or other agencies or departments, such as the CBSA or Transport Canada);
- receiving information from and imparting information to foreign agencies;
- acting upon information provided by other agencies;
- referring matters to another agency (for proceedings under the *Immigration and Refugee Protection Act* rather than criminal proceedings, for example); and
- arresting and releasing individuals pursuant to the preventive detention provisions of the *Criminal Code*.

The reality is that many discretionary operational decisions will not be subject to judicial review, particularly when there is no prosecution. And while other aspects of RCMP national security activities, such as the issuance of search warrants, remain subject to judicial oversight, that oversight in some instances is attenuated when it comes to terrorism-related investigations and the exemption of certain information from aspects of both the *Access to Information Act* and *Privacy Act* regimes.

In taking measures to protect Canada's national security interests, we must always keep in mind the importance of protecting the rights and freedoms of individuals in Canada. In this regard, the words of the McDonald Commission ring true: "Canada must meet both the requirements of security and the requirements

of democracy: we must never forget that the fundamental purpose of the former is to secure the latter."[109]

Notes

1 Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, Freedom and Security Under the Law, Second Report, vol. 1 (Ottawa: Supply and Services Canada, 1981), p. 43 (Chair: D.C. McDonald) [McDonald Commission report].

2 *Suresh v. Canada (Minister of Citizenship and Immigration)*, [2002] 1 S.C.R. 3 at paras. 3–4.

3 See generally Victor Ramraj, Michael Hor and Kent Roach, eds., *Global Anti-Terrorism Law and Policy* (Cambridge: Cambridge University Press, 2005).

4 *United Nations Security Council Resolution 1373*, UN SCOR, 56th Sess., 4385th mtg., UN Doc. S/RES/1373 (2001), online, UN Security Council, http://daccessdds.un.org/doc/UNDOC/GEN/N01/557/43/PDF/N0155743.pdf?OpenElement (accessed Feb. 1, 2006).

5 For a sampling of concerns and views on these issues, see the essays collected in Ronald J. Daniels, Patrick Macklem and Kent Roach, eds., *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill* (Toronto: University of Toronto Press, 2001) [Daniels *et al.*]; David Daubney *et al.*, *Terrorism, Law & Democracy: How Is Canada Changing Following September 11?* Papers presented at a conference organized by the Canadian Institute for the Administration of Justice held in Montreal, Quebec, Mar. 25–26, 2002 (Montreal: Canadian Institute for the Administration of Justice, 2002); and, in the U.S. context, David Cole and James X. Dempsey, *Terrorism and the Constitution: Sacrificing Civil Liberties in the Name of National Security*, 2nd ed. (New York: The New Press, 2002).

6 The *Security of Information Act*, R.S.C. 1985, c. O-5 (as am. by the *Anti-terrorism Act*, S.C. 2001, c. 41), discussed in more detail in Chapter III, protects confidential government information. Confidential sources may also be safeguarded by the doctrine of police informer privilege. See *R. v. Leipert*, [1997] 1 S.C.R. 281 at paras. 9–14. See also *Royal Canadian Mounted Police Public Complaints Commission v. Canada (Attorney General)* (2005), 336 N.R. 101 (F.C.A.).

7 R.S.C. 1985, c. C-46, ss. 83.06, 83.28 (as am. by the *Anti-terrorism Act*, S.C. 2001, c. 41).

8 S.C. 2001, c. 27, s. 78.

9 S.C. 2001, c. 41, s. 113.

10 R.S.C. 1985, c. C-5, s. 38 (as am. by the *Anti-terrorism Act*, S.C. 2001, c. 41).

11 The problems inherent in the use of secret evidence have been highlighted by a number of groups in submissions to parliamentary committees. See, e.g., testimony of George D. Hunter, Vice-President of the Federation of Law Societies of Canada, before the Special Senate Committee on the *Anti-terrorism Act*, 38th Parl., 1st Sess. (Special Senate Committee on the *Anti-terrorism Act*), Oct. 17, 2005. p 16:24; Canadian Bar Association, "Submission on the Three Year Review of the Anti-terrorism Act," Submission to the Subcommittee on Public Safety and National Security of the Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness, House of Commons, 38th Parl., 1st Sess. (House Subcommittee on Public Safety and National Security) and the Special Senate Committee on the *Anti-Terrorism Act*, 2005, p. 31 [Canadian Bar Association submission to Parliament]; B'nai Brith Canada, "A Review of Canada's Anti-terrorism Act: Presentation to the House of Commons Subcommittee on Public Safety and National Security of the Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness and to the Senate of Canada Special Committee on the Anti-Terrorism Act," 2005, pp. 15–16; Testimony of Kathy Vandergrift,

Director of Policy, World Vision Canada, before the House Subcommittee on Public Safety and National Security, Sept. 20, 2005, pp. 9–10; Canadian Arab Federation, Canadian Council on American–Islamic Relations and Canadian Muslim Lawyers Association, "Joint Statement of Principles & Recommendations for Real Security," Submissions to the House Subcommittee on Public Safety and National Security, 2005 [Joint Statement of Principles].

12 See *R. v. Ottawa Citizen Group Inc.* (2005), 255 D.L.R. (4th) 149 (Ont. C.A.) at paras. 55, 64. See also British Columbia Civil Liberties Association, *National Security: Curbing the Excess to Protect Freedom and Democracy, A Brief Prepared for the House of Commons Subcommittee on Public Safety and National Security and the Senate Special Committee on the Anti-terrorism Act*, 2005 at 43 [B.C. Civil Liberties Association submission to Parliament]; Testimony of Faisal Joseph, Legal Counsel, Canadian Islamic Congress, before the House Subcommittee on Public Safety and National Security, Sept. 20, 2005 at 15 (all testimony cited to English version of the evidence); Canadian Civil Liberties Association, Written Submissions to the Senate Special Committee on the *Anti-terrorism Act*, 2005 at 12 [Canadian Civil Liberties Association Senate Committee submissions].

13 R.S.C. 1985, c. C-5, s. 38.

14 As defined in the *Security of Information Act*, s. 2(1).

15 *Canada Evidence Act*, s. 38.13.

16 Ibid., ss. 38.131, 38.14.

17 Lorne Sossin, "The Intersection of Administrative Law with the Anti-Terrorism Bill" in Daniels *et al.*, pp. 425–426 (see note 5).

18 Canadian Bar Association submission to Parliament, pp. 22–25 (see note [11]); Amnesty International, "Security through Human Rights: Amnesty International Canada's Submission to the Special Senate Committee on the Anti-Terrorism Act and House of Commons Sub-Committee on Public Safety and National Security as part of the Review of Canada's Anti-Terrorism Act," 2005, pp. 9–10 [Amnesty International submission to Parliament]; B.C. Civil Liberties Association submission to Parliament, pp. 54–57 (see note [11]); Jennifer Stoddart, "Position Statement on the *Anti-terrorism Act*: Submission of the Office of the Privacy Commissioner of Canada to the Senate Special Committee on the *Anti-terrorism Act*," May 9, 2005, online, www.privcom.gc.ca/media/nr-c/2005/ata_050509_e.asp (accessed July 24, 2006) [Privacy Commissioner of Canada Position Statement]; Testimony of John Reid, Information Commissioner of Canada, before the Special Senate Committee on the *Anti-terrorism Act*, May 30, 2005, p. 12:7; Ann Cavoukian, Information and Privacy Commissioner of Ontario, "Submission to the House of Commons Subcommittee on Public Safety and National Security regarding the Anti-Terrorism Act Review," 2005, p. 4, adopted by David Loukidelis, Information and Privacy Commissioner for British Columbia, in his submission to the House Subcommittee, 2005, p. 3 [Ontario and B.C. Information and Privacy Commissioners' House Subcommittee submissions]; Canadian Muslim Lawyers Association, Submission to the House Subcommittee on Public Safety and National Security, 2005, p. 15; Canadian Civil Liberties Association Senate Committee submissions, p. 14 (see note 12); Iris Almeida and Marc Porret, *Canadian Democracy at a Crossroads: the Need for Coherence and Accountability in Counter-Terrorism Policy and Practice* (Montreal: International Centre for Human Rights and Democratic Development, 2004), pp. 38–39; Jeremy Patrick-Justice, "Section 38 and the Open Courts Principle" (2005) 54 U.N.B.L.J. 218; Kent Roach, "Ten Ways to Improve Canadian Anti-Terrorism Law" (2005) 51 Crim. L.Q. 102.

19 Stanley Cohen, "State Secrecy and Democratic Accountability" (2005) 51 Crim. L.Q. 27, p. 33.

20 *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403.

21 *Access to Information Act*, R.S.C. 1985, c. A-1, ss. 13, 15, 16, 19.

22 *Criminal Code*, s. 83.28.

23 *Application under s. 83.28 of the Criminal Code (Re)*, [2004] 2 S.C.R. 248.

24 *Application under s. 83.28 of the Criminal Code (Re)*, 2003 BCSC 1172, aff'd [2004] 2 S.C.R. 248.

25 See discussion in Chapter III; *Criminal Code*, s. 83.3.

26 S.C. 2001, c. 41.

27 Kent Roach, "Did September 11 Change Everything? Struggling to Preserve Canadian Values in the Face of Terrorism" (2002) 47 McGill L.J. 893, p. 925–926. See also Kent Roach, *September 11: Consequences for Canada* (Montreal: McGill–Queen's University Press, 2003), ch. 4.

28 Stanley Cohen, "Law in a Fearful Society: How Much Security?" (2005), 54 U.N.B.L.J. 143, pp. 151, 153.

29 On this point, see "Submissions to Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar," (Written submission of the Canadian Civil Liberties Association, Arar Commission Policy Review Public Submissions), Feb. 2005, p. 1 [Canadian Civil Liberties Association submissions to Inquiry].

30 *United States v. Burns*, [2001] 1 S.C.R. 283.

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

32 *Application under s. 83.28 of the Criminal Code (Re)*, [2004] 2 S.C.R. 248.

33 This concern is expressed by the B.C. Civil Liberties Association in its submission to Parliament, p. 84 (see note 11). The Association recommends prohibiting reliance in any form by any court or agency on information that is derived from torture. The Association reiterated its concerns in its Policy Review submissions dated Mar. 2005, pp. 21–22 and in its oral presentation to me: Oral Submission of Jason Gratl, Transcript of Arar Commission Policy Review Public Hearing, Nov. 18, 2005, pp. 609–610. The Canadian Bar Association submission to Parliament, at p. 17 (see note [11]) also expresses concerns about the possibility of information being obtained by torture and about the reliability of any information obtained from foreign sources. See also *A (FC) v. Secretary of State*, [2005] UKHL 71, in which it is affirmed that evidence obtained through torture should not be used.

34 Philip B. Heymann, "Civil Liberties and Human Rights in the Aftermath of September 11" (2002) 25 Harv. J.L. & Pub. Pol'y 441, pp. 453–454. See also "Submissions to Factual Inquiry and Policy Review on Behalf of The Redress Trust, the Association for the Prevention of Torture and the World Organisation Against Torture," paras. 68–80, 97–98; Oral Submissions of Carla Ferstman for The Redress Trust, the World Association For the Prevention of Torture and the World Organisation Against Torture, Transcript of Arar Commission Policy Review Public Hearing (Nov. 15, 2005), pp. 79–80; Oral Submissions of Hilary Homes for Amnesty International, Transcript of Arar Commission Policy Review Public Hearing (Nov. 16, 2005), pp. 192–193, 198–201; Oral Submissions of Riad Saloojee for the Canadian Arab Federation and Canadian Council on American–Islamic Relations, Transcript of Arar Commission Policy Review Public Hearing (Nov. 17, 2005), pp. 222–223.

35 McDonald Commission report, p. 513.

36 *R. v. Dyment*, [1988] 2 S.C.R. 417 at 428, per La Forest J. (concurring). See also Daniel J. Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy" (2000–01) 53 Stanford L. Rev. 1393, pp. 1413, 1436.

37 19 Dec. 1966, 999 U.N.T.S. 171, art. 17, online, Office of the High Commissioner for Human Rights, http://www.unhchr.ch/html/menu3/b/a_ccpr.htm (accessed Aug. 2, 2006).

38 *Privacy Act*, R.S.C. 1985, c. P-21, s. 12.

39 Ibid., ss. 19, 21, 22, 23.

40 [2002] 4 S.C.R. 3.

41 *Exempt Personal Information Bank Order, No. 13 (RCMP)*, S.O.R./90-149.

42 *Exempt Personal Information Bank Order, No. 14 (CSIS)*, S.O.R./92-688.

43 *Exempt Personal Information Bank Order, No. 25 (RCMP)*, S.O.R./93-272.

44 Oral Submissions of Jennifer Stoddart, Privacy Commissioner of Canada, Transcript of Arar Commission Policy Review Public Hearing (Nov. 16, 2005), pp. 113–114 [Privacy Commissioner of Canada oral submissions to Inquiry]; Oral Submissions of Warren Allmand for the International Civil Liberties Monitoring Group, Transcript of Arar Commission Policy Review Public Hearing (Nov. 17, 2005), p. 445–446. See also Privacy Commissioner of Canada Position Statement (see note 18). Tamra Thomson, Director of Legislation and Law Reform for the Canadian Bar Association, has recommended to Parliament that these exemptions be repealed or specific safeguards be put into place to protect individual privacy: Testimony of Tamra Thomson before the Special Senate Committee on the *Anti-terrorism Act*, May 2, 2005, pp. 9:28–9:29.

45 See "Policy Review of the Commission of Inquiry in Relation to Maher Arar" (Written submission of the Canadian Bar Association, Arar Commission Policy Review Public Submissions), Nov. 2005, p. 5 [Canadian Bar Association submission to Inquiry].

46 *R. v. Dyment*, [1988] 2 S.C.R. 417 at 429–430.

47 This point was made by the Canadian Bar Association in its submission to the Inquiry, pp. 8–9 (see note 45).

48 For a critical perspective on the exercise of discretion under the *Anti-terrorism Act*, see W. Wesley Pue, "The War on Terror: Constitutional Governance in a State of Permanent Warfare?" (2003) 41 Osgoode Hall L.J. 267, pp. 281–285.

49 Canada's use of immigration law rather than criminal law to deal with suspected terrorists is a subject of concern to the UN Committee against Torture: United Nations Committee against Torture, "Consideration of Reports Submitted by States Parties Under Article 19 of the Convention: Conclusions and Recommendations of the Committee against Torture, Canada," UN CATOR, 34th Sess., UN Doc. CAT/C/CO/34/CAN (2005), para. 4(e). Canada submits periodic reports to the Committee under the *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*, 10 Dec. 1984, 1465 U.N.T.S. 585, online, http://www.ohchr.org/english/law/cat.htm (accessed Aug. 4, 2006). See also testimony of Jean-Paul Laborde, Chief, Terrorism Prevention Branch, United Nations Office on Drugs and Crime, before the Special Senate Committee on the *Anti-terrorism Act*, June 20, 2005, pp. 14:16–14:17, stating that a state's first obligation under U.N. Security Council Resolution 1373, para. 2 is to prosecute or extradite suspected terrorists. Removal should be considered only where there is insufficient evidence to prosecute.

50 *Immigration and Refugee Protection Act*, s. 78; Audrey Macklin, "Borderline Security" in Daniels *et al.* (see note 5). Considerable controversy has been created by the federal government's attempt to deport several men detained pursuant to security certificates under the *Immigration and Refugee Protection Act* despite the existence of pre-removal risk assessments finding that the men would face a significant risk of torture if returned to their home countries. See, e.g., Amnesty International submission to Parliament, p. 18 (see note 18); Canadian Jewish Congress, "Brief to the House Subcommittee on Public Safety and National Security of the Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness on its Review of the Anti-terrorism Act (ATA) and Related Security Matters," 2005, p. 5; Canadian Council for Refugees, "Brief to the House of Commons Subcommittee on Public Safety and National Security of the Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness – Anti-terrorism Act Review," 2005, pp. 7–8.

51 *Andrews v. Law Society of British Columbia*, [1989] 1 S.C.R. 143.

52 Such discretion is arguably protected from political interference, at least in its specific application, by the principle of "police independence." See on this point the discussion of police independence in Chapter IX.

53 *Little Sisters Book and Art Emporium v. Canada (Minister of Justice)*, [2000] 2 S.C.R. 1120.

54 See, e.g., Application for Standing of the Council of Canadians and the Polaris Institute, Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (Arar Commission), p. 6; Application for Standing of the Canadian Labour Congress, Arar Commission, pp. 3–4; Application for Standing of the Muslim Community of Ottawa-Gatineau, Arar Commission, pp. 10–11; Application for Standing of the Canadian Council on American–Islamic Relations, Arar Commission, p. 7; Application for Standing of the Canadian Arab Foundation, Arar Commission, p. 3; Application for Standing of the Muslim Canadian Congress, Arar Commission, p. 4.

55 Sujit Choudhry and Kent Roach, "Racial and Ethnic Profiling: Statutory Discretion, Constitutional Remedies, and Democratic Accountability" (2002) 41 Osgoode Hall L.J. 1, para. 2 (QL) [Choudhry and Roach]. See also *R. v. Brown* (2003), 64 O.R. (3d) 161 (C.A.) at paras. 9, 42–46**;** *Report of the Commission on Systemic Racism in the Ontario Criminal Justice System* (Toronto: Queen's Printer for Ontario, 1995) (Co-Chairs: M. Gittens and D. Cole), p. 358.

56 See National Organization of Immigrant and Visible Minority Women of Canada, "Submission to the Special Senate Committee on the Review of the Anti-terrorism Act," Oct. 17, 2005, pp. 6–7.

57 Canadian Bar Association submission to Parliament, p. 4 (see note 11).

58 Choudhry and Roach, para. 58 (see note 55); Reem Bahdi, "No Exit: Racial Profiling and Canada's War Against Terrorism" (2003) 41 Osgoode Hall L.J. 293, para. 6 (QL); Lesley A. Jacobs, "Securer Freedom for Whom: Risk Profiling and the New *Anti-Terrorism Act*," Book Review (2003) 36 U.B.C.L. Rev. 375. A similar worry has been expressed by Muslim groups, which would like to see the government provide quantifiable data on the ethnicity, religion and citizenship of individuals interviewed or otherwise investigated by the government bodies involved in national security: Joint Statement of Principles (see note 11); Testimony of Ziyaad Mia**,** Former Director, Canadian Muslim Lawyers Association, before the Special Senate Committee on the *Anti-terrorism Act*, May 2, 2005, p. 9:36.

59 *Criminal Code*, s. 83.01(1)(b).

60 See, e.g., Kent Roach, "The New Terrorism Offences and the Criminal Law" in Daniels *et al.*, p. 156 (see note 5); Canadian Civil Liberties Association submissions to Inquiry, p. 3 (see note 29); Amnesty International submission to Parliament, p. 16 (see note 18); International Civil Liberties Monitoring Group, "Submission Concerning the Review of the Anti-Terrorism Act," Brief to the House Subcommittee on Public Safety and National Security, 2005, p. 7; Canadian Association of University Teachers, "Submission to the House of Commons Subcommittee on Public Safety and National Security Regarding the Review of the *Anti-terrorism Act*," 2005, p. 23; Statement by Ed Cashman, Regional Executive Vice-President, Public Service Alliance of Canada, to the Special Senate Committee on the *Anti-terrorism Act*, Sept. 26, 2005; Joint Statement of Principles (see note 11).

61 Stanley Cohen, "Law in a Fearful Society: How Much Security?" (2005), 54 U.N.B.L.J. 143, p. 158.

62 On this point, see, e.g., B.C. Civil Liberties Association submission to Parliament, pp. 43–46 (see note 11), specifically the Association's critique of the RCMP's actions in relation to Younus Kathrada.

63 McDonald Commission report, pp. 445–511.

64 Ibid., p. 46. See also pp. 47, 409.

65 See, e.g., David Schneiderman and Brenda Cossman, "Political Association and the Anti-Terrorism Bill" in Daniels *et al.*, pp. 173–194 (see note 5).

66 *Criminal Code*, ss. 83.18–83.23.

67 Canadian Bar Association submission to Parliament, p. 33 (see note 11); World Vision Canada, Submission to the House Subcommittee on Public Safety and National Security, 2005; Imagine Canada, "Submission to the Senate Special Committee on the *Anti-terrorism Act*," 2005, pp. 3–8.

68 See, e.g., testimony of Omar Alghabra, National President of the Canadian Arab Federation, before the Special Senate Committee on the *Anti-terrorism Act*, June 13, 2005 at 13:34, arguing that there has been a chill in civic and religious participation amongst Muslims in Canada; Testimony of Thomas Hegghammer, Senior Analyst with the Norwegian Defence Research Establishment, before the Special Senate Committee on the *Anti-terrorism Act*, Mar. 14, 2005 at 4:20, stating that many imams in Norway and Britain do not discuss political issues in mosques, even in a moderate vein, for fear of coming to the attention of the security services. See also the judgment of the U.S. Supreme Court in *United States v. United States District Court*, 407 U.S. 297 (1972) at 314.

69 Canadian Civil Liberties Association submissions to Inquiry, p. 5 (see note 29).

70 Privacy Commissioner of Canada oral submissions to Inquiry, pp. 112–113 (see note 44). See also Privacy Commissioner of Canada Position Statement (see note 18), where the Privacy Commissioner questions whether this change is necessary or desirable.

71 Some groups have called for a greater emphasis on prosecutions in the national security context. See, e.g., testimony of David Morris, former member of the Board of Directors, Canadian Lawyers for International Human Rights, before the Special Senate Committee on the *Anti-terrorism Act*, May 2, 2005, pp. 9:39–9:40, arguing that, where measures other than criminal prosecutions are used in a national security context, the government and the security establishment should be required to demonstrate the necessity and effectiveness of the measures taken.

72 Canadian Bar Association submission to Parliament, p. 20 (see note 11).

73 *Immigration and Refugee Protection Act*, ss. 78ff.

74 This change is criticized in the Privacy Commissioner of Canada Position Statement (see note 18), in which the Commissioner argues that the investigative necessity requirement should be reintroduced.

75 Organized crime offences are treated in the same way as terrorism offences in the *Criminal Code* in regard to the interception of private communications.

76 *Criminal Code*, ss. 185(1.1), 186 (1.1).

77 Ibid., ss. 185(1), 186(1).

78 Ibid., s.186.1(c).

79 Ibid., s. 186(4)(e).

80 Ibid., s. 186.1(c).

81 Ibid., s. 186(7).

82 Ibid., s. 196(1).

83 Ibid., s. 185(2).

84 Ibid., s. 185(2).

85 Ibid., s. 196(5).

86 Ibid., s. 196(3). The continuing investigation must relate to an authorized offence, or the subsequent investigation of an offence listed in s. 183 of the *Criminal Code*, commenced as a result of information obtained from the investigation of the authorized offence.

87 Ibid., s. 196(3).

88 In her submission to the Special Senate Committee on the *Anti-terrorism Act*, the Privacy Commissioner of Canada states that this change has serious implications for individual privacy and argues that the ordinary time limits should apply to electronic surveillance warrants in national security investigations: Privacy Commissioner of Canada Position Statement (see note 18). Similarly, the Canadian Bar Association contends that delayed notice of wiretap warrants

diminishes the accountability of law enforcement officials: Canadian Bar Association submission to Parliament, p. 25 (see note 11). See also Ontario and B.C. Information and Privacy Commissioners' House Subcommittee submissions, p. 3 (see note 18). On the other hand, the lack of harmonization of notice periods can hamper police investigations. While notification of a wiretap can be delayed for three years, notification times relating to search warrants and other technical searches are for shorter periods. Hence, an investigative target can be alerted to an investigation even where a delay in notification has been granted by a court: Giuliano Zaccardelli, Commissioner, RCMP, Testimony before the Senate Special Committee on the *Anti-Terrorism Act*, Apr. 11, 2005, p. 7:29.

89 *Criminal Code*, s. 83.3. The preventive arrest provisions apply only to persons suspected of involvement with terrorism.

90 *Criminal Code,* s. 83.31.

91 Attorney General of Canada, *Annual Report concerning Investigative Hearings and Recognizance with Conditions*, Dec. 24, 2004–Dec. 23, 2005, SECTION III – STATISTICS, online, Department of Justice Canada, http://www.justice.gc.ca/en/anti_terr/annualreport_2004-2005.html (accessed Aug. 3, 2006).

92 In their joint Policy Review submissions, the Canadian Arab Federation and Canadian Council on American–Islamic Relations expressed concern about reports from members of Canada's Muslim and Arab communities that the RCMP and CSIS have inappropriately threatened to use the preventive arrest powers to intimidate individuals during interviews or compel their co-operation in investigations: "Policy Review Submissions" (Written submission of the Canadian Arab Federation and Canadian Council on American–Islamic Relations, Arar Commission Policy Review Public Submissions), Feb. 21, 2005, pp. 10–11. This concern is based on anecdotal accounts collected in a publication by the Canadian Council on American–Islamic Relations submitted to the Inquiry, *Presumption of Guilt: A National Survey on Security Visitations of Canadian Muslims*, online, Canadian Council of American-Islamic Relations, http://www.caircan.ca/downloads/POG-08062005.pdf (accessed Jan. 12, 2006).

93 Oral Submissions of Riad Saloojee for the Canadian Arab Federation and Canadian Council on American–Islamic Relations, Transcript of Arar Commission Policy Review Public Hearing, Nov. 17, 2005, pp. 220–221, 229–230.

94 See *Ottawa Citizen Group Inc. v. Canada (Attorney General)* (2004), 122 C.R.R. (2d) 359, especially Justice Lufty's "Post scriptum: too much secrecy???" at paras. 34–45.

95 R.S.C. 1985, c. N-5, s. 273.65 (as am. by the *Anti-terrorism Act*).

96 Rt. Hon. Antonio Lamer, Communications Security Establishment Commissioner, "Note for Remarks to the Special Senate Committee on the Three Year Review of the *Anti-Terrorism Act*," 2005, p. 2.

97 See Privacy Commissioner of Canada Position Statement (see note 18), arguing that prior judicial authorization should be required to allow the CSE to intercept the Canadian end of private conversations. A warrant similar to those provided for under the *Canadian Security Intelligence Service Act* could be required.

98 *National Defence Act*, s. 273.69.

99 See testimony of Keith Coulter, Chief, CSE, before the Special Senate Committee on the *Anti-terrorism Act*, Apr. 11, 2005, pp. 7:43–7:44, 7:52; Testimony of John Ossowski, Director General, Policy and Communications, CSE, before the Special Senate Committee on the *Anti-terrorism Act*, Apr. 11, 2005, p. 7:48.

100 *National Defence Act*, s. 273.65(2).

101 The CSE Commissioner most likely would not have access to the Cabinet confidences on which the ministerial authorization was based: testimony of the Rt. Hon. Antonio Lamer, Commissioner, Communications Security Establishment, before the House Subcommittee on Public Safety and National Security, June 15, 2005, p. 8.

102 *Criminal Code*, ss. 83.05(6)(a), 83.06.

103 See ss. 38.02(1)(c), 38.11(1), 38.12(2), 38.13(5), 38.13(8). See also *Ottawa Citizen Group Inc. v. Canada (Attorney General)* (2004),122 C.R.R. (2d) 359 at paras. 34–45. Justice Lufty states at para. 44 that s. 38 is "the antithesis" of the open court principle, "a cornerstone of our democracy."

104 See *Vancouver Sun (Re)*, [2004] 2 S.C.R. 332.

105 *Immigration and Refugee Protection Act*, ss. 78ff.

106 Ibid., s. 78(j).

107 Ibid., ss. 80(1), 80(2).

108 Ibid., s. 80(3). See generally Hamish Stewart, "Is Indefinite Detention of Terrorist Suspects Really Constitutional?" (2005) 54 U.N.B.L.J. 234.

109 McDonald Commission report, p. 43.

IX
Fundamental Objectives of Review

1.
INTRODUCTION

Before turning to an assessment of the status quo and to my specific recommendations on a review mechanism for the national security activities of the RCMP, the objectives of such a mechanism need to be set out. The overarching objective can be simply stated: a review mechanism should work to ensure that the RCMP is accountable for its national security activities. In a democratic system of government based upon the protection of individual rights and freedoms, every public institution — and particularly every institution with powers that can profoundly affect the lives of Canadians, like a police force — must be answerable for its activities.

In police work in general, and arguably more so in national security police work, the police require considerable powers of intrusion. However, those powers must have limits. Most fundamentally, they must be exercised within the context of the values of our free and democratic society — liberty, the rule of law, the principles of fundamental justice and respect for equality. The police are given powers on the condition that they will exercise those powers within the limits of this context. A basic principle of our system is that public institutions, including the police, must be answerable for acting outside the limits placed on their powers.

The RCMP is accountable to the Minister, who is politically responsible for the Force in Parliament, and to the courts, which review the legality of RCMP activities in a range of contexts. Ultimately, the RCMP, the Minister and the courts are all accountable to the public at large, on whose behalf each institution operates.

This overarching objective of working to ensure accountability can be broken down into three more specific objectives:

1) to provide assurance that RCMP activities are in conformity with the *Canadian Charter of Rights and Freedoms* (the Charter), the law and the standards of propriety that are accepted in Canadian society;
2) to foster accountability of the RCMP to government; and
3) to foster accountability to the public, thereby maintaining and enhancing public trust and confidence in the RCMP.

These three objectives are subject to an important institutional or functional imperative: a review mechanism should not function so as to itself impair national security, nor should it impair the lawful and appropriate conduct of the RCMP and the operation of the criminal justice system. In Chapter VIII, I set out several features of national security activities that speak to the need for enhanced review. Other features of national security, including some of those mentioned in Chapter VIII, must also be considered in designing a review mechanism so as not to endanger Canadians' national security or unduly hinder the operation of the criminal justice system. For example, the need to respect and protect the secrecy of certain information is a critical component of the national security activities of the RCMP and other national security actors, and a review mechanism must not operate so as to expose information that should remain secret. A review mechanism should also recognize that RCMP national security activities are highly integrated with those of other federal and provincial police and other agencies. Integration is a key element of the Government's approach to national security, and a review mechanism must function effectively within the framework of integration.

I discuss each objective in greater detail below. Before turning to the objectives, however, it is important that I set out what I mean by a review mechanism.

2.
REVIEW VERSUS OVERSIGHT

The terms of reference that form the basis of this Inquiry direct me to make recommendations on "an independent arm's-length review mechanism for the activities of the Royal Canadian Mounted Police with respect to national security."[1] In the literature on the subject, "review" is sometimes used to mean a particular type of accountability mechanism. While details and features differ, "review mechanism" generally refers to a mechanism that assesses an organization's activities against standards like lawfulness and/or propriety, and delivers a report

of that assessment, with recommendations, to those in government politically responsible for the organization. Activities are usually examined after they have occurred. In this model, a review mechanism is not responsible for carrying out recommendations. It remains at arm's length from both the management of the organization being reviewed and from the government.

Other accountability mechanisms are more directly involved in managing the organization in question. These are sometimes referred to as "oversight" mechanisms. Again, while features vary, oversight mechanisms are often directly involved in the decision making of the organization they oversee. Involvement can be through setting standards against which the organization's activities are evaluated, pre-approving operations, implementing and enforcing recommendations, and/or imposing discipline. The organization's activities are sometimes assessed while they are going on. In their pure forms, oversight mechanisms can be seen as direct links in the chain of command or accountability: they both review and are responsible for the activities of the overseen body. By contrast, review mechanisms are more appropriately seen as facilitating accountability: they ensure that the entities to which the organization under review is accountable, and the public, receive an independent assessment of that organization's activities.

In conducting the Policy Review, I have not confined my research and investigations to review mechanisms as defined above. I have examined a broad range of accountability mechanisms. Indeed, it is apparent from my examination that very few accountability mechanisms used in Canada or abroad can be neatly categorized as either wholly "review" or wholly "oversight." Most are a hybrid of the features described above.[2] However, the terms are useful in assessing the general approach that is most appropriate for the RCMP's national security activities. There are two choices:

- a mechanism that facilitates the accountability structure already in place by examining completed activities (review); or
- a mechanism that itself becomes to some extent responsible for directing the RCMP's activities and so involves a change to the accountability structure (oversight).

I am satisfied that the most appropriate accountability mechanism for the RCMP's national security activities is a review model. An oversight mechanism could confuse, or even lessen, both the RCMP's accountability to government and government's responsibility for the RCMP. A body that engages in oversight might also lose some of its independence from the RCMP and become implicated in decisions that should be subject to independent review after the fact.

Most importantly, I base my conclusion on the fact that an oversight mechanism would not respect the doctrine of police independence.

2.1 POLICE INDEPENDENCE AND ACCOUNTABILITY

The doctrine of police independence gives police a significant level of independence from government, and any discussion of RCMP accountability and government responsibility must take this fact into account.

The outer limits of the doctrine of police independence continue to evolve, but its core meaning is clear: the Government should not direct police investigations and law enforcement decisions in the sense of ordering the police to investigate, arrest or charge — or not to investigate, arrest or charge — any particular person. The rationale for the doctrine is the need to respect the rule of law. If the Government could order the police to investigate, or not to investigate, particular individuals, Canada would move towards becoming a police state in which the Government could use the police to hurt its enemies and protect its friends, rather than a free and democratic society that respects the rule of law.

The modern origin of the doctrine of police independence is found in a 1968 British common law case, *Ex Parte Blackburn*, in which Lord Denning stated the following:

> I have no hesitation in holding that, like every constable in the land, [the Commissioner of the London Police] should be, and is, independent of the executive. He is not subject to the orders of the Secretary of State, save that under the Police Act, 1964, the Secretary of State can call upon him to give a report, or to retire in the interests of efficiency. I hold it to be the duty of the Commissioner of Police of the Metropolis, as it is of every chief constable, to enforce the law of the land. He must take steps so to post his men that crimes may be detected; and that honest citizens may go about their affairs in peace. He must decide whether or not suspected persons are to be prosecuted; and, if need be, bring the prosecution or see that it is brought. But in all these things he is not the servant of anyone, save of the law itself. No Minister of the Crown can tell him that he must, or must not, keep observation on this place or that; or that he must, or must not, prosecute this man or that one. Nor can any police authority tell him so. The responsibility for law enforcement lies on him. He is answerable to the law and to the law alone. [3]

This articulation of a broad doctrine of police independence has been influential, and many courts have accepted it. Most recently, the Supreme Court

of Canada, in *R. v. Campbell and Shirose*,[4] accepted Lord Denning's articulation in relation to the police where they are engaged in criminal investigations.

However, Lord Denning's statement has also been the subject of debate. Several commentators have questioned whether Lord Denning should have based the doctrine of police independence on a series of civil liability cases holding that there was no master and servant relationship between the police and the government.[5] Others have argued that Lord Denning wrongly synthesized the idea that the police should be immune from improper political control or direction with the broader and different idea that the police should not be answerable to the responsible minister, but only in a court of law. Although judicial review is an important restraint on the police, it generally occurs only in cases that result in criminal charges and trials. As discussed in Chapter VIII, most of the RCMP's national security activities do not result in criminal charges or trials.

In *Campbell and Shirose,* the Crown tried to defend police conduct in conducting a "reverse sting" operation, in which RCMP officers sold drugs to the accused, on the basis that the police were part of the Crown or agents of the Crown and protected by the Crown's public interest immunity. Justice Binnie for the unanimous Supreme Court rejected such an argument:

> The Crown's attempt to identify the RCMP with the Crown for immunity purposes misconceives the relationship between the police and the executive government when the police are engaged in law enforcement. A police officer investigating a crime is not acting as a government functionary or as an agent of anybody. He or she occupies a public office initially defined by the common law and subsequently set out in various statutes.[6]

The Court noted that the RCMP "perform a myriad of functions apart from the investigation of crimes" and that "[s]ome of these functions bring the RCMP into a closer relationship to the Crown than others." However, the Court stressed that "in this appeal . . . we are concerned only with the status of an RCMP officer in the course of a criminal investigation, and in that regard the police are independent of the control of the executive government."[7] The Court noted that this principle "underpins the rule of law,"[8] which "is one of the 'fundamental and organizing principles of the Constitution.'"[9] The Court also quoted with approval the extract from Lord Denning's 1968 decision in *Ex Parte Blackburn* set out above.

The *Campbell and Shirose* case is significant in its recognition of the doctrine of police independence from the executive in the context of criminal investigations and its connection of the principle to the rule of law.[10] The rule of

law stresses the importance of impartially applying the law to all, and especially to those who hold state and governmental power.

I am not suggesting that police independence is, or ought to be, absolute. Complete independence would run the risk of creating another type of police state, one in which the police would not be answerable to anyone. Two principal lines of accountability prevent this second form of police state: the rule of law; and answerability to the responsible Minister, the elected government and ultimately the people.

As well as being the foundation of the doctrine of police independence, the rule of law is important in holding the police answerable for their conduct. As discussed in Chapter VIII, the courts play an important role in ensuring that the police operate within the framework of the law. For example in criminal cases that reach the courts, police activities in investigating crimes are examined and assessed against legal, including Charter, standards.[11] Courts also play a role in authorizing certain police activities such as electronic surveillance and search and seizure powers.[12] As I have noted, however, only a small part of the RCMP's national security activities are reviewed by the courts, particularly in the national security context. Thus, while the line of accountability to the courts is important, it does not include all relevant activities.

The elected government also has an important role in ensuring that police forces remain accountable and answerable for their conduct. In some cases this role is manifested through a requirement that action not be taken without special government authorization. For example, the RCMP and other police forces must have the Attorney General's consent before laying charges for a terrorism offence under the *Criminal Code* or the *Security of Information Act*, and before using the extraordinary police powers of investigative hearings or preventative arrests related to terrorism investigations. As this approval requirement relates directly to individual criminal investigations, it can be seen as a restraint on the doctrine of police independence. The extraordinary nature of police powers and the serious implications of crimes affecting national security have resulted in a narrowing of police independence in relation to this type of criminal behavior. In their submissions to me, the RCMP acknowledged that these consent requirements "provide[d] a sober second thought on operational decisions."[13]

The Minister responsible for the RCMP, the Minister of Public Safety (the Minister), also has a more general accountability function. As described in Chapter II, section 5 of the *Royal Canadian Mounted Police Act* (*RCMP Act*) provides that while the Commissioner of the RCMP has the control and management of the Force, he or she does so "under the direction of the Minister."[14] However, this power of direction must be interpreted in the context of the doc-

trine of police independence developed in *Campbell and Shirose*. In that case, Justice Binnie explained:

> While for certain purposes the Commissioner of the RCMP reports to the Solicitor General, the Commissioner is not to be considered a servant or agent of the government while engaged in a criminal investigation. The Commissioner is not subject to political direction. Like every other police officer similarly engaged, he is answerable to the law and, no doubt, to his conscience.[15]

As Justice Hughes commented in his APEC report: "In respect of criminal investigations and law enforcement generally, the Campbell decision makes it clear that, despite section 5 of the RCMP Act, the RCMP are fully independent of the executive. The extent to which police independence extends to other situations remains uncertain."[16]

While the doctrine of police independence limits the Minister's ability to direct individual criminal investigations, the power set out in section 5 of the *RCMP Act* has been used by the Minister to provide policy directives[17] that do not interfere with individual investigations. The directives provide critical ministerial direction for how RCMP activities are to be carried out generally. For example, in April 2002 and November 2003 the Minister issued four directives that provide important guidance for the RCMP's national security activities. They provide that RCMP national security investigations are to be coordinated at National Headquarters; that the RCMP must inform the Minister of high-profile national security investigations; that information sharing with foreign intelligence agencies requires ministerial approval; and that national security investigations in sensitive sectors must be pre-approved by the Assistant Commissioner, Criminal Intelligence Directorate, and, in relation to post-secondary institutions, must not "impact upon the free flow and exchange of ideas normally associated with an academic milieu."[18]

The extent of the Minister's ability to issue directives in a way that is consistent with the principle of police independence is evolving. Other commissions of inquiry have commented on this issue. For example, the McDonald Commission considered the concept of police independence at some length and concluded that:

> [T]he Minister should have no right of direction with respect to the exercise by the R.C.M.P. of the powers of investigation, arrest and prosecution. To that extent, and to that extent only, should the English doctrine expounded in *Ex parte Blackburn* be made applicable to the R.C.M.P.[19]

However, even with respect to the "quasi judicial" police functions of investigation, arrest and prosecution, the McDonald Commission distinguished between control and direction on the one hand, and accountability on the other. It concluded that the Minister should have the right to be:

> informed of any operational matter, even one involving an individual case, if it raises an important question of public policy. In such cases he may give guidance to the Commissioner and express to the Commissioner the government's view of the matter, but he should have no power to give *direction* to the Commissioner [emphasis in original].[20]

The McDonald Commission expressed serious reservations about the idea that the responsible minister should be kept ignorant of day-to-day police operations. It believed that such an approach could undermine ministerial responsibility for RCMP policies. The Commission wanted to prevent any misunderstanding that important "questions concerning the distinction between legitimate dissent and subversive threats to the security of Canada" and about the "legality and propriety of a particular method of collecting intelligence in the context of a particular case," would fall under the operational independence of the police. In the Commission's view, the police should be answerable to the Minister for such policy decisions, and the Minister in turn should be answerable to Parliament for RCMP policies. [21]

The Independent Commission on Policing for Northern Ireland (the Patten Commission) concluded that the term "police independence" should be replaced by the term "police responsibility," to highlight the distinction between legitimate police independence from direction or control and illegitimate claims that the police are not answerable for their activities. It argued as follows:

> Long consideration has led us to the view that the term "operational independence" is itself a large part of the problem. In a democratic society, all public officials must be fully accountable to the institutions of that society for the due performance of their functions, and a chief of police cannot be an exception. No public official, including a chief of police, can be said to be "independent". Indeed, given the extraordinary powers conferred on the police, it is essential that their exercise is subject to the closest and most effective scrutiny possible. The arguments involved in support of "operational independence" — that it minimises the risk of political influence and that it properly imposes on the Chief Constable the burden of taking decisions on matters about which only he or she has all the facts and expertise needed — are powerful arguments, but they support a case not for "independence"

> but for "responsibility". We strongly prefer the term "operational responsibility" to the term "operational independence".[22]

Police operational responsibility as conceived by the Patten Commission involves the right of police to make decisions free from external direction or control. However, it rejects the idea that police "conduct of an operational matter should be exempted from inquiry or review after the event by anyone."[23]

I agree with both the McDonald Commission and the Patten Commission that there is an important distinction between control and direction on the one hand, and accountability on the other. Section 5 of the *RCMP Act* gives the Minister, and government in general, an important role with respect to each. The Minister has a responsibility to provide policy direction to the RCMP. While direction of operational matters is more controversial, I agree with the McDonald Commission that "if it raises an important question of public policy . . . . [the Minister] may give guidance to the Commissioner and express to the Commissioner the government's view of the matter."[24] To avoid concerns about improper influence, such guidance and expression of views should be given publicly, where possible, and always in writing. Further, in the case of extraordinary police powers, it may be necessary to restrain police independence to protect the values of our free and democratic society.

The RCMP is also generally accountable to the Minister. The Minister must be informed of RCMP conduct and be answerable to Parliament and the Canadian public for conduct that is inconsistent with the rule of law or with public policy. Without such answerability, we run the risk, particularly concerning activities that are not reviewed by the courts, of the police not being accountable to anyone.

2.2
SUMMARY

Given the complex balance between police independence and police accountability, I would be concerned about the effect a true oversight mechanism might have. A mechanism that itself had the power of direction over the RCMP could interfere with the doctrine of police independence. This would especially be so if directions were issued on operational matters and individual cases. The powers of direction inherent in oversight could also dilute or impair the independence of the review of RCMP activities. A body that pre-approved or directed activities would become tied to those activities. The body would be placed in the position of reviewing its own directions or approvals, and the independence of its assessment could be brought into question.

There is also a real risk that adding an oversight mechanism would work to diminish ministerial responsibility for RCMP activities and RCMP accountability to the Minister. As I have said, I agree with both the McDonald Commission and the Patten Commission that the police should be accountable to government and that government, through the Minister, should be responsible for police policies. This is particularly so for national security activities. An oversight mechanism that included the power to impose policy on the RCMP or to be involved with ongoing operations could water down ministerial responsibility by creating a temptation for the government to defer action to the oversight mechanism. The principle of police independence, and the sometimes politically controversial nature of issues affecting the police, can make governments reluctant to become involved. In my opinion, greater accountability to the Minister and greater ministerial responsibility for RCMP activities are highly desirable.

Therefore, I believe that the accountability mechanism that is contemplated by the mandate should be a review mechanism as described above.

3.
PRIMARY OBJECTIVES OF A REVIEW MECHANISM

3.1
ASSURANCE OF CONFORMITY WITH THE LAW AND STANDARDS OF PROPRIETY

The first objective of a review mechanism should be to review the RCMP's national security activities to ensure that those activities conform to law and to our society's fundamental values, and to report on deviations from these values. This is a necessary first step in ensuring RCMP accountability and engendering public trust and confidence.

As noted above, police independence does not mean that the police are free to carry out their activities in any manner they choose. A fundamental constraint on police power is the rule of law. As the McDonald Commission stated:

> [T]he rule of law must be observed in all security operations . . . . In our context this means that policemen and members of a security service, as well as the government officials and ministers who authorize their activities, are not above the law . . . . They must not take the law into their own hands. This is a requirement of a liberal society.[25]

The Supreme Court of Canada made the same point more recently in the *Suresh* case.[26] There, the Court emphasized that while powerful tools are needed to effectively meet the threat of terrorism, it would be too great a price if

terrorism were defeated at the cost of sacrificing our commitment to the values that are fundamental to our society — liberty, the rule of law and the principles of fundamental justice.

The legal standards against which RCMP activities should be reviewed include the *Canadian Charter of Rights and Freedoms*, which itself embodies Canada's fundamental values. Review should also include compliance with domestic statute law, such as the *RCMP Act*, the *Criminal Code*, the *Anti-terrorism Act*, human rights legislation and all other legislation applicable to the RCMP's national security activities. In addition, activities should be assessed against Canada's international obligations, and against the standards set out in ministerial directives and internal RCMP policies. While not strictly "laws," these standards are important norms that guide RCMP activities. As mentioned above, ministerial directives constitute general, but important, forms of policy direction by the Government: they provide guideposts in assessing the propriety of RCMP conduct. Internal RCMP policies constitute guideposts in assessing whether the RCMP is respecting its own internal rules and accountability mechanisms; these policies should also be subject to review to ensure they meet external standards.

To be effective, a review mechanism assessing conformity with law should look at more than adherence to the strict letter of the law. It should also assess the propriety of activities. This is especially important in the national security context, where police activities can have serious implications for human rights. By "propriety," I am referring mainly to whether RCMP actions were fair and proportionate. These concepts are inherent in Charter and human rights legislation, and should be emphasized in the context of a review mechanism.

In Canada, proportionality has been an objective of review for propriety as far back as the 1969 Mackenzie Commission. That commission concluded that review of certain RCMP national security decisions would "ensure that the rights of individuals had not been unnecessarily abrogated or restricted in the interests of the security of the state and its allies, and that no unnecessary distress had been caused to individuals."[27] In its first annual report, the Security Intelligence Review Committee (SIRC) noted that one of the purposes of its review was to ensure that CSIS activities "do not involve any unreasonable or unnecessary exercise" of its power.[28]

Three principles for assessing propriety on the basis of proportionality identified by Ian Leigh, a participant in the Policy Review Roundtable of International Experts on Review and Oversight, are as follows:

- Investigative methods should be proportionate to the threat being investigated, and evaluated against possible damage to civil liberties and democratic structures;

- The least intrusive method should be used wherever possible; and
- Discretion should be circumscribed so that the level of authorization is proportionate to the invasion of privacy.[29]

Similarly, fairness is another standard against which police conduct can be measured to assess propriety. The Mackenzie Commission first proposed adopting a review mechanism for some RCMP national security decisions to provide protection "against arbitrary, hasty or ill considered judgments."[30] SIRC, likewise, reviews CSIS activity to make sure that "while effectively protecting the nation's security against non-military threats, [CSIS] treats individual Canadians fairly, and . . . uses its intrusive powers with restraint and with an overriding sensitivity to democratic values."[31] Shirley Heafey, the former chair of the Commission for Public Complaints Against the RCMP (CPC) has identified similar functions for the CPC and national security matters:

- To ensure powers are used fairly in an environment where the activities of the RCMP will only rarely be reviewed by the courts;
- To ensure individuals are not targeted unfairly because of their racial background; and
- To ensure that all individuals "enjoy equal benefit, and protection of the law."[32]

I have cited these approaches to proportionality and fairness as examples. It is not possible, nor do I believe it would be wise, to set out an exhaustive definition. My point is that a robust review mechanism should assess conduct against not only constitutional, statute, common law or policy standards, but also against propriety in the sense of proportionality or fairness. Proportionality and fairness will also be an important guide in assessing the other standards against which RCMP activities will be reviewed, in particular the standards set out in internal RCMP policies and in ministerial directives. While the standards to be applied will generally be developed outside the review mechanism, review should include assessing those standards in the context of the impact of RCMP activities on the rights and freedoms of individuals.

Some participants in the Policy Review suggested that there should also be review for efficiency or effectiveness of RCMP activities. This is sometimes referred to as review for "efficacy." For example, at the Roundtable of Canadian Experts on Review and Oversight, Wesley Wark argued that while review for propriety is very important, it is also important that police forces and

intelligence agencies be reviewed and assessed for efficacy. By efficacy, Professor Wark was referring to competence and capacity. He stated:

> The issue in efficacy-based reviews is competence and capacity. It is essentially about knowledge. That is the thing that we require from security and intelligence communities. It is a thorough-going deep, available knowledge of threats to the security of Canada.
>
> It is very hard to know what the reality is. And in some ways it has to be hard to know what the reality is because there is a real need for secrecy in this field.
>
> But that need for secrecy has to be balanced against what I think of as a fundamental transformation in public attitudes and approaches to intelligence and security matters in this country, and worldwide, that have been stimulated by the events of September 11th and . . . the terrible intelligence failure of the Iraq war and the ways in which many publics feel that they were, as the common phrase goes, neo-conned into a war.
>
> We are in a new era, which I call an era of public intelligence, in which there will be simply a strong expectation that publics have a right and a need to know as much as possible about the activities and the competencies of the intelligence and security community that serves them.[33]

Professor Wark's argument should be considered. The need to be assured of efficacy is relevant to the intelligence community as a whole, and may be an appropriate subject for the proposed Parliamentary Committee on National Security.

I note that it was concern about the propriety of actions taken with respect to Maher Arar that gave rise to this Inquiry. I have not conducted the Inquiry with the goal of making recommendations about the efficacy of the RCMP's national security activities, and I am therefore not in a position to evaluate whether an independent review mechanism is needed from this perspective. However, review for propriety will inevitably raise issues of competence and capacity. This is evident from my Factual Inquiry report where, for example, the issue of training RCMP officers in the area of national security policing procedures was closely related to an assessment of their conduct for propriety. Also, analyzing proportionality may involve a balancing of impact upon individual rights against the utility or efficacy of a particular practice or procedure. In these circumstances, issues of efficacy and propriety are interwoven, and comments about competence or capacity related to propriety will be highly useful and desirable. Thus, while efficacy will not be the primary objective of the review mechanism I recommend, it will in many cases be a necessary element of a robust review for propriety.

3.2 FOSTER ACCOUNTABILITY TO GOVERNMENT

The second objective of a review mechanism is to enhance or foster the RCMP's accountability to those who are politically responsible for the Force, while enhancing and facilitating government responsibility or answerability for RCMP activities. As discussed above, notwithstanding the principle of police independence and the limits it places on Government interference with criminal investigations, the RCMP is accountable to the Government for, at a minimum, the legality and propriety of its activities; and the Government, through the Minister, is responsible to Parliament and to Canadians for the legality and propriety of RCMP activities.

The degree to which the Government can direct or control the RCMP's day-to-day activities is evolving and being debated. As is evident from some of my recommendations in the Factual Inquiry, I believe that greater ministerial direction is warranted for national security activities. In my view, beyond any controversy about the Minister's ability to give the RCMP direction, a fundamental element of the RCMP's status and role is that the Force be accountable to the Minister for unlawful or improper conduct, and that the Minister be responsible for ensuring that such conduct does not reoccur.

A review mechanism should foster such accountability and responsibility by reviewing RCMP activities as discussed under the first objective and reporting on the review. Reporting should include making recommendations for correction or improvement to the RCMP and to the Minister. Inherent in the review and reporting function is an obligation to follow up: a review mechanism should investigate what has been done to correct previously identified shortcomings and report on those as well.

Fostering accountability and responsibility requires a review mechanism that is independent of both the Government and the RCMP. The concerns underlying the principle of police independence — possible improper political interference in criminal investigations — are also present with respect to a review mechanism. If the mechanism is completely in the Government's hands, it could be used for an improper purpose. I am not saying the Government would intentionally do so, but, as discussed in more detail under the next objective, the possibility lessens public confidence in the process. A mechanism with significant independence from government should substantially reduce and even eliminate this concern. An independent mechanism can provide an independent and objective assessment of the legality and propriety of the RCMP's national security activities, on the basis of which the RCMP can be held accountable and the Minister can exercise appropriate direction over the RCMP.

3.3
FOSTER ACCOUNTABILITY TO THE PUBLIC AND FACILITATE PUBLIC TRUST AND CONFIDENCE

The third fundamental objective of a review mechanism is to foster RCMP accountability to the public. The important consequence of such accountability will be to engender public trust and confidence in the RCMP, which is essential if the Force is to carry out its role effectively. Public trust and confidence are to some extent a product of the first two objectives I have set out: assurance that the RCMP is operating lawfully and appropriately, and that it is answerable to those in government who are responsible for it.

As noted above, the RCMP has been granted significant powers to carry out its policing function, especially in the area of national security, and the exercise of many of these powers can be quite intrusive on individual rights and liberties. From evidence that I heard in the Factual Inquiry, and from the research conducted and submissions made in the Policy Review, it is clear to me that there is concern that such powers be used lawfully and appropriately. This concern arises largely from a lack of public information and public evaluation of the RCMP's national security activities. Without a means of being informed whether RCMP powers are being used appropriately, it is difficult for the public to develop any sense of confidence and trust in the RCMP's national security activities.

The RCMP itself clearly recognizes the importance of public trust and confidence. In his submissions to me during the Policy Review public hearings, Commissioner Zaccardelli stated:

> Participants in your inquiry have called for an assurance that the rights and freedoms of Canadians will always be respected. Nothing could be more important, not only in keeping with shared values and guarantees that are enshrined in law and in the Charter, but also to maintain one of the most precious resources available to society: trust.
>
> At the RCMP we are viscerally aware that without trust we cannot work with and for the Canadians and Canada we are mandated to serve. Without trust Canada is at risk, and no amount of review or oversight would be able to restore the confidence of a nation.
>
> In the end we all want and need the same thing: the comfort of knowing that if and when any machinery of public service should fail, that fault will be found, responsibility accepted, repairs and changes made.[34]

I agree with this assessment. A fundamental goal of a review mechanism is indeed to help provide the assurance that if something goes wrong, "fault will be found, responsibility accepted, repairs and changes made."

While it will always be necessary for certain aspects of the RCMP's national security work to take place behind closed doors, in my view, a fundamental objective of a review mechanism is to bring increased transparency to the RCMP's activities. This is accomplished in two ways. First, a review mechanism should bring to the public's attention information that can be disclosed without compromising national security or endangering lives. Second, where information must remain secret, a review mechanism must act as a kind of surrogate for the public to investigate and assess the RCMP's conduct, report any shortcomings to the appropriate body, and follow up to determine if appropriate action has been taken. Hans Born and Ian Leigh describe this aspect of review as providing a "check from the viewpoint of the citizen."[35]

As Commissioner Zaccardelli stated at the public hearing:

> [N]o more will citizens sit back and let institutions like law enforcement, the military or other government entities, operate unilaterally without transparency, accountability or consequence.
>
> The people of Canada are better informed and more challenging to even traditional[ly] sacrosanct training like ours than any generation before. Rather than decry or resist these developments, I believe we need to embrace and adopt the active involvement of individuals in governance and even some elements of operations. We need to respond [to] the new paradigm around accountability, knowing that doing so will only enhance our ability to achieve our goals.[36]

Commissioner Zaccardelli went on to endorse the concept of an independent review mechanism for the RCMP's national security activities.

The RCMP is not the only institution operating in circumstances that are not conducive to transparency. The public's understanding of CSIS' activities is subject to the same limitations. One of the most important functions that SIRC — the body that reviews CSIS — performs is to provide indirect, or surrogate, transparency. In its first annual report, SIRC described its mission in the following terms:

> For its part in the process, the Committee plans to ferret out with vigour information relevant to its duties and functions, and then, in deliberating and determining the national security requirements involved, to provide fairness to individual Canadians affected. The Committee is only one body in a complex maze of checks and balances established by Parliament in the [CSIS] Act. But through its report, the

> Committee is the single body which can give Parliament annually an independent insight into the workings of the maze. This the Committee intends to do to the best of its abilities, judgement, and experience.[37]

If the public accepts them as being independent, thorough and fair, such reports help to engender public confidence in the organization being reviewed. The general view of nearly all who made submissions to me is that SIRC has helped develop trust and confidence in CSIS in circumstances where the public does not have direct access to CSIS' operations. An RCMP review mechanism needs to serve a similar objective.

To carry out this objective effectively, the review mechanism must itself have the public's trust and confidence. In some instances, public disclosure will be limited to the review body attesting that it has thoroughly looked into an activity and is satisfied that the public's rights and freedoms have been adequately protected. Without trust and confidence in the review mechanism, such attestation will do little to promote trust and confidence in the RCMP.

Certain review features are essential if the review body is to engender public confidence in itself and in the RCMP's national security activities. First, the review mechanism must be independent of and at arm's length from both the Government and the RCMP. I have already discussed the importance of independent review in fostering accountability to the Government in the previous section of this chapter. There, I focused on independence from the potential for improper political interference in the RCMP's activities; in the present context, I refer to independence in the judicial or quasi-judicial sense of having an unbiased, neutral assessor. To gain public confidence and trust, it is essential that those responsible for review are, and are seen to be, free from interference by government, the RCMP or any other group with a particular interest in the subject matter. As the Morand Commission noted, "Justice does not appear to be done when the entire procedure is in the hands of the body against which the complaint is made."[38] Public confidence and trust will not be fostered if the review mechanism is itself seen as biased. In this regard, I endorse the description of the role of the CPC found on its website: "The CPC carries out its duties impartially . . . [It makes] unbiased findings and recommendations . . . aimed at identifying, correcting and preventing recurring problems in policing."[39]

A second feature of review needed to engender public confidence is to have the review performed by competent individuals. The public must be satisfied that those carrying out review are qualified to do so. Given the secretive nature of the activities being reviewed, I believe it is necessary to go beyond competence and ensure the involvement of those who, through their

background and experience, inspire confidence. As I understand it, this is what lies behind the requirement that those appointed to SIRC be Privy Councillors. While I am not saying that it is necessary to restrict a review body to Privy Councillors, I believe that individuals appointed to a review body must have a stature that engenders public confidence.

A third feature necessary to achieving the objective of public confidence and trust is that the review process must itself be as transparent as possible. Transparency includes an open and fair process for appointing individuals to the review body, public education about the role and activities of the review process, and as much disclosure as possible of the review body's activities and findings. The last two elements of transparency deserve particular emphasis.

Of course, public confidence will not be developed through a review mechanism if the public is unaware of the review mechanism's functions and activities. Therefore, it is important that the body take on a role of creating public awareness of its function. As I discuss in more detail below, this is especially true for the complaints aspect of a review mechanism. While the body should not "troll" for complaints — as this could have a negative effect on the appearance of independence — the body or the Government should make the public aware of the complaints process and how it works.

A review mechanism must also make its activities and findings available to the public to the extent possible. While I acknowledge the importance of secrecy in the national security field, my own experience in the Factual Inquiry clearly shows that much can be made public without endangering Canada's national security or putting individuals at risk. It is clear to me that accountability and public confidence are best engendered through transparency and the release of information to the public. It is important for a review mechanism to play a role in ensuring the public receives as much information as possible about the RCMP's national security activities and the process of review. I am not suggesting a cavalier approach to public disclosure. However, the review mechanism should challenge the inclination to keep everything related to national security from the public and should advocate for releasing all information where no harm would result.

3.4
NOT TO IMPAIR NATIONAL SECURITY

As set out in the introduction to this chapter, these three fundamental objectives are subject to an important institutional or functional imperative: a review mechanism should not function so as to itself impair national security, nor should it impair the lawful and appropriate conduct of the RCMP and operation of the

criminal justice system. In other words, the review mechanism needs to operate effectively in the context of the RCMP's national security activities and Canada's national security landscape.

Some of the submissions I received approached the concept of a review mechanism as a form of sanction for bad behavior. I disagree with that notion entirely. I do not approach review as a sanction. In my view, a properly structured review mechanism can benefit the public as I describe above and can also significantly benefit the organization being reviewed. Effective review can increase public confidence and trust in the organization. It can also provide assurance to the organization that its activities are being conducted lawfully and appropriately, as well as guidance when they are not. I heard evidence in the Factual Inquiry and received submissions in the Policy Review from those with experience in organizations that are subject to review that a review mechanism is of real and substantial benefit to the organization.

Several features of the RCMP's national security activities should be kept in mind in order to design a review mechanism that will not have an unintended negative impact upon the RCMP, the legitimate objectives of its national security activities, or the criminal justice system as a whole. These features are referred to throughout this report. However, I describe them briefly here as they provide important context for my conclusions about the need for an independent review mechanism for the RCMP and my recommendations about that mechanism.

3.4.1 Police Independence

I dealt with police independence in some detail earlier in this chapter. Police independence does not have the same implications for the work of an independent review mechanism as it does for the Minister and others in government who could be perceived to have powers of control or direction over police operational activities. Unlike the Minister, an independent review mechanism would not have a statutory power to direct the Commissioner of the RCMP, but only a mandate to make findings and recommendations about RCMP activities. Moreover, a review body would normally examine the RCMP's law enforcement decisions only after they occurred; this significantly lessens concern that review will negatively affect police independence. Even so, the nature of national security policing discussed in Chapter V suggests that national security files may be kept open for extended periods, and that a review body may sometimes have a legitimate interest in examining or commenting on RCMP law enforcement decisions in relation to ongoing investigations. In doing so, a

review mechanism, like a Minister, should respect the doctrine of police independence that allows police to continue to make law enforcement decisions independently.

3.4.2 Operation of the Criminal Justice System

The RCMP's national security activities are either criminal investigations or linked to criminal investigations and, as such, relate directly to the operation of the criminal justice system, including criminal prosecutions. Review mechanisms have the potential to disrupt criminal investigations and prosecutions in several ways. For example, to the extent that a review mechanism has powers of inquiry like those of a public inquiry, issues will arise about fairness to individuals involved in any subsequent criminal or regulatory prosecutions. These include issues relating to the right to remain silent and the right to disclosure of relevant information (section 7 of the Charter), and the right to a fair trial (paragraph 11*(d)* of the Charter).

In addition, because the review process will involve examining the activities carried out in connection with a criminal investigation, the review mechanism could itself become subject to disclosure obligations. As the Supreme Court of Canada affirmed in *R. v. Stinchcombe,* the Crown has broad disclosure obligations to the defence in a criminal prosecution. Such obligations could extend to material in the hands of a review mechanism,[40] including the product of the review mechanism's own investigations such as notes of interviews or witness statements, documents from other sources that the RCMP or the Crown did not have, and the review mechanism's own analyses. Moreover, in the national security context, requests for disclosure could include secret documents — from both the RCMP and other sources — as well as documents created by the review body itself. I note that in the context of the Air India prosecution, SIRC was compelled to release an edited version of its review of CSIS in relation to the matter.

Leaving aside issues related to secrecy — which I discuss below — potential disclosure obligations on the part of the review mechanism may have an impact on the criminal justice process. I must say that it is not clear to me that all such impacts would be negative. However, negative impacts are possible. At the Canadian Experts Roundtable, Commissioner Dirk Ryneveld — the Commissioner of the British Columbia Police Complaints Commission — explained that in a high-profile B.C. prosecution, he deferred investigating a complaint about police conduct related to the case until after completion of the

prosecution. This practice could present difficulties in lengthy criminal investigations — which are common in national security cases.

Other negative effects on the criminal justice system are possible. For example, in a review of ongoing criminal investigations, a reviewer could be placed in the chain of evidence. In other words, if a reviewer examines physical evidence relevant to the criminal proceeding, the examination may have to be explained when the evidence is sought to be introduced in court. I am not raising these factors as impediments to robust review, but to note that review may have an impact on the criminal justice system, and that minimizing unnecessary and undesirable effects should be kept in mind in designing a review mechanism.

The work of a review body can be reconciled with the operation of the criminal justice system in various ways. As Commissioner Ryneveld suggested, the review body should have the discretion to suspend its investigation in the public interest, including to prevent prejudice to an ongoing criminal investigation or prosecution. It may make sense for the review body to exercise this discretion to suspend its investigations especially if a prosecution is imminent. In such cases, the public interest in not unduly complicating the prosecution may be high, and the state's conduct may also be subject to judicial review as part of the prosecution. However, in cases where there is a lengthy criminal investigation that may never result in a prosecution, I expect there will be greater public interest in having effective review, even if the review process may result in information that could be relevant should there be a subsequent criminal prosecution.

One way to help a review body manage information that may be relevant in a subsequent trial is by giving it the discretion to disclose to the Attorney General of Canada information it collects in its review functions. Although disclosing such information to the Attorney General of Canada would not make the review body immune from requests by the accused in a criminal trial for the production of relevant information, it would diminish the importance of such requests by placing with the Attorney General of Canada copies of potentially relevant material that should be disclosed to the accused. Under the *Security Offences Act*,[41] the Attorney General of Canada can pre-empt any national security prosecutions that provincial or territorial attorneys general may conduct.

After receiving material from the review body, the Attorney General would be in a better position than the review body to determine whether the material was relevant in an ongoing criminal prosecution and subject to *Stinchcombe* disclosure obligations. The Attorney General of Canada would also be in a better position than the review body to invoke any relevant claims of privilege or

claims to national security confidentiality. The Attorney General of Canada would have both the duty to disclose under *Stinchcombe* and the ability under sections 37 and 38 of the *Canada Evidence Act* to claim privilege over relevant material that might otherwise be disclosed under *Stinchcombe*. In *R. v. Chaplin*,[42] the Supreme Court recognized that the Attorney General may have access to special procedures under the *Canada Evidence Act* to claim privilege and protect the confidentiality of material.

3.4.3
The Importance of Secrecy and the Protection of Sensitive Information

Earlier in this chapter, I discussed the importance of secrecy and the protection of sensitive information in the national security context. Disclosure of secret or sensitive information such as investigative techniques and the identity of sources could work to harm Canada's national security. In cases such as source identity, lives may be put at risk. Also, disclosing information that foreign agencies had provided on the understanding that it not be disclosed could harm relationships with those agencies and stifle international co-operation. These potential consequences must be kept in mind in designing a review mechanism.

In my view, a review mechanism requires access to all relevant information necessary to carry out its function effectively. Therefore, with limited and isolated exceptions, the review mechanism should not be barred from information because that information is secret or sensitive. In turn, the review mechanism must itself be subject to obligations not to disclose. As discussed in Chapter VI, this approach to review has worked well with CSIS and SIRC, as well as with the Communications Security Establishment (CSE) and the CSE Commissioner.

3.4.4
Excessive Review

Some who made submissions to me asked that I be conscious of what they referred to as the "burden of review." By this they meant that review involves burdens and costs, as well as benefits. In addition to financial implications, review may redirect organizational resources away from the mandate of the agency to the review process, and the attention of personnel away from their work to the process.

I agree that it is important to keep the burden of review in mind. A review should not be so onerous that it hinders the RCMP from carrying out its important functions. I am particularly conscious of duplicative mechanisms for review: in designing a review mechanism for the RCMP's national security activities, it is necessary to be mindful of other mechanisms that perform the same function.

3.4.5
Ability to Deal with the Integrated Nature of National Security Activities

In chapters IV and V, I describe in some detail the highly integrated nature of the RCMP's national security activities. Integration is an extremely important element of the Government's approach to protecting Canada's national security. The nature of integration ranges from units such as INSETs (Integrated National Security Enforcement Teams) — where personnel from many agencies work together on national security criminal investigations — to relationships that are less structured and exist, for example, primarily for information sharing. Integration raises two issues that are critical to effective review:

- To what extent should review encompass the activities of non-RCMP personnel who are working under RCMP control and direction?
- To what extent does the work of a review mechanism need to extend beyond the RCMP?

Regarding the first issue, I believe it is critical that a review mechanism be able to assess all national security activities under the RCMP's control and direction. Excluding any such activities on the grounds that they are carried out by personnel who are not formally or permanently members of the RCMP would mean that the review is incomplete. INSETs, for example, are clearly under RCMP control and direction. All members — whatever their home organization — work together on the same investigations. It would be impossible to comprehensively assess an INSET investigation without assessing the conduct of all those involved in it.

In some circumstances, the activities of a participant from an outside agency may not fall under RCMP control and direction. I understand, for example, that even in INSETs, CSIS personnel have a different role than police personnel: they do not participate directly in INSET criminal investigations, but are present to monitor such investigations and facilitate information exchanges. In such circumstances, however, an RCMP review mechanism must be able to review the conduct of CSIS personnel as it relates to the INSET activities. For example, it will be necessary in information exchanges to review whether it was appropriate for the RCMP to receive the information as they did or to provide information to CSIS. By contrast, it is not critical for an RCMP review mechanism to assess the conduct of the CSIS representatives as it relates to CSIS' mandate. As I discuss in more detail below, this is better left to SIRC.

The same is true of other personnel who interact with the RCMP in either formally integrated units or less-structured relationships. The activities of such

individuals that are directly related to RCMP criminal investigations and that are, or should be, under RCMP control and direction must be subject to review by an RCMP review mechanism.

Because some INSET personnel are from provincial agencies, the issue of constitutional jurisdiction arises. In my opinion, there is no constitutional impediment to a federal review mechanism assessing activities that are under RCMP control and direction. The federal government clearly has constitutional jurisdiction over national security policing. In addition, the RCMP is a federal police agency and its activities fall within federal jurisdiction. INSET activities are under RCMP control and direction, and this control and direction extends to those personnel from other agencies, including provincial agencies. In these and similar circumstances I see no constitutional impediment to review of those activities by a federal mechanism.

The question of constitutional jurisdiction becomes more complex if a federal mechanism has the power to compel a provincial actor to take action or the power to discipline an individual whose home agency is provincial. However, given my conclusions about the objectives of a review mechanism, it is not necessary for me to deal with that issue. As I said above, an effective review mechanism should have a mandate of making findings and recommendations, not of imposing discipline, compelling remedial action or engaging in oversight.

The second integration issue that is important to the objectives of a review mechanism is the extent to which a review mechanism should go beyond the personnel and material that are under RCMP control and direction to effectively carry out its mandate. Although a review mechanism should focus on assessing RCMP national security activities, in my view, it will need to go beyond the strict confines of the RCMP to achieve this objective.

Given the role of integration and co-operation among agencies in national security activities, it does not seem to me possible to assess RCMP activities without understanding the circumstances in which these activities occur. For example, if the RCMP takes action based on information it has received from another agency, it may be necessary to determine the circumstances in which that information was provided in order to assess the propriety of the RCMP's conduct. The RCMP review mechanism will need the power to have access to all information and individuals necessary to review the RCMP's activities, even if that information or those individuals are from other agencies, whether federal or provincial. I am not suggesting that the RCMP mechanism should assess the other agencies' conduct — only that it must have the power to access information and personnel from those agencies.

The need to go beyond the RCMP is important in another way. Because of the integrated and co-operative approach that the Canadian government has taken to address threats to national security, review of only one agency, such as the RCMP, will sometimes not be enough. To assess the merits of some complaints, the activities of multiple national security actors will have to be reviewed. My own experience from the Factual Inquiry illustrates this point: to assess Mr. Arar's case, I had to investigate the activities of several national security actors. The point was also made in many of the submissions I received. Riad Saloojee, who appeared at the public hearings on behalf of the Canadian Arab Federation and the Canadian Council on American-Islamic Relations, underscored the point by pointing out that some who felt that their rights might have been affected by government action did not know which agency to complain about.

In these circumstances of integrated national security activities, it is critical that there be an ability to integrate review. In other words, it is important to have available a mechanism that can accomplish review of multiple agencies when the activity being reviewed involves multiple agencies. I provide recommendations to ensure integrated review in Chapter XI. For the purposes of this chapter, it is important to note that to achieve the objective of operating effectively in the national security context, an RCMP review mechanism must be able to integrate with review mechanisms for other national security actors.

Notes

1 See Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, online, www.ararcommission.ca/eng/index.htm (accessed June 16, 2006) [Arar Commission].

2 See chapters VI and VII.

3 *R. v. Metropolitan Police ex parte Blackburn*, [1968] Q.B. 116 at 135–136. See also *R. v. Chief Constable of Sussex ex parte International Trader's Ferry Ltd.* [1999] 1 All E.R. 129.

4 [1999] 1 S.C.R. 565.

5 *Fisher v. Oldham Corporation*, [1930] 2 K.B. 364; *Attorney General for New South Wales v. Perpetual Trustee Company*, [1955] A.C. 457. In the Canadian context, see *McCleave v. City of Moncton* (1902), 32 S.C.R. 106 at 108–109. For an examination of other early Canadian civil liability jurisprudence, see Stenning, *Legal Status of the Police* (Ottawa: Law Reform Commission of Canada, 1981), pp. 102–112. Professor Stenning concludes that "none of these cases, however, determines the implications of the constitutional status of the police in terms of their liability to receive direction of any kind with respect to the performance of their duties." Ibid., p. 110. See also G. Marshall, *Police and Government* (London: Methuen, 1965).

6 *Supra* note 4 at para. 27.

7 Ibid. at paras. 28–29.

8 Ibid. at para. 29.

9 Ibid. at para. 18.

10 *Quebec Secession Reference,* [1998] 2 S.C.R. 217 at 249.

11 See Chapter VIII.

12 See Chapter III.

13 "RCMP Response to the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar," (written submission to the Arar Commission Policy Review Public Submissions) February 21, 2005, p. 28 [RCMP submission].

14 R.S.C.1985, c. R-10, s. 5 [*RCMP Act*].

15 *Supra* note 4 at para. 33.

16 Canada, Commission for Public Complaints Against the RCMP, *RCMP Act — Part VII, Subsection 45.45(14), Commission Interim Report Following a Public Hearing Into the complaints regarding the events that took place in connection with demonstrations during the Asia Pacific Economic Cooperation Conference in Vancouver, B.C. in November 1997 at the UBC Campus and at the UBC and Richmond detachments of the RCMP* (Ottawa: The Commission for Public Complaints Against the RCMP, 2001), para. 10.2 (Commissioner: Ted Hughes, QC).

17 "Directives" are sometimes referred to by the Minister as "directions."

18 See Chapter IV.

19 Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Freedom and Security under the Law*, Second Report, vol. 2 (Ottawa: Supply and Services Canada, 1981), p. 1013, para. 19 (Chair: D.C. McDonald) [McDonald Commission report, vol. 2].

20 Ibid.

21 Ibid., p. 869, para. 60.

22 The Independent Commission on Policing for Northern Ireland, *A New Beginning: Policing in Northern Ireland* (Belfast, U.K.: September 1999), para. 6.20, online, www.belfast.org.uk/report.htm.pdf (accessed June 16, 2006).

23 Ibid., para. 6.21.

24 McDonald Commission report, vol. 2, p. 1013, para. 19.

25 Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Freedom and Security under the Law*, Second Report, vol. 1 (Ottawa: Supply and Services Canada, 1981), p. 45 (Chair: D.C. McDonald) [McDonald Commission, report, vol. 1].

26 For the relevant portion of the *Suresh* decision, see Chapter VIII.

27 Canada, Mackenzie Commission, *Report of the Royal Commission on Security* (Abridged) (Ottawa: The Queen's Printer, 1969), p. 41, para. 114 (Chair: M.W. Mackenzie) [Mackenzie Commission report].

28 Canada, *SIRC Annual Report, 1984–1985* (Ottawa: Minister of Supply and Services Canada, 1985), p. 4.

29 Ian Leigh, *National Legal Dimension of the Democratic Control of the Security Sector: Values and Standards in Developed Democracies* (Geneva: Centre for the Democratic Control of Armed Forces, 2002), DCAF Working Paper No. 80, p. 13. Professor Leigh cites the McDonald Commission for the principles.

30 Mackenzie Commission report, p. 41, para. 110.

31 *SIRC Annual Report, 1984–1985*, p. 22.

32 Shirley Heafey, "Civilian Oversight in a Changed World," in David Daubney et al., eds., *Terrorism, Law and Democracy: How is Canada Changing Following September 11?* (Montreal: Les éditions thèmis 2002) 395 at 398.

33 Wesley Wark, Transcript, Roundtable of Canadian Experts on Review and Oversight (Arar Commission Policy Review), June 10, 2005, pp. 76–77.

34 Giuliano Zaccardelli, Royal Canadian Mounted Police, Transcript of Policy Review Public Hearing, Arar Commission (November 18, 2005), pp. 721–722.

35 Hans Born and Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* (Oslo: Publishing House of the Parliament of Norway, 2005), p. 23.

36 Zaccardelli, pp. 719–720.

37 *SIRC Annual Report,1984–1985*, p. 25.

38 Ontario, Royal Commission into Metropolitan Toronto Police Practices, *Report of the Royal Commission into Metropolitan Toronto Police Practices* (Toronto: The Commission, 1976) (Commissioner: D.R. Morand).

39 Commission for Public Complaints Against the RCMP, "Welcome!", online, www.cpc cpp.gc.ca/DefaultSite/Home/index_e.aspx? ArticleID=1 (accessed April 10, 2006).

40 For a discussion of such disclosure obligation, see *R. v. Stinchcombe*, [1991] 3 S.C.R. 326. In a criminal prosecution, the Crown has a legal duty to disclose all relevant information to the defence, whether or not the Crown intends to use the information at trial and regardless of whether the information is inculpatory or exculpatory. Information in the Crown's possession is not the property of the Crown for use in securing a conviction, but the property of the public to be used to ensure that justice is done. The Crown may withhold information from the defence only if the information is irrelevant or covered by a form of legal privilege, such as solicitor-client privilege or police informer privilege. The trial judge may review any decision by the Crown to withhold information. In principle, information should not be withheld if there is a reasonable possibility that withholding it will impair the right of the accused to make full answer and defence.

41 R.S.C. 1985, c. S-7.

42 [1995] 1 S.C.R. 727 at 741.

X
Is the Status Quo Adequate?

1.
INTRODUCTION

To this point, I have set out the background information that I think is necessary to address the question raised by the Inquiry mandate. I have outlined the nature and characteristics of the RCMP's national security activities, the Canadian national security landscape, the Canadian and international experiences with review of national security activities, and the fundamental objectives of review. The first question that arises is whether the status quo is adequate in light of this information. The answer to this question was never a foregone conclusion; maintaining the status quo was one of the options included in the Policy Review Consultation Paper issued in October 2004.

It would be wrong to equate maintaining the status quo with no review and no accountability. In this chapter I will examine the existing review mechanisms that can be applied to the RCMP's national security activities. These mechanisms include both internal and external controls. Internally, individual RCMP officers are subject to directions from senior officers and internal discipline under the RCMP Code of Conduct and disciplinary hearings. There are also several ministerial controls. These include specific requirements for the Attorney General's consent for many national security prosecutions and powers, and the use of ministerial directives by the Minister of Public Safety to provide policy guidance for RCMP national security activities.

The RCMP's national security activities are also subject to various external controls and review mechanisms. Among these are judicial oversight resulting from the prosecution process and judicial requirements for authorizing certain police powers. Courts in Canada have stressed quite properly the importance of the independent judiciary in maintaining the rule of law and respect for rights

and freedoms, even in the face of serious threats to national security.[1] In addition to judicial review, the Commission for Public Complaints Against the RCMP (CPC) reviews how the RCMP handles public complaints about the conduct of individual officers and can initiate its own public interest hearings. Finally, like other federal agencies, the RCMP is subject to review by several other accountability bodies, including the Auditor General, the Canadian Human Rights Commission (CHRC) and the Privacy Commissioner.

Although the functions of all these existing review and accountability bodies and processes are important, I conclude that they are inadequate for effective review of RCMP national security activities. In reaching this conclusion, I have been guided by a number of factors.

A primary factor is the changing nature of the RCMP's national security activities. As I discussed in Chapter III, the RCMP was given many new legal powers and responsibilities under the *Anti-terrorism Act* enacted at the end of 2001. Although the RCMP must exercise these new powers and responsibilities in a manner consistent with its law enforcement mandate, both the secret nature of national security policing and its reliance on information sharing with a wide range of domestic and foreign agencies bear similarities to CSIS' mandate as Canada's civilian security intelligence agency. However, review of CSIS' national security activities differs greatly from review of the RCMP's national security activities. As discussed in Chapter VI, to ensure the legality and propriety of its day-to-day conduct, CSIS is reviewed by both the Inspector General and the Security Intelligence Review Committee (SIRC). In contrast, the RCMP's national security activities are generally reviewed only if there are complaints about individual officers, even though many national security activities will remain secret and improprieties may result from systemic factors.

The changes in the RCMP's organizational structure for national security policing since 2001, which I examined in Chapter IV, have been as significant as the Force's increased powers. Increased integration of RCMP national security policing with the activities of CSIS, the Canada Border Services Agency, immigration authorities, and municipal and provincial police forces, and increased information sharing within and between governments are an important feature of Canada's approach to national security, but present new and difficult challenges for review bodies. Review bodies should have powers and resources that are adequate and commensurate to the powers and resources devoted to pursuing the vital and pressing goal of national security. In its 2004 national security policy, the Government of Canada recognized that to ensure compliance with the rule of law, review should keep pace with the evolving nature of national security activities.[2] The Auditor General, the Commission for Public

Complaints, the Security Intelligence Review Committee and the Privacy Commissioner have all independently raised concerns in recent reports about the adequacy of their powers or resources in the new security environment.[3] A crucial challenge for Canada and other democracies will be to ensure that review and accountability structures develop in step with the increased integration and intensity of the State's security activities.

A second factor I considered is the domestic experience with review bodies as examined in Chapter VI. Both SIRC and the Communications Security Establishment (CSE) Commissioner have broad, self-initiated review powers, while the CPC has no similar powers over the RCMP. SIRC was created as a review body with broad powers at the same time that CSIS was created as a civilian security intelligence agency as recommended by the McDonald Commission. However, the McDonald Commission also recommended that an independent body have some review powers over the RCMP.[4] This recommendation was not implemented when the CPC was created in 1988, and the need for review powers has only increased in importance since that time.

Self-initiated review powers are critically important with respect to national security policing because of the distinct qualities of such policing. As I describe in the preceding chapter, national security investigations differ from other police investigations because of the secret nature of much national security policing; the difficulty of monitoring information sharing and intelligence analysis; the infrequency of prosecutions with consequent judicial review of police activity; and the potentially adverse effects of national security investigations, including those on privacy and equality.

A further influence on my conclusion that the status quo is not adequate was the international experience with review of security intelligence agencies and national security policing discussed in Chapter VII. All democracies are struggling with the challenges to review and accountability presented by increased integration, increased information sharing and increased powers in the national security field. Several, including the United Kingdom and the United States, have taken steps to more effectively review national security activities, including those carried out by the police. Experts and policy-makers from around the world have expressed considerable interest in the Inquiry's conduct and conclusions. Going forward and building on this experience, I believe that Canada can and should aspire to become a leader in effective review of the state's national security activities.

Finally, I have been guided by the objectives of and constraints on effective review as examined in the preceding chapter. A primary objective of review is to maintain public confidence in the agency subject to review. The need to

maintain such confidence is particularly important with respect to national security activities, which by their nature often must remain secret.

In this vein, I am influenced by the fact that none of the groups that made public submissions on this issue defended the status quo as adequate. Indeed, the RCMP Commissioner, on behalf of the RCMP, acknowledged that strengthening the present system as it applies to national security investigations would promote public confidence.[5] The CPC, the body currently responsible for monitoring public complaints against the RCMP, including those arising from its national security activities, strongly argued that it does not have the powers it needs to review those activities effectively.[6]

Another important objective of a review process is to ensure that the agency being reviewed respects the law and human rights. It is significant that the existing review process — especially the CPC — is complaint-driven, and that many of the RCMP's national security activities are secret and thus will not likely become the subject of complaints. Furthermore, existing discipline and complaint mechanisms are designed to deal with allegations of misconduct against individual RCMP officers. They are not well suited to examining whether the RCMP's organizational practices and culture are designed to ensure proper conduct, including compliance with existing laws and ministerial directives. They also do not recognize that people may be harmed by conduct that stems, not from intentional or individual misconduct, but from inadequate systemic and organizational controls.

In reaching the conclusion that the status quo is inadequate, I have been conscious of the need that increased review not harm the RCMP's legitimate national security activities, including the need to work with other agencies in an integrated fashion and to share information. I have been careful to consider the unique aspects of policing, as distinct from security intelligence, including the issue of police independence discussed in Chapter IX.

Increased review powers and new review structures should not be seen as mechanisms that will simply restrain or hamper state security activities. Proper review can help ensure that the agency being reviewed respects its mandate and uses efficient, effective and fair procedures. I was impressed by the testimony of Mr. Jack Hooper, CSIS' Assistant Director of Operations, who stated that despite "tremendous resistance to having external review" when CSIS was first created, his view now is that "[e]xternal review has made [CSIS] better" and that SIRC's external audits of CSIS' activities perform "an invaluable function."[7] Commissioner Zaccardelli also spoke eloquently during the Policy Review public hearings of the RCMP's need for trust and public confidence, and how effective and independent review can contribute to that process.[8] It is my hope

that the recommendations proposed in this report, if implemented, will make the RCMP better and increase public confidence in the Force.

2.
WHY THE RCMP'S INTERNAL CONTROLS ARE NOT ADEQUATE

As would be expected given its large size and enviable reputation, the RCMP has devoted considerable effort to internal controls and accountability structures. These are described in some detail in Chapter IV.

Even the best internal review and discipline mechanism may not inspire public confidence and trust as an independent process would, however. In the national security context, in which much police activity must remain secret for legitimate reasons, the issue of public confidence and trust is especially important. In a free and democratic society, even legitimate claims of secrecy can raise understandable concerns and suspicions. In the national security environment, the public must have confidence that independent and respected people will see what the public cannot see and ask the difficult and informed questions the public cannot ask.

Another reason internal processes are inadequate is that they are often tied to complaints from the public or from other RCMP members about the conduct of individual members of the Force. Although public complaints should be taken seriously, and no one within the RCMP should turn a blind eye to their colleagues' misconduct, an effective review mechanism will have to be concerned with systemic failures and deficiencies as much as with the failures of individuals within the organization. Effective review should seek to reform and discipline systems, even where it would not be possible or fair to discipline individuals. Moreover, the secrecy of many of the RCMP's national security activities limits a complaint-based approach. Even within the RCMP, knowledge about national security activities will be restricted by the need-to-know principle.

In concluding that the internal controls within the RCMP are not adequate, I do not want to be interpreted as criticizing or diminishing the importance of these controls. Indeed, I believe that independent review will be more effective to the extent that it is integrated with and supported by effective internal controls. In this respect, I agree with Mr. Arar's counsel when they state in their submission to the Policy Review that:

> Internal audit mechanisms are essential in making timely identification of investigative errors, which can promptly foreclose the escalation of undesirable and harmful violations of human rights that might otherwise occur if not immediately

> addressed. Since an external review mechanism may not operate to prevent harm until 'after the fact', an internal audit mechanism is an important first line of defence. The integral functions of internal audit will be made more effective if the external review mechanism works in concert with it by establishing clear criteria for internal audit processes and reviewing compliance . . . . [A]ny effective external review body must build on and supervise the internal audit procedures that have and will be put in place within the context of national security investigations.[9]

While internal controls are vital and must complement external review, by definition they lack the quality of independence that will inspire public confidence in the often secret national security field. Furthermore, many internal controls focus on allegations of individual misconduct and not on systemic matters that may be fundamentally important when assessing the propriety of the RCMP's national security activities.

3. WHY MINISTERIAL CONTROLS ARE NOT ADEQUATE

Section 5 of the *RCMP Act* provides that the RCMP Commissioner is under the direction of the Minister of Public Safety. As discussed in the preceding chapter and in Chapter IV, however, the Minister's powers to direct the RCMP are constrained by the doctrine of police independence. This constraint would prohibit the Minister from directing individual RCMP decisions to start investigations, make arrests, conduct searches and carry out other law enforcement activities.

Ministerial directives issued in November 2003 direct the Commissioner to inform the Minister of "high profile" national security investigations and cases.[10] While it is appropriate for the Minister to have this information and to issue public policy directions and guidelines to the RCMP, many national security cases will never become high-profile. Moreover, with the responsibilities of a large department, the Minister does not have time to review all those that do become high-profile. Even if the Minister could somehow review all these files, he or she may, for understandable and legitimate reasons related to police independence, be reluctant to intervene in law enforcement decisions in individual cases.

Ministerial directives issued in 2002 and 2003 provide a valuable framework for information sharing and other agreements between the RCMP and other agencies. A 2003 directive requires ministerial approval of information-sharing agreements with foreign intelligence agencies.[11] However, this directive does not contemplate ministerial monitoring of information sharing or compliance with such agreements. These matters would be of legitimate concern to an in-

dependent review body, but are unlikely to command attention from the responsible minister.

There are other limits to the Minister's ability to monitor the RCMP's national security activities. Unlike CSIS, the RCMP does not have an inspector general to act as the Minister's eyes and ears, and it would be inappropriate to expect either the Minister's senior civil service or the Minister's political staff to play such a role. For reasons related to police independence and expertise, parliamentary committees also may be more reluctant to monitor the RCMP's national security activities than those of other agencies and departments.[12]

Even when combined with the RCMP's internal controls, ministerial controls may not be adequate to inspire public confidence. Although ministers can and should act with independence and integrity, they are also responsible to Parliament and the public for national security. There may be a tendency — or a perceived tendency — for a minister to err on the side of caution and secrecy with respect to national security matters, where one failure may have devastating results. A minister might be seen to be too closely identified with the Government's response to terrorism or other threats to national security. The Ontario Provincial Police pointed out in their submission that "it is inevitable that there would be less public confidence in a system of enhanced ministerial oversight than in other forms of oversight."[13] In such an environment, there is a need for independent review beyond what even the most dedicated and conscientious of ministers can perform.

In concluding that ministerial controls are not adequate, I do not want to be interpreted as criticizing or diminishing the importance of such controls. I believe that the Minister should be encouraged to provide policy guidance to the RCMP in writing. In my view, the 2002 and 2003 ministerial directives are helpful in giving the RCMP transparent and sensible guidance on its national security activities. As the RCMP noted in its submission, ministerial directives establish a policy framework for the RCMP, "provide the RCMP with standards in selected areas of policing activity for achieving a balance between individual rights and effective policing practices," and "inform the public about the character of supervision provided by the political executive to the RCMP."[14]

I also believe that the independent review of RCMP national security activities that I recommend in the following chapter will be more effective to the extent that the Minister pays close attention to the review body's reports and implements its recommendations, where appropriate. The Minister should also have the power to ask the review body to examine certain matters, where appropriate — I note that SIRC has often been tasked by the Minister to examine

various matters. Ministerial responsibility and control is a fundamental and valuable feature of Canada's parliamentary democracy.

A consideration of ministerial controls on the RCMP's national security activities would not be complete without examining the important role of attorneys general. As discussed in Chapter III, the attorney general of the province or of Canada must agree to start proceedings in relation to a broad range of terrorism offences under the *Criminal Code*, and the Attorney General of Canada must agree to start proceedings for offences under the *Security of Information Act*. An attorney general's consent is also required before the police can use the powers of investigative hearing and preventive arrests in terrorism investigations. As mentioned earlier, the RCMP stated in its submissions that "the consent requirement means that to some extent the federal and provincial prosecutors often provide a sober second thought on operational decisions."[15] Attorneys general should approach consent requirements in a quasi-judicial manner consistent with their unique constitutional responsibilities within government to ensure that justice is done and that rights and freedoms are respected. However, it is significant that the *Anti-terrorism Act* does not rely only on prior consent by the Attorney General, but also provides for various judicial controls.

In addition, the Attorney General's consent is not required for certain police powers in the national security field, including powers of electronic surveillance, the performance of acts that would otherwise be illegal,[16] the opening of investigations or the exchange of information — all matters that may have serious consequences for the individual concerned.

Without in any way diminishing the importance of ministerial controls in the national security field, I cannot conclude that ministerial controls alone or combined with the RCMP's internal controls will provide adequate review of the RCMP's national security activities to inspire public confidence or respect for rights and freedoms.

4.
WHY JUDICIAL CONTROLS ARE NOT ADEQUATE

The RCMP's national security activities are subject to a number of judicial controls. Prior judicial authorization is required for electronic surveillance, and judges play a key role in supervising the extraordinary powers of preventive arrests and investigative hearings. Indeed, the Supreme Court has recently affirmed the important role that judges will play in the conduct of investigative hearings, including the open court presumption.[17] In addition, national security prosecutions will allow an accused to challenge police conduct in obtaining evidence, on the basis that the evidence has been obtained in a way that violates the

Charter and that its admission would bring the administration of justice into disrepute.

Judicial controls are of great value in maintaining Canada's commitment to the rule of law, and the independence of the judiciary is especially important when national security is threatened. However, the judiciary is a reactive institution that can respond to police misconduct only when it becomes an issue in a criminal prosecution or the subject of a civil lawsuit or a judicial review of executive behaviour. Because many of the RCMP's national security activities will remain secret for legitimate reasons, affected individuals may never know that they have been the subject of a national security investigation. Even if they do know, they may not have the resources for a civil action or an action for damages under the Charter. The affected individual may be faced with claims of national security confidentiality that could prevent a full trial on the merits. Furthermore, the state may, for legitimate reasons, decline to prosecute a case because of a lack of admissible evidence that can be revealed in open court and disclosed to the accused, or a lack of a reasonable prospect of conviction. The reality is that most of the RCMP's national security activities will never be the subject of judicial review.

5.
WHY THE CPC'S EXISTING POWERS ARE NOT ADEQUATE

It would be wrong to suggest that there is no independent review mechanism now in place to review the RCMP's national security activities. As discussed in Chapter VI, the *RCMP Act* permits any person to complain about RCMP conduct, either directly to the RCMP or to the CPC. In extraordinary circumstances, such as the APEC demonstration and the Arar case, the CPC has begun its own public interest investigation or hearings. Normally, however, a complaint against the RCMP will be investigated by the RCMP itself, with possible further review by the CPC should the complainant not be satisfied with how the RCMP has settled the matter. The CPC can propose a resolution of the complaint — and reports that the RCMP accepts its resolution in most cases — but accepting this resolution remains a matter for the RCMP Commissioner.

While the existing system does allow some independent civilian scrutiny of the complaints process, and the CPC has in the past made a valuable contribution to the review of the RCMP, I conclude that it is inadequate for effective review of the RCMP's national security activities. One limit of the present system is that it is complaint-driven. As discussed above, many of the RCMP's national security activities will remain secret and thus will not be subject to complaints. Even with respect to activities that are not secret, such as the interviewing of

possible witnesses, some complainants may be unwilling to come forward with a complaint against the RCMP. Shirley Heafey, the former chair of the CPC, has spoken of the reluctance of possible complainants in national security cases to come forward. Several other intervenors, including the Canadian Arab Federation and the Canadian Council on American-Islamic Relations, have confirmed that many in the Muslim and Arab communities are reluctant to bring forward complaints against the authorities. While the existing *RCMP Act* provides some valuable alternatives to personal complaints — namely third-party complaints and public interest investigations and hearings — I agree that an effective review of the RCMP's national security activities cannot rely solely on complaints.

Complaints can provide a valuable window into RCMP activities, but given the secret and covert nature of many of the Force's national security activities, complaints in the national security context will provide only a small window into those activities. In 2003, the Auditor General concluded that "there should be more consistency in the extent of independent review applied to any environment where intrusive investigative measures are used."[18] The Auditor General noted that many national security investigations will not result in prosecutions or detailed supervision by the courts, and that the CPC does not review RCMP activities systematically to determine compliance with the law and ministerial direction.[19] Specifically, the Auditor General stated:

> The Commission for Public Complaints against the RCMP, in comparison to the Security Intelligence Review Committee, does not undertake reviews aimed at systematically determining compliance with the law, nor does its mandate provide for unrestricted access to all information.[20]

I agree that the CPC is deficient in this regard and does not have review powers to ensure systematically that the RCMP's national security activities are conducted in accordance with the law and with respect for rights and freedoms.

The existing CPC has fewer powers available to it than other review bodies in the national security field, including SIRC, the CSE Commissioner, the Privacy Commissioner and the Information Commissioner. In its submissions to this Inquiry, the CPC frankly and clearly argued that it lacked sufficient powers to review the RCMP. It observed that the current review process was crafted before integrated or intelligence-led policing and with:

> limited national security functions in mind . . . . As the CPC is a complaint-based review system, few intelligence-led policing activities will likely become the subject of reviews. The ability to perform audits of RCMP files would greatly enhance the CPC's effectiveness in this area . . . . The constraints imposed on the CPC include

> an inability to access all relevant information and the need for a complaint to base a review, investigation or hearing. Since 1988, changes in the way the RCMP police this country have only magnified the limits hampering the CPC's ability to review RCMP conduct. Intelligence-led policing, integrated policing and a re-emergence by the RCMP in the field of national security activities have only served to highlight the CPC's pre-existing limitations.[21]

Although the CPC raises these concerns about lack of powers with respect to all its dealings with the RCMP, its lack of powers could particularly weaken its effectiveness in the national security context because of the role of national security confidentiality. I am convinced that to do an adequate job, a review body must have unrestricted access to all information, including confidential national security information. The increase in information exchange between governments around terrorism investigations also means that the RCMP will increasingly have information obtained from a foreign entity during national security investigations. In such an environment, it is vitally important that the body that reviews the RCMP's national security activities have the same powers to access RCMP information that SIRC has in relation to CSIS.

In the past, the CPC has had difficulty getting access to information that would be harmful to international relations, national security or defence.[22] Any difficulty in having access to such information raises distinct concerns in the national security context, where most information by definition will relate to national security and often may have implications for international relations. The CPC also was recently denied access to information covered by informer privilege.[23] In the national security field, there may be extensive reliance on informers. Moreover, there is a legitimate public interest in ensuring that proper practices and procedures are followed with respect to informers, who might provide unreliable and even deliberately misleading information.

The existing jurisprudence further suggests that the CPC may have difficulty obtaining information provided to the RCMP by its legal advisors. This raises distinct concerns in the national security context because of the requirements that an attorney general consent to the prosecution of terrorism and *Security of Information Act* offences, as well as to investigative hearings and preventive arrests. When evaluating the propriety and legality of a past event, a review body may have a legitimate public interest in examining the legal advice the RCMP has received about that past event. In its own submission, the RCMP recognizes that requirements for the Attorney General's consent operate as a "sober second thought" on some operational decisions. In such a context, the review body may have a legitimate interest in examining the content and pattern

of such sober second thoughts. I hasten to add, however, that solicitor-client privilege remains an important and foundational privilege. A review body would not have an interest in seeing information exchanged between an individual RCMP member and that member's lawyer, or legal advice that the RCMP has received about an ongoing dispute with the review body.

Some might argue that the need-to-know rules and concerns about leakage suggest that the RCMP's review body should not have access to information covered by national security confidentiality. I reject these arguments. Those who are entrusted with review functions will be subject to security clearances and possible prosecution under the *Security of Information Act*. I am also influenced by CSIS' submission about its positive experience with SIRC and the Inspector General around national security confidentiality, where it noted that:

> [initial] concerns that comprehensive SIRC/IG access to Service files would cause nervous international partners and liaisons to restrict intelligence exchanges have not, in the long run, come to pass. Related worries about SIRC/IG ability to provide proper security to Service information and protect its human sources and sensitive collection methodologies have not been justified – "leakage" of classified information has not been a factor.[24]

In my view, CSIS' positive experience with SIRC suggests that increased review of the RCMP's activities can take place without compromising the RCMP's vital responsibilities for national security.

6. WHY THE EXISTING POWERS OF OTHER ACCOUNTABILITY BODIES ARE NOT ADEQUATE

The CPC is not the only body that could review the RCMP's national security activities at this time. Several other federal review bodies, including the Auditor General, the Canadian Human Rights Commission and the Privacy Commissioner, could also review RCMP activities in certain circumstances. Although each of these could make important and distinctive contributions to review, I nevertheless conclude that even when collectively combined with the CPC, they lack sufficient powers, resources and expertise to fully and effectively review the RCMP's national security activities.

Each of these agencies has a different mandate. The Auditor General is generally concerned with the efficiency of governmental work, although the Office has shown an increasing interest in ensuring that proper systems are in place. In a November 2003 report, the Auditor General raised concerns about whether the review of the RCMP was adequate, compared to the review available for

much of Canada's security intelligence community.[25] While the Office has done valuable work on various national security matters and can bring fresh and critical eyes to a broad range of governmental work, it does not have the expertise to review RCMP national security activities to ensure their legality and propriety. As the British Columbia Civil Liberties Association (BCCLA) noted in its supplementary submission, the Auditor General's criticisms are appropriately "focused on enhancing performance and efficiency" and not on "respect for the rule of law and civil liberties."[26]

The Canadian Human Rights Commission has legal expertise, but focuses on the important issue of discrimination. I believe that the review body for the RCMP should work closely with the CHRC, especially concerning allegations of racial or religious profiling or other discriminatory practices. However, as the BCCLA argued, equality is not the only constitutional value that can be adversely affected by national security investigations. A review body should have expertise with respect to the Charter and statute law as they affect all police powers, and on issues such as privacy, fairness and reliability of investigative procedures.

I also note that regarding CSIS, sections 45 and 46 of the *Canadian Human Rights Act* allow the Canadian Human Rights Commission to refer matters to the Security Intelligence Review Committee where the Minister has indicated that there are national security concerns. Consideration should be given to enacting a similar provision to allow the Canadian Human Rights Commission to refer matters involving the RCMP and national security to the enhanced review body. More statutory gateways are needed between the various review bodies that examine matters affecting national security so as to ensure that investigations are not frustrated by concerns about national security confidentiality. In appropriate circumstances, an enhanced review body might be able to assist the work of the CHRC in investigating complaints that involve the RCMP and national security matters.

In her submission to this Inquiry, the Privacy Commissioner was candid about the limits on her resources and powers when it comes to reviewing the RCMP's national security activities: "We recognize and accept that we cannot exercise effective oversight on our own. The task is simply too large and too important to be entrusted exclusively to any single agency."[27] At the same time, the Privacy Commissioner, like the Auditor General, has already made valuable contributions to the review of the RCMP. In 2002, the Privacy Commissioner reviewed the information-handling practices of both Integrated National Security Enforcement Teams and Integrated Border Enforcement Teams,[28] and plans to examine data banks that are exempt from public disclosure within the RCMP for compliance with the *Privacy Act*.[29]

Despite the fact that these review bodies cannot themselves provide adequate review of RCMP national security activities, I envision that they will continue to play a role in the enhanced review that I recommend. As in other areas of governance, there is much to be said for checks and balances and multiple perspectives when it comes to review. While every effort should be made to avoid wasteful duplication of review structures, it is valuable that the Auditor General, the CHRC and the Privacy Commissioner all approach review of the RCMP with different perspectives and different mandates. Moreover, each of these bodies can help remind the institution that reviews the RCMP's national security activities of its distinct concerns.

All review institutions should meet regularly to share information and work plans with other review institutions. In some cases, coordinated reviews, and even joint reviews, may be appropriate. In the next chapter I will recommend a new institution that can play a valuable role in coordinating review. At the same time, all the review bodies examined in this section have important responsibilities across the federal government. There remains a need for specialized and day-to-day review of the RCMP's national security activities.

Notes

1 *Re s. 83.28 of the Criminal Code*, [2004] 2 S.C.R. 248; *Re Vancouver Sun*, [2004] 2 S.C.R. 322; *R. v. Malik*, [2005] B.C.J. 350 (B.C.S.C.).

2 "As the legal authorities and activities of our security and intelligence agencies evolve to respond to the current and future security environment, it is vitally important that we ensure that review mechanisms keep pace.": *Securing an Open Society: Canada's National Security Policy* (Ottawa: Privy Council Office, 2004), p. 19, online, http://www.pco-bcp.gc.ca/docs/Publications/NatSecurnat/natsecurnat_e.pdf.

3 2003 Reports of the Auditor General of Canada to the House of Commons, Chapter 10: "Other Audit Observations" (Ottawa: Public Works and Government Services Canada, 2003), paras. 10.139–10.150, online, http://www.oag-bvg.gc.ca/domino/reports.nsf/html/20031110ce.pdf [Auditor General of Canada report]; "Submissions of the Commission for Public Complaints Against the RCMP Regarding the Policy Review of the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar" (Written submission to the Arar Commission Policy Review Public Submissions), February 21, 2005, pp. 20–40 [CPC submission]; *SIRC Annual Report 2004–2005: An Operational Review of the Canadian Security Intelligence Service* (Ottawa: Public Works and Government Services Canada, 2005), p. 95, online, http://www.sirc_csars.gc.ca/pdfs/ar_2004-2005_e.pdf; Privacy Commissioner of Canada Submission to the Arar Commission Policy Review (Written submission to the Arar Commission Policy Review Public Submissions), November 2, 2005 [Privacy Commissioner of Canada submission].

4 The McDonald Commission stated: "Our view is that the work of an external review body should go beyond the traditional role of the Ombudsman of responding to individual complaints and should involve a *continuing* review of the adequacy of the R.C.M.P.'s practices. Such matters, we feel, should be within the mandate of an external body charged not only with

reviewing the R.C.M.P.'s disposition of complaints, but also with identifying problems within the R.C.M.P. which may have contributed to the incidents in question [emphasis in original]." Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Freedom and Security under the Law*, Second Report, vol. 2 (Ottawa: Supply and Services Canada, 1981), p. 987, para. 52 (Chair: D.C. McDonald).

5 The RCMP, the Ontario Provincial Police and the Ottawa Police Service in their respective submissions directed us to the many existing review mechanisms on police forces. The Canadian Association of Chiefs of Police raised concerns about the lack of a policy framework for integrated policing.

6 CPC submission.

7 Hooper testimony, Arar Commission Factual Inquiry Public Hearing (June 22, 2004), pp. 435–436.

8 Giuliano Zaccardelli, Transcript of Arar Commission Policy Review Public Hearing (November 18, 2005).

9 "Policy Review Submission of Maher Arar" (Written submission to the Arar Commission Policy Review Public Submissions), November 14, 2005, pp. 2–3 [Arar submission].

10 Exhibit P-12, Tab 24, Arar Commission Factual Inquiry.

11 Ibid.

12 "The RCMP is a police force and as such its investigations are carried out at arm's-length from government . . . . The practice is for police matters to be subject to independent review by special-purpose commissions, and ultimately by the courts . . . . [There is a] general practice, in Canada and elsewhere, of not engaging Parliament in the review of police investigations . . . . " *A National Security Committee of Parliamentarians: A Consultation Paper* (2004), pp. 9–10, online, ww2.psepc-sppcc.gc.ca/publications/national_security/nat_sec_cmte_e.pdf (accessed April 25, 2006).

13 "Submission on Behalf of the Ontario Provincial Police to the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar" (Written submission to the Arar Commission Policy Review Public Submissions), p. 13.

14 "RCMP Response to the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar" (Written submission to the Arar Commission Policy Review Public Submissions), February 2005, p. 27 [RCMP submission].

15 Ibid., p. 28.

16 *Criminal Code*, ss. 25.1, 186.

17 *Re s. 83.28*, *supra* note 1; *Re Vancouver Sun*, *supra* note 1.

18 Auditor General of Canada report, para. 10.161.

19 Ibid., para. 10.144.

20 Ibid., para. 10.161.

21 CPC submission, pp. 35, 37, 39.

22 *Re Rankin*, [1992] F.C. No. 502.

23 *Royal Canadian Mounted Police Public Complaints Commission v. Attorney General of Canada*, 2005 F.C.A. 213 at para. 32.

24 "Control, Accountability and Review: The CSIS Experience" (Written submission to the Arar Commission Policy Review Public Submissions), February 21, 2005, p. 5.

25 Auditor General of Canada report, para. 10.120ff.

26 "British Columbia Civil Liberties Association Supplementary Submission" (Written submission to the Arar Commission Policy Review Public Submissions), November 9, 2005, p. 15.

27 Privacy Commissioner of Canada submission, p. 2.

28 Privacy Commissioner of Canada, *Annual Report to Parliament 2003–2004*, pp. 48–49, online, http://www.privcom.gc.ca/information/ar/200304/200304_e.pdf.

29 Privacy Commissioner of Canada submission, p. 6.

XI
Recommendations

1.
INTRODUCTION

The RCMP is presently subject to a number of different accountability mechanisms, both internal and external, for its national security activities. While they perform valuable roles in facilitating its accountability, I have reached the conclusion that the RCMP's national security activities can most effectively be reviewed by a new review mechanism with enhanced powers that would be located within a restructured Commission for Public Complaints Against the RCMP (CPC).

This chapter contains my recommendations and rationale for this review mechanism, as well as for independent review of five other departments and agencies, and for mechanisms to coordinate the work of all national security review bodies. A summary list of the recommendations is set out at the end of this chapter.

Before turning to a discussion of my recommendations, I believe it is useful to summarize the following points made in the previous three chapters:

- what I mean by "review;"
- the important characteristics of national security; and
- the fundamental objectives of review.

1.1
REVIEW VERSUS OVERSIGHT

In Chapter IX, I describe the difference between "review" and "oversight," and explain why I believe that the most appropriate accountability mechanism for the RCMP's national security activities is a review body. To summarize, a review

body assesses the activities of an organization against standards such as lawfulness and propriety and delivers reports, which often contain recommendations, to those in government who are politically responsible for the organization. In contrast, an oversight body performs the same functions but plays a more direct role in the management of the organization.

One of the main reasons I reject the option of an oversight mechanism is that it could intrude upon the principle of police independence if it became involved in management or operational decisions relating to the RCMP's activities as a law enforcement agency. There is also a risk that an oversight mechanism could confuse or even diminish the accountability of the RCMP to government and, correspondingly, the responsibility of government for the RCMP. Finally, there is a danger that an oversight body's review function would be compromised by its active involvement in the activity being reviewed. This could occur where the oversight body approved or, alternatively, failed to veto or prevent an activity by the agency subject to oversight.

In contrast, a body that exercises nothing but review has greater independence and can maintain a critical distance from the activities being reviewed. I note that it was broadly accepted by virtually all participants in this Inquiry that the "review mechanism" referred to in my mandate should in fact be a review body rather than an oversight mechanism.

1.2
CHARACTERISTICS REQUIRING ENHANCED REVIEW

Many of my conclusions and recommendations address the special characteristics of national security that I describe in detail in Chapter VIII. In summary, these are:

Lack of Transparency

The lack of transparency in national security investigations means that those affected will often not know that an investigation is taking place or has been completed. Even if they do learn of the investigation, they will seldom be aware of the specific investigative steps that may have an impact on their interests. As a result, the usefulness of a complaints process such as that provided by the existing Commission for Public Complaints Against the RCMP (CPC) is greatly diminished. Instead, what is needed to achieve accountability for national security investigations is a review body that is able to conduct self-initiated reviews similar to those conducted by the Security Intelligence Review Committee (SIRC), which reviews the frequently secret activities of CSIS.

Increased Information Sharing

As the flow of information between agencies increases, so too does the need for a strong and effective review mechanism. To ensure that information sharing is being conducted in conformity with law and policy and that it is not having an unfair or improper impact on individuals or groups, it is essential that RCMP policy in this regard be followed. A strong system of review should play an important role in ensuring that information-sharing practices comply with policy and accepted norms.

Increased International Co-operation

National security investigations typically involve more co-operation with agencies of foreign governments than do other criminal investigations, and it most often includes information sharing. The RCMP has policies to guide decision making about information sharing when there are potential human rights implications. In the Factual Inquiry report, I concluded that the policies are inadequate, especially in relation to terrorism investigations, and should be strengthened to ensure that greater attention is paid to the human rights implications of sharing information with countries with poor human rights records, as well as receiving information from them. Decisions in such instances are vitally important and must be made in ways that are accountable and subject to independent review. It is therefore essential that there be a strong review mechanism that has ready access to all relevant information and is not tied to the investigation of individual complaints.

Potential for Racial, Ethnic and Religious Profiling

National security investigations create more of a potential for discriminatory profiling decisions than virtually any other type of criminal investigation. Moreover, any such decisions in the national security context are highly unlikely to be made public or come to the attention of the individuals affected. The likelihood of a complaint that could form the basis for review is small. A purely complaints-driven review process would fall well short of the mark in terms of providing accountability for discriminatory profiling decisions. An enhanced, robust review system should go a long way toward addressing the perceptions of some that discriminatory profiling is a reality in the national security field.

Lack of Judicial Scrutiny

One of the most effective means of ensuring accountability for law enforcement activities is scrutiny by the courts. However, the opportunity for judicial scrutiny

in the case of national security investigations is far less than for all other types of criminal investigations because of the much smaller number of prosecutions. Moreover, in the case of national security investigations, judicial pre-authorizations for certain investigative steps are necessarily obtained *ex parte* — in the absence and without the knowledge of those affected — and there is no opportunity to challenge them if there is no subsequent prosecution. Enhanced and effective independent review is essential to compensate for this lack of judicial scrutiny.

1.3 OBJECTIVES OF REVIEW

The overarching objective of review of the RCMP's national security activities is straightforward: to hold the RCMP accountable for those activities. To summarize my analysis in Chapter IX, this overarching objective may be broken down into a number of more specific objectives, as follows.

Ensure Conformity With Law, Policy and Standards of Propriety

Review should provide assurance that the activities of the RCMP comply with the *Canadian Charter of Rights and Freedoms* (the Charter), the law, ministerial directives, RCMP policy, international obligations and standards of propriety that are expected in Canadian society. Although the review body should focus mainly on legality and propriety, it should not be prevented from making recommendations dealing with the efficacy of national security activities, particularly when issues in this regard arise out of propriety reviews or complaints.

Foster Accountability to Government

The second fundamental objective of review of the RCMP's activities is to enhance or foster the RCMP's accountability to those politically responsible for it and, concurrently, to enhance and facilitate government answerability for those activities. Notwithstanding the principle of police independence and the limits it places on government involvement in criminal investigations, the RCMP is accountable to the government for, at a minimum, the legality and propriety of its activities. In turn, the government, through the Minister, is responsible to Parliament and to Canadians for the legality and propriety of RCMP activities. An independent review mechanism should foster ministerial accountability and also provide the Minister with recommendations for improvement.

Foster Accountability to the Public and Facilitate Public Trust and Confidence

The third fundamental objective of a review mechanism is to enhance the RCMP's accountability to the public, thereby engendering public trust and confidence in the Force. Certain features of review will be essential to achieve this objective. First, the review mechanism must be independent of and at arm's length from both government and the RCMP. Second, the public must be satisfied that those carrying out the review are qualified to do so. Finally, the review body must aim for as much transparency as possible. This means an open and fair process for appointing individuals to the review body, public education about the role and activities of the review process, and disclosure, to the extent possible, of its activities and findings.

2.
RECOMMENDATIONS AND RATIONALES

In light of the above discussion and conclusions, the following are my detailed recommendations regarding review of the RCMP's national security activities**.**

2.1
Recommendation 1

Existing accountability mechanisms for the RCMP's national security activities should be improved by putting in place an independent, arm's-length review and complaints mechanism with enhanced powers.

Presently there are a variety of internal and external controls or accountability mechanisms for the RCMP's national security activities. In Chapter X, I discuss the role of each of these accountability mechanisms and why, in my view, they, either individually or taken together, do not adequately review the RCMP's national security activities and do not achieve the objectives for review that I have discussed in Chapter IX. Without repeating the analysis in the preceding chapters, it is useful to set out, in summary form, the main features that, in my view are required for effective review[1] of the RCMP's national security activities.

Independence — A review mechanism for the national security activities of the RCMP must be, and be seen to be independent. Independence and the perception of independence are critical to ensuring accountability and developing public trust. Therefore, I recommend that the review body for the RCMP's national security activities be independent in the judicial sense from the RCMP, the government and other interested parties. Those appointed to the review body must have no interest or perceived interest in matters that may be the subject of

review. They must be impartial in the same way that judges are impartial. In addition, those appointed must be credible and have all of the skills and expertise necessary to conduct effective reviews. Importantly, their backgrounds should engender public confidence and trust in their review activities.

Power to Provide Comprehensive Review, Both Through Self-Initiated Review and the Investigation of Complaints — To be effective, review must be comprehensive. Comprehensive review encompasses three elements. First, it must encompass a comprehensive range of standards, including review for compliance with law, policies, ministerial directives, international obligations and standards of propriety. To be comprehensive, review must also cover the full range of RCMP national security activities. In this regard, the current mechanisms fall short. There are a number of review bodies, including the Auditor General and the Canadian Human Rights Commission, that in certain circumstances review some RCMP activities. While each of these bodies makes an important contribution to RCMP accountability, they do not individually or collectively have the jurisdiction to provide comprehensive review of the RCMP's national security activities. Thirdly, comprehensive review must be carried out in a manner likely to lead to the assessment of the full range of these activities. In other words, a jurisdiction covering all national security activities is not enough. The form that review takes must be such that the full range of activities are actually reviewed. In this regard it is critical that review of national security activities go beyond the investigation of complaints. While a complaints investigation power is important, because of the covert nature of so many of the activities it will inevitably miss many of the types of activities that should be reviewed.

Extensive Investigative Powers — In order to be effective, it is critical that a review body have adequate powers to conduct comprehensive and effective reviews. The CPC has been frank and unequivocal in stating that it does not have sufficient powers to effectively review the RCMP's national security activities. Effective review requires adequate powers to access all information relevant to its mandate, including national security information, and, with only minimal exceptions, other confidential information from both within and outside of the RCMP. Moreover, the review mechanism requires the power to determine itself what information is necessary in order to conduct an effective review. Clearly, the final say with respect to what information the review mechanism can access cannot lie with the entity being reviewed.

Power to Conduct Integrated Reviews — The review body for the RCMP's national security activities should have sufficient powers to ensure that the integrated activities of the RCMP are effectively and throroughly reviewed. Given

the importance of integrated and cooperative activities among Canada's national security actors, it is critical that a review mechanism include an ability to conduct reviews on an integrated basis.

2.2
Recommendation 2

The review and complaints body should be located within a restructured Commission for Public Complaints Against the RCMP, and be renamed the Independent Complaints and National Security Review Agency for the RCMP (ICRA for short) to reflect its expanded role.

2.2.1
Background

2.2.1.1
Law Enforcement / Security Intelligence Operations

Over twenty years ago, Canada made a considered decision to separate the law enforcement activities of the RCMP, a law enforcement agency, from security intelligence activities. In 1984, the government implemented the recommendations of the McDonald Commission and created CSIS, a civilian security intelligence agency. In doing so, it provided that the RCMP would continue to have primary responsibility for law enforcement in the national security field. The principal reasons underlying the recommendations in the McDonald Commission report are discussed in Chapter II. They relate to important differences in mandates, powers and political accountability between security intelligence agencies and police agencies. The rationale to which the government responded was sound then and continues to be sound today.

Under the *RCMP Act*, the RCMP has a law enforcement mandate. It is responsible for investigating, preventing and prosecuting criminal activity. That mandate is linked to criminal or other offences, including inchoate offences such as conspiracy, counseling and attempts. As a law enforcement agency, the RCMP has a broad range of coercive powers, including powers to detain, search, use force and arrest. Since, in our society, such coercive powers of the state are generally restricted to agencies with a mandate linked to criminal or unlawful activity, it is important that the RCMP remain within its law enforcement mandate, no matter what type of activity is being investigated.

CSIS, on the other hand, has a security intelligence mandate. It collects and analyzes information for purposes of advising government and assisting it with

the development of policy for addressing threats to the security of Canada. As emphasized by the Royal Commission on Security (MacKenzie Commission) in 1969 and the McDonald Commission in 1981, it is not appropriate for a body whose role is to advise and assist government in the development of policy to have the same coercive powers as a law enforcement agency. Most other federal agencies involved in national security activities tend to fit the security intelligence mold more than the law enforcement one. Some, such as the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) and DFAIT, have an explicit mandate to pass information on to the police in appropriat cases. The one exception is the CBSA, the mandate of which includes some law enforcement.

In the Factual Inquiry report, I indicated that it is important to maintain the operational distinction between law enforcement and security intelligence activities in the national security field. The distinction is fundamental and results in a principled and practical way of approaching Canada's national security operations.

I say principled because the use of police powers should not be expanded beyond law enforcement simply because a matter relates to national security. The rationale for confining the use of police powers to a crime-based law enforcement mandate, whether prevention or prosecution, is as valid in the national security field as elsewhere. It is also practical to maintain the distinction between law enforcement and security intelligence agencies because the expertise and techniques required for law enforcement are significantly different from those used by security intelligence personnel. While there may be overlap in the subject matter of the two types of investigation, the aims and the techniques and procedures used are different.

Thus, for operational purposes, maintaining a distinction between law enforcement and security intelligence activities is important.

2.2.1.2

Function-Based Versus Agency-Based Review

One of the threshold issues in considering a review mechanism for the RCMP's national security activities is whether the review body should have jurisdiction over all institutions involved in national security activities, including the RCMP, or whether it should be dedicated solely to the RCMP. At the extreme, the choices are between a function-based body and an agency-based body, that is, a body with a mandate to review all federal national security activities or functions, no matter what agency conducts them, and a review body that, as in the case of the RCMP, is dedicated to reviewing only the activities of the RCMP, -

including its national security functions. Between the two are countless possible variations of models that have both agency-based and function-based aspects.

A function-based system encompassing all of the Canadian government's national security activities would have several advantages, mostly related to situations where the activities being reviewed are integrated, are carried out cooperatively or otherwise overlap. A broad function-based review system could avoid accountability gaps, as a single review body would have jurisdiction over all of the agencies involved. It could also be an effective platform from which to make observations and report on the overall functioning of the country's national security system, with a view to identifying emerging trends or problems. Moreover, a function-based review body could ensure a single point for laying complaints and provide consistent and coordinated review for several agencies involved in national security activities.

The main advantage of an agency-based system, on the other hand, is the capacity to develop greater expertise and acquire more experience in reviewing the activities of one agency. This is particularly advantageous when those activities differ significantly from those of other agencies involved in national security. Also, in the case of the RCMP, a broad function-based review mechanism would have a mandate to review only one small portion of its overall activities — those related to national security. Clearly, an agency-based review body that would look at all of the RCMP's activities would be better positioned to develop a sophisticated understanding of the Force.

There can also be practical difficulties in a function-based mechanism, in terms of separating one function from the balance of operations for review purposes. For example, in the case of the RCMP, what starts out as a criminal investigation into suspected fraud or theft may turn into a criminal investigation related to national security, and what starts as a national security criminal investigation may turn into a regular criminal investigation. As the Ottawa Police Service submitted at the Policy Review public hearing, there is often no bright line between national security and other forms of policing. When there is more than one review body for an agency, it becomes necessary to draw lines for jurisdictional purposes and there is a danger that matters will fall between the cracks and produce accountability gaps.

The national security activities of the RCMP as a law enforcement agency are different from those of most other national security actors. In addition, their potential impact on people's lives is different. To repeat just one of many examples, the RCMP, unlike most other agencies, has powers to arrest, charge and detain. There is a risk that basing a review on a national security function alone would minimize the important distinctions between law enforcement

and other national security activities, such as analyzing and developing security intelligence to advise government of security threats and making security threat assessments.

The model I propose for Canada has both agency- and function-based features. The review body for the RCMP is agency-based, but is also grounded in the law enforcement function and would include review of the national security activities of the CBSA. The expanded mandate for SIRC and INSRCC are clearly function-based.

2.2.1.3 Existing Arrangements in Canada and Elsewhere

There is a long tradition of independent review of law enforcement agencies in Canada. In Chapter VI I describe the current regimes for reviewing some of the police forces across the country. There is no experience in Canada with combining the review of law enforcement agencies with the review of other agencies. The Canadian tradition does not include this type of function-based review. While there may be co-operation among review bodies for police forces or other agencies, the tradition in Canada has been for dedicated review bodies to review law enforcement agencies.

The international experience is interesting, but, in the end, it is so varied and intertwined with the unique constitutional, cultural and historical features of each country, that it does not point to a single solution in the Canadian context. Ultimately, the model that is best for a particular country depends on that country's constitutional framework, the culture, history and effectiveness of the agencies involved in national security activities and, importantly, the practicalities that may make one model more effective than another.

Of the eight countries examined in Chapter VII, three separate the review of police forces from that of intelligence services: Belgium (Committee P and Committee I), Germany[2] and New Zealand (Police Complaints Authority and Inspector-General of Intelligence and Security). In the United Kingdom, the primary review bodies are specialized either in police (Independent Police Complaints Commission / Police Ombudsman for Northern Ireland) or intelligence review (Intelligence Services Commissioner). However, the review of certain investigatory powers is functionally defined to cover all domestic, covert investigative activities, whether carried out by the police or the security intelligence agency. Functional review in the United Kingdom is therefore limited to particularly intrusive investigative techniques. It does not cover the exercise of most police powers related to investigation, information sharing, arrest powers, or use of force.

In the United States, review jurisdiction is based entirely on the government department: the FBI is reviewed by the Inspector General of the Department of Justice, the CIA, by the Inspector General of the CIA, the National Security Agency, by the Inspector General of the Department of Defense, and so on. It must be noted that the FBI has both a law enforcement mandate and a dedicated national security branch, which is the United States' primary domestic intelligence agency. All FBI officers have full police powers and receive police training. Given the breadth of the FBI's mandate, review by the Inspector General includes both law enforcement and security intelligence activities.

The Norwegian Police Security Service has both law enforcement and security intelligence functions, as does Sweden's security service, *Säpo*. The Australian Crime Commission, reviewed by the Commonwealth Ombudsman, is really an integrated team, with members from both intelligence and police agencies. In all three countries, the review body reviews both law enforcement and security intelligence activities. However, as with the FBI in the United States, this is the result of the fact that both types of activities are carried out by a single agency.

2.2.2
Rationale for Recommendation

In the sections that follow, I set out my three main reasons for recommending that the review of the RCMP's national security activities should be located within the same body that reviews other RCMP activities. They are effectiveness, practicality and the capacity to deal with integrated operations. In the final section under this recommendation, I explain why I believe this review body should be a restructured CPC.

2.2.2.1
Effectiveness

The most important factor in recommending that a review mechanism for the RCMP's national security activities be located within the same body that reviews other RCMP activities is maximizing the effectiveness of review. Effectiveness is to a large extent dependent on the experience and expertise of the review body. I am convinced that a review body dedicated to reviewing all of the RCMP's law enforcement activities will have a much greater ability to develop the expertise and experience necessary to effectively review the Force's national security activities. In addition, a review body dedicated to the review of all RCMP law enforcement activities will heighten effectiveness by

eliminating the difficulties associated with trying to separate national security activities from the RCMP's other activities.

Reviewing law enforcement activities is difficult and complex. It requires detailed and sophisticated expertise and knowledge of a broad range of matters. Such expertise and knowledge are not developed quickly and, once developed, need to be updated regularly. Experience acquired over time, including through ongoing exposure to a broad range of law enforcement activities, is very important to maintaining the necessary level of expertise for effective review.

Proper review of the RCMP's activities, whether in the national security field or other fields, requires detailed knowledge of, among other things, the *Canadian Charter of Rights and Freedoms* and related jurisprudence, criminal law, criminal procedure, the laws of evidence, voluminous RCMP policies, ministerial directives, principles relating to police independence, common law jurisprudence and Quebec civil law relating to peace officers, law relating to police use of force, and often complex law governing the use of law enforcement powers.

In addition, effective review requires an understanding of the criteria applied in deciding to initiate investigations and an understanding of policing methods and techniques, including those for interviewing witnesses, interrogating suspects, conducting surveillance, obtaining and executing warrants, using force, issuing police cautions and exercising powers of arrest.

It is also necessary for a review body for the RCMP's national security activities to have an understanding of the command structure within the RCMP, the ways in which information collected is analyzed and shared, and the manner in which the RCMP relates to other law enforcement agencies. In the latter regard, the review body needs to appreciate the ways the RCMP shares information with foreign agencies and how it co-operates internationally, and what Canadian law enforcement officers should and may properly do outside of Canada.

Two points regarding expertise and experience are particularly important. First, the expertise required to review law enforcement activities in the national security field is very different from that required to review security intelligence activities. That should not be surprising. The two types of activities have entirely different purposes: law enforcement seeks to prevent and prosecute crimes; security intelligence aims to collect and analyze information to guide government policy making in relation to addressing threats to Canada's national security. The RCMP's law enforcement mandate means that a review mechanism must have expertise in the above activities and powers, many of which are not part of the mandates of security intelligence agencies (for example, the interrogation of suspects or use of force, powers of arrest, or the power to

perform acts that would otherwise be unlawful). Even where powers are broadly similar (interviewing people or collecting and analyzing information), the context will be different. Most significantly, the RCMP's activities must always be carried out within the particular discipline of its law enforcement mandate. This means that admissible evidence must be obtained to establish that a crime has been committed, and the product of an investigation may be used as evidence in court. This is not the case with the activities of a security intelligence agency such as CSIS.

That said, the subject matter of an RCMP national security investigation may often cover the same area and may even rely on information obtained from CSIS. Clearly, co-operation between the two agencies in the national security field is critical. However, the need for co-operation should not mask the fundamental difference in what each does.

The second point is that, while I recognize that authority to review the RCMP's national security activities could be vested in a separate division of a review body that also reviews the security intelligence activities of other agencies, and while such a division potentially could, over time, develop expertise and experience in reviewing law enforcement activities, such an approach carries risks that are easily avoided by establishing a review body with jurisdiction over all of the RCMP's activities. The RCMP's national security activities are a very small part of the Force's overall operations. Only about 300 officers out of 22,000 are dedicated solely to such activities. A review body limited to reviewing the RCMP's national security activities would have a very narrow window from which to gain expertise and experience in reviewing law enforcement activities generally. I am very concerned that such a review body would constantly be confronted with unfamiliar circumstances and issues relating to the conduct of criminal investigations and the use of law enforcement powers. It seems clear that a review body that examines all of the RCMP's activities will be far better positioned to develop the expertise and experience necessary to effectively review its national security activities. Obviously, those reviewing such activities will need some special training on national security matters. However, the knowledge necessary to review national security matters is far more easily acquired than that required to review law enforcement activities generally.

I am also very concerned that, if the review of the RCMP's national security activities were separated from that of the rest of the RCMP's operations, expertise and experience in reviewing law enforcement activities would diminish over time. That would be the case even if those at the CPC with experience were to be transferred to a new review body. Without ongoing exposure to all

of the RCMP's law enforcement activities, a review body would inevitably become less effective.

Furthermore, as mentioned above, there is often no bright line between the RCMP's national security and other law enforcement activities. What starts out as a fraud or theft investigation may turn out to be a national security investigation if the act or omission being investigated was committed by or for the benefit of a terrorist group. The *Criminal Code* covers both national security and regular policing matters. It defines a terrorist offence as including not only indictable offences that constitute terrorist activity, but also any indictable offence committed for the benefit of, at the direction of or in association with a terrorist group.

There may also be legitimate reasons for charging a subject of a national security investigation with a variety of criminal offences that do not on their face involve national security. The line between national security and regular criminal law enforcement matters is often a fine one and the RCMP may choose to use the regular tools of law enforcement in some investigations that actually concern national security. In some cases, it may be easier to prove beyond a reasonable doubt that the subject of a national security investigation committed a fraud or a murder than to prove any of the terrorism offences set out in the *Criminal Code*. *Criminal Code* and *Security of Information Act* prosecutions may also raise complex issues concerning national security confidentiality and disclosure to the accused.

It is vitally important that the review body be able to follow the national security trail within the RCMP wherever it may lead. A body with jurisdiction over all RCMP law enforcement activities will be in the best position to provide effective review of all the Force's national security activities, including those that may not be formally designated as such.

Some have suggested that the review of the RCMP's national security activities should be divided into self-initiated reviews by a review body and complaint investigations. According to this suggestion, the self-initiated review function would be moved to a review body with jurisdiction over all of Canada's national security activities, while the complaint handling function would continue in a body dedicated to investigating and reporting on all complaints with respect to the RCMP. This is not the best approach, in my view. There is considerable advantage to having all complaints and self-initiated reviews involving national security activities handled by the same review body. The importance of having the two functions within the same body was stressed repeatedly during our consultation with review bodies in other countries, and SIRC made the same

point. The skills and expertise developed in investigating and reporting on complaints greatly enhances the capacity to conduct effective self-initiated reviews.

I recognize that, if separate bodies handled complaints and self-initiated review, the review body could deal with some of the more significant, policy-related complaints. Even then, however, a review body that considered only some complaints might not always be able to assess from the outset whether a particular complaint would raise important policy issues. Moreover, separating the two functions could lead to the application of inconsistent or different standards by different bodies, which is undesirable. I am of the view that the complaints and self-initiated review functions should reside in the same body.

2.2.2.2
Practicality

The second reason for having a single review body for all RCMP activities is that it is the most practical approach. A single agency avoids having to make changes to existing institutions when not required.

All things being equal, it makes sense that I not make recommendations to create new institutions. Start-up costs of new institutions, both financial and otherwise, can be considerable. Currently, the RCMP is subject to independent review by the Commission for Public Complaints Against the RCMP (CPC). However, there are a number of problems with the CPC as it is now structured. As I discuss below, I am of the view that the CPC can be restructured to make it an effective review body. It makes practical sense to have a restructured CPC with enhanced powers continue as the review mechanism for the RCMP's activities, including its national security activities.

2.2.2.3
Integrated Activities

The third reason for a single review body for all RCMP activities is more in the nature of an answer to arguments for a single review body for all of Canada's national security activities. Arguments in favour of the latter are not based on the idea that such a body would be more effective in reviewing the RCMP's national security activities. Rather, they rest primarily on the notion that the challenge of reviewing integrated operations can only be addressed by establishing a common review body for all national security activities. In addition, some proponents of a single national security review body appear to believe that such a body could be used to extend independent review to federal agencies and departments involved in national security activities, but currently not subject to independent review.

I have two responses to these arguments. First, I am satisfied that statutory gateways and a national security coordinating committee, along with genuine co-operation among review bodies, can be effective and can address concerns about reviewing integrated operations. I discuss the reasons for this conclusion in recommendations 11 and 12.

Second, in Recommendation 9, I propose the expansion of independent review to cover certain other agencies involved in national security activities. In any event, the need for independent review of a broader range of national security actors is a separate issue and should not be allowed to detract from the objective of recommending the most effective review mechanism for the RCMP's national security activities.

Concerns arising from the integrated nature of the RCMP's national security operations need not govern the decision about which body would provide the most effective review for its national security activities. I am satisfied that both the goals of providing effective review and meeting the integrated operations challenges can be achieved by having all RCMP activities, including national security activities, reviewed by a single body and developing other means to deal with integrated national security activities. As already mentioned, I discuss two such means, statutory gateways and the Integrated National Security Review Coordinating Committee, in recommendations 10 and 11.

2.2.3
A Restructured CPC

In my view, the advantages of building the new single review mechanism on the foundation of the existing CPC are significant and the disadvantages, not insurmountable.

There are three principal advantages to beginning with the CPC. The first is that the CPC has extensive expertise in reviewing law enforcement activities. I have already noted the importance of such expertise and the difficulty involved in creating it in a body that does not have extensive exposure to law enforcement activities and the overall context of a law enforcement agency. The CPC is in an excellent position to continue to develop expertise in the evolving world of national security policing.

The second advantage is that the CPC's mandate extends beyond the RCMP's national security activities to all of its law enforcement activities. The risks associated with reviewing the RCMP's national security activities in isolation, including the possibility of jurisdictional disputes and accountability gaps, can therefore be avoided.

The third advantage is that the CPC already exists. Creating a new agency carries the risk of unintended consequences. I would be inclined to recommend an entirely new review mechanism only if I concluded that the CPC is irreparably broken.

That brings me to the disadvantages of using the CPC as the foundation for the new review mechanism. The first is that the CPC currently deals with only one aspect of the review function, complaints. In order for review in the national security field to be effective, it must include not only a complaints function, but also a self-initiated systemic review capability. The CPC would therefore have to be restructured to include such capability. I do not see any problem in this regard, as the review and complaints functions are complementary. SIRC and the CSE Commissioner handle both. Of course, the addition of this function to the review body would require a name change. I suggest that it be renamed the Independent Complaints and National Security Review Agency for the RCMP (ICRA), to reflect its broader role.

The second disadvantage is that, as currently constituted, the CPC has insufficient powers to effectively carry out a complaints and self-initiated review mandate in respect of the national security activities of the RCMP. This, of course, would be addressed by providing ICRA with the mandate and powers I discuss in recommendations 3 and 4.

The third disadvantage to basing a review mechanism on a restructured CPC is the one that causes me the most concern. It arises from the perceptions held by many that the RCMP and CPC have a dysfunctional relationship. Such perceptions are the result of a number of public disagreements in recent years between the CPC and the RCMP, including several recent court cases. Without commenting on the merits of either side of these disputes, I note that they have led to a lack of public confidence in the CPC that does not serve the objectives of a review mechanism. Public confidence is crucial, particularly in the field of national security where the requirements of secrecy place significant restraints on transparency.

Having said this, I am confident that the relationship between the RCMP and an independent review and complaints agency can be more constructive. What seems to lie at the core of the recent disputes between the RCMP and the CPC is a lack of clarity about the powers and objectives of the CPC. This is illustrated in both the Trial Division and Federal Court of Appeal reasons in *Royal Canadian Mounted Police Public Complaints Commission v. Attorney General of Canada*.[3]

My recommendations include substantial enhancement of the mandate and powers of the new review body when compared to those of the CPC.

Furthermore, the new review body's mandate and powers are to be clearly and unequivocally set out. In this way, there will be no reasonable basis for disputes that can damage the relationship between the review body and the RCMP. In any event, perfect harmony and agreement should not be expected between an independent and effective review body and the agency being reviewed. There should be a clear legal foundation for the rights and responsibilities of each, but some degree of creative tension is perhaps inevitable, given their respective mandates.

On balance, it is my view that the advantages associated with using the CPC as the foundation for a review and complaints agency are of a kind that will be difficult to duplicate in another agency, while the disadvantages can be overcome by restructuring the CPC and ensuring that the new body has sufficient powers to carry out its mandate.

2.3 Recommendation 3 (a)

ICRA's mandate should include authority to conduct self-initiated reviews with respect to the RCMP's national security activities, similar to those conducted by the Security Intelligence Review Committee (SIRC) with respect to CSIS, for compliance with law, policies, ministerial directives and international obligations and for standards of propriety expected in Canadian society.

In 1981, the McDonald Commission recommended that the government establish a limited self-initiated review of the RCMP's remaining national security activities. However, the government did not implement that proposal. When it created the CPC in 1988, it confined the CPC's authority to complaint investigations.

The case for giving an independent review body the mandate to conduct self-initiated reviews of the RCMP's national security activities is now overwhelming. In recent years, the RCMP has had to dramatically expand the number and extent of its national security investigations. Quite properly, given events, information sharing and integration with other domestic and foreign agencies have also increased. Moreover, the anti-terrorism legislation enacted at the end of 2001 has created both new terrorism offences and new investigative powers. These changes have led to an ever greater need to go beyond a complaints-based mechanism to one that includes self-initiated review.

I recognize that the RCMP's national security activities are those of a law enforcement agency and thus are different in many important respects from those of CSIS. Nevertheless, the reasons for creating a self-initiated review capacity

for the activities of CSIS apply in the main to the national security law enforcement activities of the RCMP. Common to both agencies are the need to maintain secrecy in many of the operations being reviewed, the inability of potential complainants to lay complaints, the threat that investigative activities may pose to individual liberties, the lack of judicial or other independent scrutiny, and the need for public confidence and trust in the agency being reviewed.

It is worth noting that in a November 2003 report, the Auditor General addressed, among other things, the level of review that exists in relation to the national security activities undertaken by the many federal agencies engaged in such activities. With respect to the CPC's review of RCMP national security activities, the Auditor General concluded that, because the CPC has no audit (self-initiated review) power, it "does not undertake reviews aimed at systematically determining compliance with the law, nor does its mandate provide for unrestricted access to all information."[4] She recommended that the government take steps to redress the gaps in civilian review of agencies with "intrusive powers."

It is also useful to note the types of review used in other countries. In Chapter VII, I describe in detail the systems for reviewing national security investigations conducted by security intelligence and law enforcement agencies in eight countries: Australia, Belgium, Germany, New Zealand, Norway, Sweden, the United Kingdom and the United States. The features and models vary widely, depending on the constitutional arrangements and institutional structure and cultures of the different countries, but all eight countries generally have independent review bodies that are primarily complaints-based for police forces and review bodies that are complaints-based, but also have a self-initiated review capacity, for security intelligence agencies. In all the countries except Germany, police forces involved in national security activities are subject to review by something more than a complaints-based body.

For example, national security policing in Belgium is conducted by divisions of the regular police, which fall under the complaint-processing and (self-initiated) review jurisdiction of a review body called "Committee P." In the United States, such policing is conducted largely by the FBI, which is subject to the complaints-processing, audit, inspection (or review) and investigation jurisdiction of the Inspector General of the Department of Justice. The Department of Homeland Security, which also engages in law enforcement activities related to national security through its agencies, including the Transportation Security Administration, U.S. Secret Service, U.S. Immigration and Customs Enforcement and U.S. Customs and Border Protection**,** is subject to similar review by the Inspector General of the Department of Homeland Security. Inspectors general

have self-initiated review powers for national security law enforcement investigations.

Police forces in England and Wales, which carry out national security policing to varying degrees, are subject to the complaint-processing jurisdiction of the Independent Police Complaints Commission (IPCC) and the Investigatory Powers Tribunal. In addition, certain covert activities conducted by police forces are subject to the inspection-based jurisdiction (self-initiated review) of the Interception of Communications Commissioner (ICC) and the Office of Surveillance Commissioners (OSC). The police are subject to these review and inspection powers relating to covert activities regardless of whether the investigation relates to national security or conventional law enforcement. Police forces in Northern Ireland and Scotland are also subject to review for certain specified covert activities. The Police Ombudsman for Northern Ireland has complaints-based jurisdiction over the Police Service of Northern Ireland.

2.3.1 Scope of National Security Activities Subject to Review

RCMP national security activities subject to review by ICRA should include the following:

(a) activities relating to the *Security Offences Act*;
(b) activities relating to the *Security of Information Act*;
(c) activities relating to Part II.1 of the *Criminal Code*[5] or relating to any other offence under the *Criminal Code* or other legislation, the investigation of which may relate to national security;
(d) any other activities undertaken to respond to threats to the security of Canada as defined in section 2 of the *Security Offences Act*, including activities pursuant to section 18 of the *RCMP Act* respecting duties of members who are peace officers;
(e) any activities carried out on an integrated basis with domestic or foreign agencies and related to national security;
(f) any other activities undertaken by personnel units or resources within the RCMP's national security organizational structure; and
(g) any other matter that ICRA deems necessary to examine in order to ascertain whether it relates to the RCMP's national security activities.

The concern here is to define national security activities for purposes of ICRA's self-initiated review process in a manner that is sufficiently broad to include all activities that have a national security aspect. ICRA's mandate and jurisdiction should make it clear that it may examine anything it deems advisable

to determine whether it relates to national security and should be reviewed. This includes activities relating to investigations of specified offences, including collateral offences, examined in part because of concerns that the person may be a threat to national security. For example, the investigation of fraud, theft or other *Criminal Code* or other offences by suspected terrorists would fall within the scope of matters to be reviewed as national security activities of the RCMP. In addition, the definition of national security activities should include all activities of RCMP personnel assigned to units or branches within the RCMP organizational structure that are responsible for conducting national security activities.

It is clear from my review of the RCMP's national security operations that the nature of some RCMP investigations may change over time. As I discuss earlier, an investigation may start out as a national security investigation, but, as information is gathered, be found to have no connection to national security. The opposite can also be true. Thus, it will be necessary to have a flexible approach when examining whether a particular investigation falls within the review body's mandate and to understand that the characterization of investigations may change as further information is obtained.

Two points are important to note concerning the characterization of investigations as national security or other investigations. The first is that, since ICRA would have the mandate to investigate and report on all types of complaints involving RCMP activities, the importance of the distinction between national security and other activities is greatly diminished. The ability to draw lines between national security and other activities would be of much more consequence if the model adopted involved different review bodies for complaints relating to the different types of activities.

That said, there are potential differences in the way ICRA would review national security and other complaints. Below, I recommend that, for investigations into complaints about the RCMP's national security activities, ICRA have investigative powers similar to those for public inquiries under the *Inquiries Act*. Such powers are much greater than those currently held by the CPC. Of course, if no further changes were made to its powers, ICRA would then have different powers for obtaining information depending on whether complaints related to the RCMP's national security or other activities. This could generate jurisdictional disputes and even litigation about whether a complaint related to the RCMP's national security activities or not. That would be a most undesirable situation. I therefore suggest that the power of ICRA to obtain information be made uniform for investigations of all complaints, whether related to national security or not.

My recommendation concerning a mandate to conduct self-initiated reviews relates only to the RCMP's national security activities. I am not recommending

that authority to conduct self-initiated reviews extend to matters not involving national security. This is not because I am opposed in principle to such reviews in other areas, but because I have assessed the need for them only in the context of the RCMP's national security activities. I do not consider that this difference in mandate based on the type of matters involved would have the same undesirable consequences as would a difference in the powers available to ICRA in investigating national security versus other complaints.

The result, however, is that the distinction between what is and what is not a national security activity assumes some importance. To avoid problems that might arise from the need to characterize RCMP activities, the mandate for self-initiated reviews should be interpreted broadly so that effective review is not curtailed by jurisdictional disputes. It is essential that ICRA be able to examine all RCMP activity and all documents under the control of the RCMP, as well as interview all regular and civilian members of the RCMP in order to determine whether any activity is related to national security and therefore within its mandate for self-initiated review purposes.

2.3.2 Specific Review Subjects

Unlike the investigation of complaints, self-initiated reviews would focus more on institutional or systemic practices, rather than on individual conduct or behaviour. Reviews would be directed at identifying problems of a structural nature or recurring practices that cause concern in national security investigations.

A good starting point for determining the specific types of matters to be reviewed would be to examine SIRC's experiences with reviewing the activities of CSIS over the past 20 years, making allowance for the RCMP's law enforcement mandate. Patterns of complaints could also be examined, as these may point to systemic problems that require special attention.

Without limiting the scope of the proposed reviews, I wish to draw attention to a number of matters that arose during the Factual Inquiry that I suggest be included in a list of what ICRA should examine from time to time:

- **Law Enforcement Mandate** – ICRA should review the RCMP's national security activities to ensure that they are properly within its law enforcement mandate. In my Factual Inquiry report, I emphasized the importance of confining RCMP investigations to the RCMP's statutory mandate, which is to investigate criminal or illegal activities for the purpose of prevention or prosecution.

- **Information Sharing** – National security investigations necessarily involve considerable information sharing. The RCMP currently has sound policies in this regard that, for example, require an assessment of the reliability and relevance of the information to be shared and the use of caveats to restrict and govern the use and further dissemination of the information. I made some recommendations for improvements to these policies in my Factual Inquiry report. What is critical, however, is that those involved in information sharing comply with the relevant policies. In the Factual Inquiry, I found that the RCMP repeatedly had not followed its own policies when sharing information with American agencies about the investigation involving Maher Arar. ICRA should ensure that the RCMP's policies are properly and routinely applied to all information sharing. The process should include regular reviews of information-sharing protocols and agreements with domestic and foreign agencies, organizations and governments.
- **Relations With Other Agencies** – The RCMP must interact with other agencies, both domestic and foreign, in conducting its national security activities. In the Factual Inquiry report, I recommended that those relationships be governed by a framework that is reduced to writing in order to avoid misunderstandings about what is expected in co-operative efforts among agencies. ICRA should ensure that co-operative efforts comply with the framework arrangements and, where appropriate, should make recommendations about the need to clarify or improve such arrangements.
- **Training Programs** – While national security investigators use regular law enforcement powers and techniques in conducting investigations, they do so in a context unfamiliar to most RCMP officers. In my Factual Inquiry report, I made recommendations concerning the content of training programs for national security investigations. ICRA should examine training programs from time to time to ensure that such programs are properly preparing investigators to address the many difficult issues that arise in the national security context.
- **Human Rights Issues** – In today's world, national security investigations are largely focused on the prevention of terrorism and often involve members of the Arab and Muslim communities. In the Factual Inquiry report, I recommended that the RCMP set down in writing its policy directing that investigations not be based on racial, ethnic or religious profiling. Moreover, it is important that all aspects of national security investigations pay appropriate attention to the human rights and interests of those who may be affected. In this regard, the principles of proportionality and fairness are important. ICRA will play an important role in examining RCMP

investigations to ensure that they conform to standards of propriety that the Canadian public accepts and expects.

- **Integration** – The RCMP's national security activities are increasingly integrated with those of other federal agencies, including CSIS. ICRA will play an important role in reviewing the propriety of the RCMP's interactions with other agencies. In Recommendation 11, I propose that the government legislate statutory gateways to link the independent bodies responsible for reviewing Canada's national security activities. It is very important that these statutory gateways operate so as to ensure integrated and coordinated review of national security activities that involve more than one federal entity. ICRA can play an important role in ensuring that the RCMP respects both the letter and spirit of the statutory gateway requirements. As discussed in Recommendation 12, the Chair of ICRA will be a member of INSRCC and, as such, will play an important role in ensuring that integrated operational activities are properly reviewed.
- **Communications With Foreign Countries When Canadians Are Detained** – In my Factual Inquiry report, I recommended a protocol governing how Canadian officials, including members of the RCMP, should proceed in circumstances where Canadians are being detained abroad in connection with terrorist-related investigations. Briefly, the protocol recommends that there be a consultative, cohesive approach among Canadian entities and that Foreign Affairs and International Trade Canada (DFAIT) take the lead in such matters. ICRA should review RCMP activities to ensure compliance with that approach.
- **Interaction With Countries With Poor Human Rights Records** – During the course of national security investigations, it will sometimes be necessary for RCMP investigators to receive information from, or provide information to, countries with poor human rights records. These situations raise special concerns. In the Factual Inquiry report, I made several recommendations for policies governing activities in this area. These recommendations were aimed at ensuring that there is no support or condonation of torture or other human rights abuses and that special care is taken to assess the reliability of any information the RCMP accepts from countries with poor human rights records. ICRA should ensure that RCMP investigations conform to RCMP policies governing these types of relationships.
- **Issues of Public Interest** – ICRA should have the ability to investigate and, if necessary, hold public hearings on matters of public interest and controversy involving the RCMP's national security activities that, if not examined by the review body, might undermine public confidence in the RCMP. In

both Belgium and Sweden, review bodies have initiated investigations of issues related to national security based on newspaper allegations, even though no complaint has been made. I think that this would be a valuable way for the agency to foster confidence in the RCMP. In this kind of investigation, ICRA should be able to hold hearings, issue subpoenas and use all of the other powers it is otherwise given.

2.3.3
Review for Efficacy

Some participants in the Inquiry suggested that, in addition to reviewing for conformity with the law and propriety, the review body for the RCMP's national security activities should review for efficiency and effectiveness. In other words, it has been suggested that a review body should assess RCMP activities to determine whether the force is competent and/or has the capacity to carry out its mandate effectively. Recent failures of intelligence relating to the decision by the United States to go to war in Iraq, and other failures highlighted by the National Commission on Terrorist Attacks Upon the United States (9/11 Commission) support arguments in favour of review for efficacy of national security actors.

I note, however, that the events giving rise to the creation of the 9/11 Commission were very different from those that led to this Inquiry, which has focused almost entirely on matters of propriety, not efficacy. As a result, I have not examined issues related to review for efficacy in any depth and am not in a position to make detailed recommendations about the form that such review should take. I have some reservations about locating review for propriety and review for efficacy in the same body, as it strikes me that the skill sets required for each are quite different. My conclusions that the status quo is inadequate and that there is a need for an arm's-length, independent review body for the national security activities of the RCMP are based solely on considerations relating to propriety. I have concluded that review of national security activities for propriety is required regardless of whether or not there is also review for efficacy.

That said, review for propriety will sometimes raise issues of efficacy, in the sense that competence and capacity will necessarily become issues in a review. For example, my Factual Inquiry report made clear how the lack of training of RCMP officers in the area of national security policing procedures may have been closely linked to the impropriety of their conduct.

A proportionality analysis relating to the propriety of certain activities may involve judgments about whether an activity that adversely affects a person's rights or interests is rationally connected with legitimate security objectives and

whether less drastic measures would be equally effective in fulfilling the RCMP's law enforcement and crime prevention mandate. In such cases, the review body should have the authority to investigate and report about efficacy, including issues of competence and capacity, and about whether other equally effective means exist for the RCMP to fulfill its mandate. Thus, while propriety should be the primary objective of the review body, issues of efficacy, particularly in terms of "lessons learned," will in some cases be a necessary or useful element of such review. ICRA should have the mandate to investigate and comment upon such issues.

2.4
Recommendation 3 (b)

ICRA's mandate should include authority to investigate and report on complaints with respect to the RCMP's national security activities made by individual complainants and by third-party groups or individuals.

ICRA should have a mandate to review a wide range of complaints pertaining to the RCMP's national security activities. Complaints about the conduct of RCMP members can provide an important window into national security work. Effective review of complaints should determine whether the Force's national security activities comply with relevant law, policies, ministerial directives, international obligations and standards of propriety, while at the same time ensuring that public confidence is maintained. Although review based on complaints is not in itself sufficient to ensure effective review of the RCMP's national security activities, hearing and monitoring complaints are a necessary and important part of effective review.

The body that has responsibility for self-initiated reviews should also handle the complaints process, in order to ensure integration and consistency between the two functions. Indeed, patterns of complaints regarding particular RCMP activities may trigger self-initiated review by the review body. One of the aims of this type of review will be to make recommendations to address areas that produce patterns of complaints. The complaint handling and self-initiated review functions of the review body should be complementary and mutually reinforcing.

2.4.1
Third-Party Complaints

Because of the secret nature of much national security policing, those directly affected by such policing may never learn of circumstances that might form

the basis of a complaint. Even if they become aware of grounds for a complaint, they may be reluctant to initiate one, for a variety of reasons. They may fear that friends, employers and the public will learn that they have been involved in some way in a national security investigation. The potential stigma caused by association with such an investigation may be severe and long-lasting. Although presumption of innocence is a fundamental legal principle, it is not always foremost in the minds of the public. Many people may not appreciate basic distinctions between a person being the subject of an investigation and a person being found guilty of some offence, let alone finer distinctions between being the subject of an investigation and being a person of interest to an investigation. In addition, people affected by national security investigations may not have sufficient trust in the police or the system for reviewing complaints against the police to be willing to bring a complaint. As the Canadian Arab Federation and Canadian Council on American-Islamic Relations stated in their Policy Review submissions, "[m]ost aggrieved communities do not report complaints for a variety of reasons: lack of knowledge, confidentiality, fear of reprisal, safe space issues and, for far too many, a social culture that discounts the value of reporting."[6]

It is therefore vitally important that groups and individuals not directly affected by RCMP actions, including public interest organizations, be able to make complaints with respect to the national security activities of the RCMP. Although there may be concerns that politically motivated "busybodies" will avail themselves of the opportunity to make third-party complaints that are little more than "fishing expeditions," I am not aware of any evidence of such abuses in relation to existing systems that permit complaints by third parties. I have also been informed of a concern that the complaint system could be used, either directly or through a third party, by persons legitimately the subject of a criminal investigation to gather information to impede that investigation. While this is a valid concern, the answer in my view does not lie in placing limits on who can make a complaint. Rather, a case-by-case approach should be adopted. As I discuss below, ICRA should have the power to dismiss complaints that are trivial, frivolous or vexatious, or made in bad faith; the ability to refuse to confirm or deny elements of a complaint; and discretion to delay the investigation of a complaint if immediate investigation would prejudice an ongoing criminal investigation or prosecution.

My recommendation that third parties be allowed to make complaints with respect to the RCMP's national security activities does not break new ground. The *RCMP Act* already grants "any member of the public . . . whether or not that member of the public is affected by the subject-matter of the complaint"[7] the

right to make complaints against any RCMP member or any other person employed under the Act. Moreover, I note that the power of those not directly affected to make third-party complaints against the RCMP has recently been exercised with respect to RCMP national security investigations and operations. The Canadian Civil Liberties Association asked the CPC to investigate a complaint relating to the RCMP's actions with respect to Maher Arar, and a third party made a complaint in relation to Operation Thread, an investigation that culminated in the arrest and detention of over 20 mostly Pakistani individuals in August 2003. I also note that the Honourable Patrick LeSage, former Chief Justice of the Ontario Superior Court of Justice, who recently conducted a review of the Ontario police complaints system, recommended that the Ontario police complaints systems be expanded to allow complaints by third parties on the basis of cogent evidence,[8] and the Ontario government has proposed amendments to adopt this recommendation.[9]

2.4.2 No Initiation of Complaints by Review Body

The *RCMP Act* allows the Chair of the CPC to initiate a complaint against an RCMP member or other person employed under the Act when satisfied that there are reasonable grounds to investigate the complaint.[10] The former Chair of the CPC, Shirley Heafey, used this power to initiate a complaint concerning the RCMP's actions in relation to Maher Arar. The CPC also has the power to initiate a public interest investigation without laying a formal or specific complaint. This approach has the advantage of avoiding the appearance that it endorses the validity of a self-initiated complaint. Given the broad review powers I recommend for ICRA, I am of the view that it is not necessary for it to have a specific complaint ability. ICRA may choose to initiate a review into a matter of public interest. In my view, to avoid any apprehension of bias, it is preferable for it to act pursuant to its review powers rather than by means of own-motion complaints.

2.4.3 No Evidentiary Threshold Needed for Complaints

The nature of national security policing will often mean that complainants, whether directly affected or not, will not have full information about police conduct related to the action of which they are complaining. For example, had Mr. Arar made a complaint against the RCMP, he would not have been in a position to know the full extent of the RCMP's actions in relation to his case. Nor would a third party, such as the Canadian Civil Liberties Association. Much

national security policing involves information gathering and sharing in secret. The role of different agencies may not be understood until extensive investigation is undertaken.

In view of these characteristics of national security policing, it would not be appropriate to require an evidentiary threshold for complaints. Subsequent investigation will often be necessary to flesh out the grounds for complaints. This in part underlies my recommendation that ICRA have the authority to initiate an investigation into specific events and hold public interest hearings where desirable.

My recommendation that no evidentiary threshold be imposed on complaints is also not a new idea. At present, the *RCMP Act* does not require an evidentiary threshold for complaints against the RCMP. However, the Act provides a means to deal with some complaints in a summary or informal manner. It contemplates both informal resolution of complaints and the dismissal of complaints on the grounds that they are trivial, frivolous or vexatious, or were made in bad faith. Below, I recommend that ICRA continue to have these powers.

Finally, in my view, ICRA should maintain its own complaints intake system. In Recommendation 12, I propose that INSRCC be mandated to receive complaints with respect to national security investigations. However, I also indicate that, after assessing complaints, INSRCC should direct them to the appropriate review body. I envision that ICRA will receive complaints both directly from the public and from INSRCC. In either case, ICRA will require an intake system to screen and review complaints.

Under Recommendation 5 below, I propose improvements to the way complaints are handled under the existing complaint process.

2.5
Recommendation 3 (c)

ICRA's mandate should include authority to conduct joint reviews or investigations with SIRC and the CSE Commissioner into integrated national security operations involving the RCMP.

The review body for the RCMP's national security activities should have sufficient powers to allow effective and thorough review of any integrated activities involving the RCMP. Given the importance of integrated and co-operative activities among Canada's national security actors, it is critical that a review mechanism have the ability to conduct reviews on an integrated basis. There is no mechanism with this ability at present. For example, given the relationship between the RCMP and CSIS and the interconnectivity of their activities, it would

be useful if the RCMP's review body and SIRC had the power to consider joint or co-operative reviews.

I look at the extent of the integration of the RCMP's national security activities with those of other agencies in chapters IV and V. Integrated operations often make eminent sense from a national security perspective, but they present a number of challenges for a review body. It is essential that a review body for the RCMP's national security activities have access to the information and evidence it considers necessary from agencies and individuals the RCMP co-operates with, either formally or informally, in conducting its national security activities. It is also essential that it be able to assess all national security activities under the control and direction of the RCMP, including the activities of Integrated National Security Enforcement Teams (INSETs) and other integrated units. If some of these activities were to be excluded on the grounds that they were carried out by personnel not formally or permanently members of the RCMP, review would be incomplete.

In some circumstances, the activities of a participant from another agency in an RCMP investigation may not be under the control and direction of the RCMP. For example, in INSETs, the role of CSIS personnel is different from that of police personnel, in that they do not participate directly in INSET criminal investigations. Nonetheless, the RCMP review body must be able to review their conduct to the extent that it relates to the activities of INSETs. The same is true of other personnel who interact with the RCMP in formally integrated units or less structured relationships.

Because some personnel in INSETs are from provincial agencies, the issue of constitutional jurisdiction also arises. In my view, there is no constitutional impediment to assessment by a federal review mechanism of the activities of provincial officials operating under the direction and control of the RCMP. National security policing is clearly an area over which the federal government has constitutional jurisdiction. The RCMP is a federal agency and its activities are within federal jurisdiction. Indeed, a provincial or municipal police officer could be compelled to provide information or documents under the broad powers, similar to the powers under the *Inquiries Act*, that I recommend for the RCMP's review body. That said, I do not find it necessary to go the next step and address the issue of whether the RCMP's review mechanism could compel a provincial actor to take action or impose discipline on an individual whose home agency is provincial. The review body I propose will have the authority to make findings and recommendations, but not to order discipline or other remedies.

Another issue related to integration that is critical to the objectives of a review body for the RCMP is the manner in which that body would interact with

the review mechanisms for other agencies involved in the integrated activities. Co-operative review for integrated activities is needed for three reasons: to avoid accountability gaps or matters "falling between the cracks," to promote consistency and coherence in the review of integrated activities by more than the one review body, and to provide complainants with a single location for making complaints about national security activities that may have been carried out by a number of different agencies subject to different review regimes.

I have been told that there is currently little integration between the RCMP's national security activities and those of the CSE. In anticipation that this situation might change, I feel it makes sense to provide for joint reviews and investigations with the CSE Commissioner as well.

In my rationales for recommendations 11 and 12 below, I set out further details regarding review of integrated activities.

2.6
Recommendation 3 (d)

ICRA's mandate should include authority to conduct reviews or investigations into the national security activities of the RCMP where the Minister of Public Safety so requests.

Ultimately, the Minister of Public Safety is responsible and accountable for the policy direction of the RCMP and must also ensure that RCMP investigations conform to law and standards of propriety. Under the *RCMP Act*, the Commissioner is subject to the direction of the Minister.[11] In accordance with this approach to accountability, which stresses ministerial responsibility for the RCMP and the Commissioner's responsibility for the control and management of the Force, I recommend that the review body submit its reports to both the Commissioner and the Minister. Given the Minister's ultimate responsibility for the activities of the RCMP, it makes sense that the Minister be able to direct ICRA to conduct reviews of or investigations into the Force's national security activities.

Under the *Canadian Security Intelligence Service Act* (*CSIS Act*), SIRC has a mandate to take action on request by the Minister:

> The Review Committee may, on request by the Minister or at any other time, furnish the Minister with a special report concerning any matter that relates to the performance of its duties and functions.[12]

I recommend a similar provision in respect of the review body for the RCMP's national security activities.

2.7
Recommendations 3 (e) and (f)

ICRA's mandate should include authority to:

(e) conduct reviews or investigations into the activities related to national security of one or more government departments, agencies, employees or contractors, where the Governor in Council so requests; and

(f) in exercising its mandate with respect to the matters in paragraphs (a) to (d) above, make recommendations to the Minister of Public Safety, and with respect to matters in paragraph (e), to make recommendations to the relevant Ministers.

ICRA should have the authority to investigate or review national security activities that take place wholly or in part outside the RCMP when so requested by the Governor in Council. There could be a number of reasons for such a request. Some government departments and agencies involved in national security activities are not subject to independent review. It may be that the government will consider that a particular event or series of events warrants independent investigation or review and that ICRA is best suited for the task, perhaps because of its special expertise in law enforcement matters. Power on the part of the Governor in Council to direct that ICRA conduct an investigation or review in such circumstances could be very useful in filling review gaps, potentially obviating the need for a public inquiry such as the one I have conducted, or ad hoc reviews in individual cases.

In Recommendation 9, I propose that the government extend independent review to the national security activities of certain other government entities. However, even after this has been accomplished, there will still be some gaps in the review of national security activities. The Governor in Council should have the option of directing ICRA to conduct an investigation or review in such circumstances. It may make sense as well for the government to enact another, similar provision pursuant to which SIRC may be directed to conduct an investigation or review of the national security activities of entities not within its mandate.

In general, I would expect that the Governor in Council would direct ICRA to investigate matters that would draw on its law enforcement expertise and SIRC to investigate those that draw on its expertise with respect to security intelligence and aspects of national security not related to law enforcement.

2.8
Recommendation 4 (a)

ICRA should have extensive investigative powers, similar to those for public inquiries under the *Inquiries Act*, to allow it to obtain the information and evidence it considers necessary to carry out thorough reviews and investigations; those powers should include the power to subpoena documents and compel testimony from the RCMP and any federal, provincial, municipal or private-sector entity or person.

2.8.1
Need for Extensive Powers

ICRA requires extensive investigative powers in order to fulfill its statutory mandate and engender public confidence and trust. The powers required to obtain information can be divided into two categories: power to access all information from within the RCMP that the review body considers necessary to fulfill its mandate, subject only to two minor exceptions, Cabinet confidences and, in some circumstances, solicitor-client privilege; and power to access information from sources outside the RCMP, including other federal, provincial or municipal agencies and the private sector. In both its self-initiated review and complaint investigation functions, ICRA must be able to "follow the trail" of information or evidence in order to obtain a complete picture of the RCMP's activities. Given the integrated nature of many of the RCMP's national security activities, the trail will sometimes lead to information outside the RCMP. ICRA should not be stymied by jurisdictional boundaries in its efforts to fully and thoroughly review the RCMP's activities.

Moreover, ICRA must be able to compel the production of documents or testimony at any stage of an investigation or review. While compelling individuals to provide information under oath may not be a means used in many circumstances, it is nonetheless essential that the power be available. ICRA alone should determine what is necessary or relevant for an investigation or review.

The powers for accessing information that I propose are broad. However, the issue of these extensive powers was thoroughly addressed in the submissions made during the Policy Review and it was accepted by everyone, including the RCMP, that the review body needs to have investigative powers that enable it to obtain the information necessary to fulfill its mandate.

In addition to the obvious advantage to having a uniform investigation system for all complaints against the RCMP, it makes sense that the review body

investigating complaints about activities not related to national security be able to obtain all information that is relevant and necessary to thoroughly investigate the complaints. The rationale behind my recommendation for enhanced powers of access to information for investigating complaints related to national security activities applies equally to other types of RCMP activities. In any event, I am concerned that it will be difficult in some cases to determine whether a complaint relates to national security or some other matter, and that the review body's investigations of complaints about the RCMP's national security activities could be compromised and delayed by jurisdictional disputes that can be avoided by extending its investigative powers to all complaints.

A review agency must have adequate powers to conduct thorough and effective reviews. In its submission to this Inquiry, the CPC was clear in stating that it did not have sufficient powers to effectively review the RCMP. In general terms, the most serious inadequacy is that it is not able to access all relevant information to carry out its mandate. Access to information is essential to effective review. The CPC has encountered difficulties in accessing information the disclosure of which could be injurious to international relations, national security or defence, as well as information covered by various evidentiary privileges. It has also been involved in several disputes with the RCMP about what evidence is necessary or relevant to its investigations. This has hampered or delayed investigations. Inability to obtain all of the relevant information in the national security context greatly diminishes the role of a review body.

The CPC moreover does not have statutory authority to obtain information from outside the RCMP. Given the enormous increase in integrated operations in the national security field, access to that type of information is vitally important for effective review of the RCMP's national security activities.

The deficiencies in the CPC's information-gathering powers are apparent when compared to those of other review bodies in the national security field, including the CSE Commissioner, the Privacy Commissioner and the Information Commissioner (discussed in detail in Chapter VI).

The powers applicable to public inquiries under the *Inquiries Act* provide a good model for the powers that ICRA should have. One of the primary purposes of a public inquiry is to assure the public that there will be an independent and thorough examination of the events in question. Thoroughness is seen as essential for restoring or maintaining public confidence. A public inquiry that is unable to access all of the necessary information will fall short in this respect.

The same is true in relation to the review of the RCMP's national security activities. The public will have confidence and trust in a process only if it is

satisfied that the process has been thorough. Broad powers to access information can also minimize the chance of disputes or even litigation between the review body and the RCMP that may delay the performance of vital review functions and undermine public confidence in the process.

As I mentioned above, the Auditor General noted in a November 2003 report that the CPC's mandate does not provide for unrestricted access to all information and recommended that the government take steps to redress this shortcoming.

The need for thoroughness applies to both self-initiated review and the investigation of and reporting on complaints. I therefore envision powers for an effective review body similar to those applicable to public inquiries under the *Inquiries Act*. ICRA should have access to all information it considers necessary to conduct a thorough review, subject only to two minor qualifications, which I discuss below.

2.8.2
Authority to Decide What Is Necessary

ICRA must have the authority to decide what information it requires for thorough review and to compel the RCMP and other institutions or individuals to produce any such information in their possession when requested. Of course, ICRA may not always know with certainty whether information is necessary (or relevant) until it has examined it. Thus, ICRA's requests for information should be granted and any disputes about relevance or the use to which information may be put should be addressed after the review body has had the opportunity to review the information. This will help ensure that relevant information is not withheld. It will also be necessary for those within the RCMP to co-operate and answer any queries. Public confidence and trust will be higher if the public is satisfied that ICRA has access to all information and personnel it deems necessary to conduct a thorough review.

A system that allows those with information requested by a review body to withhold such information on the basis that they do not consider it relevant to the review can lead to confrontations, extensive delays in review, unfortunate and costly litigation, loss of public confidence and, ultimately, ineffective review. In the past, there have been disputes between the RCMP and the CPC about what information the RCMP should produce. The RCMP has given various reasons for its resistance to producing the information. There is no advantage to revisiting those disputes here. The very fact of such disputes makes the point: if there is to be credible independent review, the RCMP cannot be the one

holding the key to evidence that may be necessary to the review process. I note that, in the case of the CSE Commissioner, who has the same powers I am recommending for ICRA, there is little opportunity for the CSE to resist disclosure of relevant information. The same should be true for the RCMP.

2.8.3 Confidential Information

The nature of national security investigations makes it inevitable that ICRA will require access to information that must be protected to safeguard Canada's national security interests. Public disclosure of secret or sensitive information, such as investigative techniques or the identity of sources, could harm Canada's national security and put individuals at risk. In addition, disclosure of information provided by foreign agencies on the understanding that it will not be disclosed could harm relationships with those agencies and inhibit international co-operation.

However, within the limits that I set out below, ICRA must have access to all relevant information and should not be refused information on the basis that it is secret or sensitive. The concomitant obligation is for ICRA to be subject to stringent non-disclosure requirements.

Full access to all information has worked well in the cases of SIRC and the CSE Commissioner. According to the information provided to me, neither of those review bodies has breached security obligations, and there has been no suggestion that international co-operation has been diminished because of their access to foreign-source information.

This Inquiry is another example of how a review body can protect the confidentiality of information. Although Commission staff had little previous experience in handling classified or sensitive information, we were able to receive and process an enormous amount of information subject to national security confidentiality concerns without breaching confidences. There is no reason a properly structured review body for the RCMP could not provide an absolute assurance of security of confidential and sensitive information.

2.8.4 Information From Outside the RCMP

As I note throughout this Report, the RCMP's national security activities are highly integrated with other federal, provincial and municipal agencies. The nature of integration ranges from involvement in units such as INSETs, where personnel from many agencies work together on national security activities, to

relationships that are less structured and exist, for example, for the purpose of information sharing.

Given the RCMP's level of integration and co-operation with other agencies, an effective review mechanism for its national security activities will require authority to go beyond the personnel and material resources under the control and direction of the Force. While the focus of the review mechanism should be the RCMP's activities, the review body must be able to follow the trail and access information from all of the institutions or individuals with whom the RCMP interacted in conducting its national security activities.

The Factual Inquiry provides a good example of the point I am making. My mandate directed me to investigate and report on the actions of Canadian officials as they related to Maher Arar. This included the actions of the RCMP and its officers. In order to properly investigate the RCMP's actions, it was essential that I have access to information and personnel from other federal agencies, including CSIS, Foreign Affairs and International Trade Canada (DFAIT), the Canada Border Services Agency (CBSA), and other provincial and municipal police forces. Given the integration and co-operation among these entities, I would not have been able to assess the RCMP's activities properly and thoroughly without information from the other sources. That information from outside the RCMP provided me with an understanding of the circumstances in which the RCMP had acted and, in several instances, shed direct light on the RCMP's actions.

In making these comments, I am not suggesting that the RCMP review body should assess the conduct of other agencies as the Factual Inquiry did. The review body should have the power to access information and personnel from other agencies solely for the purpose of assessing the conduct of the RCMP, including the adequacy of the procedures and understandings that govern the RCMP's necessary interaction with other agencies.

At the same time, information received from other agencies may in some cases reveal a need for a coordinated review involving another federal agency to evaluate the national security activities of both the RCMP and the other agency. Indeed, providing the review body for the RCMP's national security activities with access to information from other agencies with which the RCMP conducts integrated operations would be a major step in addressing some of the review problems that arise as a result of integrated operational activities. The RCMP review body would be able to assess the degree of integrated activity and the need for coordinated review with the review bodies for other agencies.

I note that the power to obtain information beyond that in the possession or control of the body being reviewed is a common feature of the international review bodies we have examined.

2.8.5 Exceptions to Access to Information

There should be two exceptions to ICRA's full access to information: Cabinet confidences as I describe them below and, in limited circumstances, information subject to solicitor-client privilege.

The reasons for excepting Cabinet confidences are well established. As Chief Justice McLachlin stated in *Babcock*:

> Those charged with the heavy responsibility of making government decisions must be free to discuss all aspects of the problems that come before them and to express all manner of views, without fear that what they read, say or act on will later be subject to public scrutiny. If Cabinet members' statements were subject to disclosure, Cabinet members might censor their words, consciously or unconsciously. They might shy away from stating unpopular positions, or from making comments that might be considered politically incorrect.
>
> . . . . The process of democratic governance works best when Cabinet members charged with government policy and decision-making are free to express themselves around the Cabinet table unreservedly.[13]

In order to withhold Cabinet confidences under the *Canada Evidence Act*, the Clerk of the Privy Council must determine whether information falls within the statutory definition provided in subsections 39(1) and (2) of the Act and must then consider whether the information in question should be protected, taking account of the competing interests in public disclosure and retaining confidentiality. The government may voluntarily disclose Cabinet confidences, but Cabinet confidence privilege may not in any ordinary sense be waived.[14]

The types of documents over which Cabinet confidence privilege may be claimed are defined by law. They include memoranda to Cabinet, discussion papers presenting background information, records of the decisions or deliberations of Cabinet, records of discussions between ministers relating to government decisions or policy, records created to brief ministers or that are the subject of communications between ministers, and draft legislation.[15]

ICRA should not, in my view, have the power to compel disclosure of records of discussions at Cabinet meetings or between ministers, nor should it be able to require the production of final memoranda delivered to Cabinet. ICRA will examine the activities and decisions of the RCMP. It would be

inappropriate for it to comment on the wisdom or propriety of decisions or deliberations of Canada's elected representatives. In any event, in most circumstances, information subject to Cabinet confidence privilege would not be particularly helpful for reviewing the RCMP's national security activities. Because of police independence, it is unlikely that the operational details of a national security investigation — those that a review body would want to review — would be included in material covered by Cabinet confidence. Cabinet confidence privilege should not prevent ICRA from accessing certain types of documents and information used as the basis for recommendations to Cabinet or Cabinet deliberations, such as documents or information used to create memoranda to Cabinet or Cabinet briefing documents; background material incorporated into briefing documents or discussion papers used during Cabinet deliberations; and documents or information discussed by ministers (but not the record, substance or outcome of the discussions).

ICRA will have access to ministerial directives that outline policies and procedures for national security investigations. It will moreover have a legitimate interest in assessing the accuracy of information the RCMP provides to the Minister for eventual discussion in Cabinet, since such information is part of the national security activities being reviewed. However, it will not have a legitimate interest with respect to the actual debate in Cabinet, as it will not and should not have the mandate to review national security decisions made by Cabinet.

I note that, in its 2004–2005 Annual Report, SIRC criticized the use of Cabinet confidence privilege in relation to the listing of terrorist groups under section 83.05 of the *Criminal Code*. It stated that it could not perform a complete review of the role of CSIS in the listing process, as it could not access the Security Intelligence Reports prepared by CSIS for Cabinet regarding organizations suggested for listing. The RCMP prepares Criminal Intelligence Reports to assist the Minister in making recommendations to Cabinet about the listing of individuals under section 83.05. It may be useful for the review body in respect of the RCMP's national security activities to have the ability to review the RCMP's reports to the Minister. In the rare instances where ICRA determines that access to documents actually submitted to Cabinet for deliberation is necessary to complete its investigation, the RCMP should be required to provide full records of the information submitted to the Minister for possible discussion in Cabinet. These records should not be designated Cabinet confidences.

I wish to emphasize that claims of Cabinet confidentiality may not be made merely to thwart review or gain advantage. The certificate claiming Cabinet confidence privilege may be scrutinized to ensure that the government representative has properly considered whether a document ought to be protected from

disclosure on this basis. Evidence may be presented on the question of whether the certificate was properly issued and government witnesses may be cross-examined on the information produced.[16]

The question of solicitor-client privilege is also somewhat complex. In my view, ICRA should have access to information covered by solicitor-client privilege if the communication in question took place as part of the decision-making process or series of events being investigated or reviewed. Accessing solicitor-client advice provided in this context will help ICRA make a thorough and accurate assessment of the RCMP's activities. This is of particular importance in the national security context, as the prior consent of an attorney general is required to lay charges for terrorism offences or offences under the *Security of Information Act*, as well as to exercise the new preventive arrest and investigative hearing powers. It is therefore important that ICRA have access to the legal advice given the RCMP about the exercise of such powers, not to second-guess or evaluate that advice, but to determine the propriety of the RCMP's actions in seeking and complying with the advice received. Legal advice plays such an important role in national security investigations that a review body unable to examine the legal advice received by the RCMP would have only a partial and, at times, distorted view of the Force's national security activities.

I caution, however, that ICRA should not have access to information subject to solicitor-client privilege that relates to any disputes concerning the exercise of the review body's powers or other proceedings intended to assess the RCMP's activities or the activities of individual officers or employees. In other words, ICRA should not have access to advice given to the RCMP, other institutions or individuals in connection with their individual interests as they relate to responding to a legal proceeding or to an investigation or review being conducted by ICRA itself. It is essential that the solicitor-client privilege apply in such circumstances. My recommendations regarding ICRA's power to access information from the RCMP are designed in part to limit disputes between the RCMP and ICRA. It is in respect of those hopefully very rare disputes that the RCMP will retain a legitimate right to claim solicitor-client privilege.

There is one final issue regarding limitations on access to information on which I wish to comment. It has been suggested to me that the review body should not have access to information that would be covered by police informer privilege, which protects the identity of those who come forward with information regarding alleged criminal activity unless the innocence of an accused is at stake. It is designed to ensure that informers can come forward without suffering reprisal. In most circumstances, information covered by this privilege,

such as the identity of a source, will not be relevant to a review. On the other hand, I can envisage very rare circumstances where such information might be relevant because, for example, the police may have obtained information from an unreliable informer. In such cases, it is important for ICRA to have access to the human source information while at the same time protecting the informer's identity from public exposure. I note that SIRC and the CSE Commissioner, as well as a number of international review bodies have access to human source information and identity in exceptional circumstances. These bodies may and do exercise their discretion not to request source information unless it is necessary for the purposes of review, but they are entitled to disclosure as a matter of law.

While it would not, in my view, be prudent to recognize police informer privilege as a limitation on ICRA's powers of access to information, it should be incumbent upon ICRA to exercise judgment about whether the information is relevant and, therefore, whether it is necessary to obtain access to it, given the sensitive nature of such information. Practices such as consistent use of code names for human sources will generally allow review bodies to review relevant issues without requiring access to the names of informers. Indeed, in documents examined in the Factual Inquiry, human source names had generally been replaced with consistent code names. My review of the relevant information was not impaired by this. In any event, it should never be necessary for ICRA to disclose the identity of a source in any of its reporting. ICRA must take every step necessary to protect the identity of sources.

2.9
Recommendation 4 (b)

ICRA should have the power to stay an investigation or review because it will interfere with an ongoing criminal investigation or prosecution.

Normally, ICRA will examine law enforcement activities after they have taken place. Because of the retrospective nature of ICRA's mandate, concerns about interference with police independence are significantly reduced. ICRA will not control or direct the operations of the RCMP. Nonetheless, the nature of national security policing suggests that many files may be kept open for extended periods and ICRA may have a legitimate interest in examining and commenting on law enforcement decisions or activities made by the RCMP in ongoing investigations. I note that many review bodies in other countries have the power to conduct investigations in parallel with criminal investigations. These include the Independent Police Complaints Commission in the United Kingdom, the Police Ombudsman for Northern Ireland, the Commonwealth Ombudsman in

Australia, and Committee P in Belgium. In Canada, one need only think of the Air India investigation to recognize that some national security investigations may remain open for long periods of time.

Conceptually, I see no problem with investigation or review of ongoing files by ICRA. However, ICRA should respect the principle of police independence that allows the police to make law enforcement decisions in an independent manner. It should also ensure that it does not disrupt or unduly interfere with criminal investigations and prosecutions. A review body has the potential to do this in a number of ways. For example, where a review body has powers of inquiry whereby it may compel testimony, issues may arise regarding fairness to individuals involved in any subsequent criminal or regulatory prosecutions. These include issues relating to the right to remain silent and the right to a fair trial under section 11(d) of the Charter. In addition, as I point out in Chapter IX, ICRA itself could become subject to disclosure obligations in a criminal prosecution. The Crown's obligations under *Stinchcombe* could extend to material in the hands of a review body. Disclosure obligations could include the products of the review body's own investigations, such as interview notes, witness statements, documents from other sources that were not in the possession of the RCMP or the Crown, and the review body's analysis. Potential disclosure obligations could have an impact on the criminal justice process. In addition, the review body could be placed in the chain of evidence. Specifically, if physical evidence relevant to a criminal proceeding is examined by a reviewer, such examination may have to be explained when the evidence is introduced in court.

I do not raise these potential effects to suggest that reviews should not take place during ongoing criminal investigations or prosecutions. As I suggest in Chapter IX, many potential disclosure problems can be managed by allowing the review body to provide copies of material that may fall under disclosure requirements to the Attorney General of Canada, who will be in a position to either make the required disclosure or assert any relevant privilege, including one relating to national security confidentiality. I note only that a review may have repercussions in respect of the criminal justice system and ICRA will need to eliminate or minimize unnecessary and undesirable impacts. One of the tools that should be available to it is the power to stay an investigation of a complaint or a self-initiated review.

2.10
Recommendation 4 (c)

ICRA should have the power to conduct public education programs and provide information concerning the review body's role and activities.

A public education function for ICRA is important in two main respects. First, public education should play an important role in engendering public trust and confidence in both ICRA and the RCMP. Given the necessarily secret world of national security activities, ICRA will act as a surrogate for the public in ensuring that the RCMP is accountable for its actions. This will only work if there is public trust in ICRA, and such trust can only be established if the public understands how the body works. Thus, it will be important for ICRA to educate the public about its processes and procedures. To some extent, this can be done in the reports it releases. Public education activities such as seminars and conferences may also be used.

I caution, however, that ICRA must remain sensitive to its critical function as an independent and unbiased body. The public education function should not be used as a platform to campaign for change within the RCMP. In its quasi-judicial role of reviewing complaints and even in its reports on the product of its self-initiated reviews, ICRA should generally allow any criticisms and recommendations to speak for themselves.

The second important role of a public education function is to foster better public understanding of and more comfort with the complaints process. In the course of this Inquiry, I heard on numerous occasions about reluctance to make complaints and even fear of doing so, particularly among new Canadians. I propose that ICRA engage in public education to publicize the complaints process and make it more readily accessible. Again, I caution that this public education must be neutral. ICRA may not use it, or be perceived to be using it, to "troll for business."

Moreover, public outreach should be a two way street, used by ICRA not only to educate the interested public about its activities, but also to learn about the public's concerns relating to its activities and those of the RCMP.

2.11
Recommendation 4 (d)

ICRA should have the power to engage in or to commission research on matters affecting the review body.

One of the features of national security activities that has emerged most clearly from this Inquiry is their ever-changing nature. As seen in chapters II through V, both the nature of the threats to Canada and the government's response to those threats are perpetually evolving. There is no reason to believe that this will not continue in the future and that the requirements for an effective review and complaints mechanism will not continue to change accordingly. New issues will arise concerning potential harm to Canadians from national security activities and new approaches will have to be developed to ensure that the RCMP is accountable for its actions.

If ICRA is to be effective, it will need to keep abreast of these changes and respond proactively to new challenges for effective review. It will be assisted in this regard by a research function. In its supplementary submissions to the Inquiry, the CPC pointed out that it had conducted research and gained expertise in regard to many matters involving the law affecting the RCMP, as well as the RCMP's policies, training and procedures.

Similarly, I have benefited enormously from the Inquiry's research into the approaches to review and oversight taken in other countries. In some cases, issues that are new to Canada have already been dealt with successfully elsewhere.

The importance of a research capacity will only increase with the recommended self-initiated reviews of the RCMP's national security activities. Research into the complex and specialized laws and procedures affecting national security will be essential to effectively use the new review powers.

The review body should also be open to receiving representations from the public concerning its operation and mandate, as well as areas that would benefit from research.

2.12
Recommendations 5 (a) and (b)

ICRA's complaints process should incorporate the following features:

(a) in the first instance, ability on the part of ICRA to refer a complaint to the RCMP for investigation or to investigate the complaint itself, if deemed appropriate;

(b) ability on the part of the complainant to request that ICRA review the complaint if the complainant is not satisfied with the RCMP's investigation and disposition of it.

I recommend that complaints be investigated by the RCMP at first instance, subject to ICRA's discretion to perform the initial investigation itself where it considers it necessary or in the public interest. This is similar to what occurs under the existing CPC complaint investigation model. I recognize, however, that the particular context of national security policing, including the centralized nature of such policing within the RCMP, and the need to maintain national security confidentiality may cause ICRA to exercise its discretion to investigate complaints itself more frequently than would be the case for other types of investigations. At times, it may also be more efficient in the national security context for ICRA to investigate a complaint from the outset.

It is common practice in most parts of Canada and elsewhere to have police forces conduct the initial investigation of public complaints, even when there is an independent civilian review body responsible for the complaints process. There are sound reasons for this practice. Complaints frequently involve misunderstandings between members of the public and the police, and quick resolution is often in the public interest. Moreover, complaints often involve matters of discipline, which are within the management prerogatives of the individual police forces. I do not recommend that ICRA be given the power to impose discipline. Although independent monitoring of the handling of complaints is appropriate, police management will most often be in a better position to impose discipline on officers.

The distinctions between review and oversight should be borne in mind. The fact of not having the power to issue directions or impose discipline on police officers will help the review body to achieve critical distance from the matters being reviewed. Once the review body makes its findings and recommendations, the RCMP will be required to justify its response to them and its decision to either discipline or not discipline individual officers.

The current process for handling complaints against the RCMP is quite sophisticated. It has a number of layers and structures that encourage discussion between complainants, the RCMP and the CPC. Initially, this process relies more on consensual resolution than authoritative decision making. The *RCMP Act* requires the Commissioner of the RCMP to consider whether a complaint can be disposed of informally, with the consent of the complainant. Where the complaint is not disposed of in this manner, the Commissioner must provide the complainant and affected members of the RCMP with interim reports and a final report setting out the results of the RCMP's own investigation of the complaint and the action that has or will be taken to resolve the complaint.[17]

A complainant who is not satisfied with the resolution of the complaint has the option of referring it to the CPC. If the Chair of the CPC is not satisfied with how the RCMP resolved the complaint, the Chair has several options, including requesting that the Commissioner of the RCMP conduct further investigation, having the CPC investigate further, instituting a hearing into the complaint, and preparing a report with findings and recommendations and sending it to the Minister and the Commissioner of the RCMP.[18] The Chair of the CPC also has the authority, where he or she considers it advisable in the public interest, to investigate or institute a hearing into a complaint, regardless of whether or not the complaint has been investigated, reported on or otherwise dealt with by the Force.[19]

In cases where the CPC sets out findings and recommendations in a report, the Commissioner of the RCMP is required to review the complaint and notify the Minister and Chair of the CPC of further action that will be taken or the reasons for not taking further action. Based on this response, the Chair of the CPC then provides a final report to the complainant, the Minister and the Commissioner.[20]

Although this structure is somewhat complex, I am satisfied that it provides a sound and flexible framework for the investigation and resolution of complaints. It allows the RCMP to handle the initial investigation of a complaint, but also enables the CPC to take action when it deems it necessary. It thus provides a system of checks and balances between the RCMP and the CPC, along with a flexible array of options in recognition that one process will not be appropriate for all complaints. The CPC appears to be satisfied that it has adequate options under the existing system, as it recommended in its Policy Review submissions that "the existing system be maintained such that all complaints are investigated by the RCMP at first instance, bearing in mind the CPC Chair's existing ability to perform the initial investigation where she considers it necessary in the public interest."[21] I also note that the existing process has considerable

force, in that the Commissioner is required to consider the CPC's findings and recommendations and then justify the decision to follow or depart from those findings and recommendations.

When asked to review a complaint, the chair of ICRA should have the option of dismissing the complaint, asking the RCMP to reinvestigate the complaint or reconsider its disposition, investigate the complaint itself, order a hearing into the complaint, or make its own report with findings and recommendations, to be sent to the Commissioner and Minister.

2.13
Recommendation 5 (c)

ICRA's complaints process should incorporate an ability on the part of ICRA to dismiss a complaint at any stage of an investigation as trivial, frivolous or vexatious, or made in bad faith.

I am not recommending that there be a threshold for receiving complaints or processing them through different stages of an investigation or review process. In my view, a more flexible approach is desirable, especially since a complainant will often not know the full extent of RCMP involvement in a national security investigation. However, it is essential that ICRA be able to screen out complaints without merit at any stage.

Periodically, ICRA should assess investigations of complaints to determine whether any complaints are frivolous or vexatious. Where it is apparent there is no need for investigation, the investigation should be discontinued and the complaint, dismissed. It is in the interest of no one, including the RCMP and the complainant, to have the investigation of a complaint continue past this point.

I note that, in his report concerning the police complaints system in Ontario, the Honourable Patrick LeSage recommended that a new independent civilian review body "review complaints to determine whether they should be pursued further and screen out those that do not reveal a reasonable basis for the complaint, those that may be more suitably addressed through another process or those that should otherwise not be subject to further action."[22] There is obvious merit to such a screening mechanism. My one concern relates to the fact that decisions about reasonable basis should be based on sufficient information, but the nature of the RCMP's national security activities means that such information may not be available until after significant investigation by ICRA. I do not propose to provide the detail of the process that should be followed when consideration is being given to dismissing a complaint because it is frivolous or without merit. I leave that to those responsible for implementing these recommendations.

2.14
Recommendation 5 (d)

ICRA's complaints process should incorporate the establishment of a program providing opportunities for the use of mediation and informal complaint resolution, except where the complainant does not have the information about the RCMP activities that are relevant to the complaint.

I recommend that there continue to be a process for the informal resolution of complaints. I also recommend that ICRA have the discretion to delay or bypass the use of such process where the circumstances of a national security investigation require it.

At present, the *RCMP Act* specifically contemplates the informal resolution of complaints with the agreement of the complainant.[23] The CPC has undertaken an alternative dispute initiative with a view to reducing the backlog of complaints. In its Annual Report for 2004–2005, it reported that alternative dispute resolution was attempted with respect to 502 cases, and 471 cases were successfully resolved.[24] Although I do not wish to diminish the importance or utility of a voluntary and consensual process of alternative dispute resolution with respect to the wide range of complaints made against the RCMP, I do express a note of caution about the use of such processes in complaints relating to national security activities. My concern relates to the fact that, in the national security context, complainants often may not have full information about police actions relating to them at the time they make their complaints. In such circumstances, it may be appropriate to delay alternative dispute resolution until after the complainant has the advantage of an investigation into the police activities. Alternative dispute resolution is a voluntary process that involves those who have an interest in reaching an agreement. It is important that complainants be fully informed about their treatment by the police before they agree to a settlement.

Further, because of national security confidentiality, a complainant may never be given all of the details of the relevant actions of the RCMP. Thus, depending on the nature of the information withheld, informal resolution may not be appropriate at any stage of a complaint investigation. Given the objective of ensuring RCMP accountability, where ICRA is aware of relevant information withheld from the complainant, it should have the discretion to take a complaint investigation to conclusion without resort to alternative dispute resolution initiatives.

2.15
Recommendations 5 (e) and (f)

ICRA's complaints process should incorporate:

(e) opportunity for the Commissioner of the RCMP and affected members of the RCMP to make representations to ICRA and, where a hearing is commenced, to present evidence and be heard personally or through counsel;
(f) opportunity for the complainant to make representations to ICRA and to present evidence and be heard personally or through counsel at a hearing.

It is important that the parties to a complaint have an opportunity to participate in the hearing of a complaint to the extent possible. The parties to a complaint should include the individual or group making the complaint, the RCMP members and employees who are the subject of the complaint, and the Commissioner of the RCMP. There will be circumstances, however, where the complainant's right to participate will of necessity be abrogated.

The existing system appropriately provides that complainants be notified of important decisions made with respect to their complaints. As I mention above, the Commissioner of the RCMP is required to inform the complainant of the results of the investigation and of any action that will be taken. In addition, the Commissioner is required to notify the complainant in writing where a decision is made not to investigate a complaint on the grounds that it should be dealt with by another federal mechanism; that it is trivial, frivolous or vexatious, or was made in bad faith; or that investigation is not necessary or reasonably practicable.[25] Further, the CPC is required to notify the complainant if it is satisfied with the Commissioner's disposition of a complaint, and to provide the complainant with a copy of its final report, including findings and recommendations, if it decides to conduct its own inquiries into a complaint.[26]

Where a hearing is held with respect to a complaint against the RCMP, the parties are given notice of the hearing, and they and any other person with a substantial and direct interest in the complaint have a right to be "afforded a full and ample opportunity, in person or by counsel, to cross-examine witnesses and to make representations in the hearing."[27] This represents a stronger set of procedural rights to participate than under the *CSIS Act*, which provides that the complainant, the deputy head and the director "shall be given an opportunity to make representations to the Review Committee, to present evidence and to be heard personally or by counsel, but no one is entitled as of right to be present during, to have access to or to comment on representations made to the Review Committee by any other person."[28]

Generally speaking, the provisions in the *RCMP Act* relating to hearings are preferable to those in the *CSIS Act* because of their recognition of a right of the complainant and other parties to cross-examine those who provide evidence. However, the provisions in the *CSIS Act* are based on recognition that the right of cross-examination cannot always be absolute in the national security context. In some cases, complainants are not allowed to participate because of national security confidentiality concerns. Below, I recommend that ICRA have the authority to appoint an independent, security-cleared counsel to assist with hearings when complainants are not able to participate.

2.16 Recommendation 5 (g)

ICRA's complaints process should incorporate open and transparent hearings of a complaint, to the extent possible, but authority for ICRA to conduct all or part of a hearing in private when it deems it necessary to protect national security confidentiality, ongoing police investigations or the identity and safety of sources.

Hearings into complaints should be open and transparent to the extent possible. Proceedings are improved by openness and adversarial cross-examination. Complainants not given the opportunity to cross-examine a person giving evidence may understandably feel that there has not been a fair hearing. Public confidence may also be eroded by so-called "secret hearings." Nonetheless, ICRA should have the authority to conduct all or part of a hearing in private when this is necessary to protect national security confidentiality, ongoing police investigations, or the identity and safety of sources.

As I discuss above, under the existing RCMP complaints process, most complaints are initially investigated by the RCMP. As with most police investigations, such investigations should be confidential. I note that the *CSIS Act* is more explicit in this regard, providing that "[e]very investigation of a complaint . . . by the Review Committee shall be conducted in private."[29]

In my view, investigations into complaints about the RCMP's national security activities, whether by the RCMP or the review body, should be conducted in private. This will work to protect both national security confidentiality and the privacy interests of the complainant. However, as I indicate below, complainants should generally be informed of the results of an investigation and be free to make such results public.

Although initial investigations of complaints should be conducted in private, hearings into complaints are a different matter. Such hearings are infrequent, as they are usually held only when there is a special public interest to a complaint.

Be that as it may, the general rule that hearings should be held in public should apply to such hearings, subject to specific and proportionate restrictions as required to protect national security confidentiality, ongoing investigations or proceedings, or the identity and safety of sources.

At present, hearings into complaints against RCMP officers are held in public. However, the CPC does have discretion to hold the hearing in private if the members of the CPC presiding at the hearing are of the opinion that information will be disclosed that "could reasonably be expected to be injurious to the defence of Canada or any state allied or associated with Canada or the detection, prevention or suppression of subversive or hostile activities," "could reasonably be expected to be injurious to law enforcement," or is information "respecting a person's financial or personal affairs where that person's interest or security outweighs the public's interest in the information."[30]

The above provisions of the Act should be revised and updated to conform more closely with both the requirements concerning national security confidentiality under the *Canada Evidence Act* and recent rulings on the importance of transparency in legal proceedings.[31] This will give those holding hearings the advantage of the considerable jurisprudence that has developed around these issues.

2.17
Recommendation 5 (h)

ICRA's complaints process should incorporate discretion by ICRA to appoint *security-cleared* counsel independent of the RCMP and the government to test the need for confidentiality in regard to certain information and to test the information that may not be disclosed to the complainant or the public.

Investigation of many complaints regarding national security investigations will require consideration of information that cannot be disclosed to the public or the complainant. In the event of a hearing, it will be necessary to exclude the complainant and his or her counsel for any portion that involves evidence that must be kept secret. Closed hearings raise three potential problems: the complainant who has a direct interest in the hearing is not able to participate and may understandably question the adequacy and fairness of the process; closed hearings may undermine the public trust and confidence in the process and outcome; and members of ICRA will not have the benefit of having evidence tested in an adversarial proceeding.

One mechanism sometimes used to address these problems is the appointment of an independent counsel with the necessary security clearance to

participate in the closed hearing and perform, at least partially, the role that would have been played by the complainant or other affected party excluded from all or a portion of the hearing. Although models for the use of independent counsel vary, an independent counsel typically does two things: tests the need for confidentiality of information and for a closed hearing in regard to all or some of the evidence, and tests the evidence called from the perspective of the affected parties who are excluded. Although such participation by independent counsel is not a complete substitute for the involvement of excluded parties, it provides a significant benefit to the process and is a useful compromise that can allow cross-examination and adversarial argument and inspire public confidence.

In the Factual Inquiry report, I commented on the important role that had been played by Commission counsel during the *in camera* hearings when Maher Arar and his counsel had been excluded, and also described the role played by Ronald Atkey and Gordon Cameron, the *amici curiae*, who had made submissions with respect to the government's claims regarding national security confidentiality. Together, Commission counsel and Messrs. Atkey and Cameron carried out the function of independent counsel. Commission counsel met with Mr. Arar and his counsel to seek their suggestions and views on the conduct of *in camera* hearings. I emphasize that Commission counsel were able to consult in this fashion even after reviewing confidential material, without disclosing such information to those without security clearance.

In the United Kingdom, there is a well-established program for appointing independent counsel, called special advocates, in a variety of proceedings in which evidence must be kept confidential. Although the proceedings covered by the special advocate process do not include police complaints, the experience in the United Kingdom is still instructive. The role of special advocate was first introduced in the United Kingdom by the *Special Immigration Appeals Commission Act 1997* (*SIAC Act*), which established the Special Immigration Appeals Commission (SIAC) to hear appeals by individuals against various immigration orders involving such matters as deportation, detention and refusal of admission. The *SIAC Act* and accompanying instruments provide for the appointment by the government of a special advocate to represent the appellant's interests where the government wishes to exclude the appellant and his or her legal representative from certain proceedings on the basis of the sensitivity of the information to be adduced. The Act followed a 1996 ruling[32] by the European Court of Human Rights that the United Kingdom's former procedure, which excluded the appellant and did not allow for sufficient testing of the

evidence, breached the *Convention for the Protection of Human Rights and Fundamental Freedoms*.[33]

Today, special advocates are used in numerous proceedings in the United Kingdom. They receive general instructions and support from the government and may consult with the affected parties before they receive confidential material. However, once they receive such material, they are prohibited from communicating with the affected parties without SIAC's consent, although they may still receive unsolicited information from those parties.[34]

In the "closed" portion of proceedings, special advocates' duties and powers in representing the interests of appellants and other relevant individuals in the proceedings are twofold:

- to test the claims made by the Home Secretary in support of non-disclosure of material (for example, to ascertain whether any possible or real harm could arise from disclosure, or whether the material in question is already in the public domain); and
- to represent the affected parties' interests in relation to those parts of the hearings held *in camera*. This entails making the best case possible from all the available evidence, both "open" and "closed" — but without informed instructions from the appellants and without the ability to call witnesses.

The use of special advocates in the United Kingdom has been subject to some criticism, including criticism of the role of the government in selecting advocates, the advocates' expertise and resources, restrictions on their ability to call evidence, and restrictions on their ability to communicate with the affected parties after they have received confidential information. All of these criticisms deserve consideration if the model is adapted to the Canadian context.

Nevertheless, I am convinced that independent counsel can play an important role in ensuring both adversarial challenge to claims of national security confidentiality and an appropriate testing of the evidence in closed hearings. The experience in the Factual Inquiry supports this conclusion and also suggests that, with caution and care, independent counsel can still communicate with an affected party after being exposed to material covered by national security confidentiality. Properly supported and resourced independent counsel can play a valuable role in relation to hearings of complaints about the national security activities of the RCMP.

ICRA should have the discretion to appoint independent counsel in those cases where it considers it to be a benefit. In making this recommendation, I recognize that ICRA may have its own counsel present during a hearing to present

evidence and, in such cases, that counsel may be able to fulfill the role of independent counsel in a satisfactory manner. Ultimately, the goal must be to provide a process that fosters confidence on the part of complainants and the public and that assists ICRA by ensuring that national security confidentiality claims and evidence called at hearings are properly tested.

2.18
Recommendation 5 (i)

ICRA's complaints process should incorporate the ability for ICRA to seek the opinions or comments of other accountability bodies, such as the Canadian Human Rights Commission, the Privacy Commissioner of Canada and the Information Commissioner of Canada.

As already mentioned, the RCMP is subject to review by several bodies, including the Canadian Human Rights Commission and the Privacy Commissioner. The jurisdiction of these two bodies in particular will overlap with that of ICRA. In some cases, it is in the public interest for review bodies to co-operate with each other and share their particular expertise. ICRA should not hesitate to seek outside opinions from other review bodies with special expertise that may be relevant to a complaint. Moreover, consistent with the need to allow the affected parties to participate as much as possible and the need to ensure that the process is as transparent as possible, ICRA should disclose any such assistance to the parties to the complaint and allow them to comment on the outside opinions provided.

ICRA should also have the power to retain independent experts to assist it in its work.

2.19
Recommendation 6

ICRA should be structured so that complaints and reviews related to the RCMP's national security activities are addressed only by specified members. Appointments of such members should be aimed at inspiring public confidence and trust in their judgment and experience. Appointees should be highly-regarded individuals with a stature similar to SIRC appointees.

The CPC as currently structured has the potential for 29 members. Typically, however, the government has made far fewer appointments. The large size of the CPC is designed to provide for provincial representation, because in all but two provinces (Ontario and Quebec), the RCMP provides law enforcement services.

A commission of 29 members would be extremely unwieldy and even impractical. However, the size and composition of the component of the review body that would deal with RCMP activities other than national security activities raise issues that are beyond my mandate and that I have not examined. Thus, my recommendation with respect to the composition of the RCMP's review body pertains only to those members who would have responsibility for reviewing national security activities and hearing complaints related to such activities.

Complaints and reviews related to the RCMP's national security activities should be addressed by specified members of ICRA. In my view, three to five members would be appropriate in this respect.

In making appointments, the credibility of ICRA is crucial. I recommend that appointees be highly-regarded individuals whose judgements would be broadly accepted. Individuals should have the stature of SIRC appointees. In addition, it is important that the Governor in Council consider individuals with knowledge and experience in the areas of policing, national security, human rights and freedoms, public law and multicultural communities, as well as a demonstrated commitment to public service. Taken collectively, the appointees should be of such a stature that the public will have confidence that they can serve as surrogate reviewers of those national security activities that cannot be disclosed to the public. This is a high threshold. However, it is essential that the government make appointments that foster confidence and trust in ICRA. In my view, there is merit in having the government consult with political party leaders before making appointments to ICRA, as it does for SIRC. In addition, I note that the Minister of Public Safety and the Minister of Justice have jointly established a Cross-Cultural Roundtable on Security to advise them with respect to national security issues that may emerge in a diverse and pluralistic society. To build confidence in ICRA, the government might wish to engage in a broad consultation about potential appointees with bodies such as the Roundtable.

It will obviously be necessary for the specified members to have the necessary security clearances to access all of the necessary information to effectively review the RCMP's national security activities.

Finally, if the government makes appointments to respond to the need for provincial and territorial representation on the review body for the RCMP, I do not think that it is necessary for those appointees to form part of the specified group responsible for reviewing the RCMP's national security activities. Matters relating to national security fall within the federal domain. Therefore, in my view, the rationale for provincial and territorial representation does not apply to the "national security" appointees.

2.20
Recommendation 7

ICRA should prepare the following reports to the Minister of Public Safety (the Minister) and the Commissioner of the RCMP:

(a) Reports arising from self-initiated reviews and investigations of complaints, which should include non-binding findings and recommendations.
(b) Annual reports on its operations to the Minister, who should lay an edited version of the report, omitting national security information, before each House of Parliament.

All of the above reports may include confidential information (including information subject to national security confidentiality) and should also include an edited version that ICRA proposes for public release.

ICRA should make reports arising from self-initiated reviews to the Minister and the Commissioner of the RCMP. The Minister is the appropriate government official to receive ICRA's reports, as he or she is responsible for the overall direction of the RCMP and is politically accountable for the propriety of the RCMP's activities. The Commissioner is also an appropriate recipient, given his or her management responsibility for the Force.

Such reports should include the results of the reviews conducted, as well as any recommendations for improvements. I would also expect that they would include the review body's strategy for conducting self-initiated reviews. SIRC's annual reports may serve as a useful model in this regard. ICRA's reports regarding self-initiated reviews should set out in detail the activities reviewed, the nature of potential difficulties, and its process and recommendations. It may be that some of the information contained in those reports will need to be kept confidential. In such cases, ICRA should indicate in its reports what portions are subject to confidentiality requirements.

With respect to investigations or hearings into complaints, I recommend the continuation of the current procedure, whereby the Commissioner makes an initial report about the complaint, subject to review by the review body, then the review body has the option of asking the RCMP to conduct further investigation, conducting further investigation itself, or commencing a hearing. Reports by ICRA should be non-binding, as is now the case with CPC reports, and the Commissioner should continue to be required to respond to those reports. In most cases, I would expect the Commissioner to agree with recommendations

made by ICRA. If, however, the Commissioner disagrees, then the Commissioner should be required to provide reasons to the Minister and ICRA.

At the present time, complaint reports are generally not made public by the CPC, except where the CPC determines that it is in the public interest to do so, subject to privacy concerns. However, complaint reports are subject to release under access to information legislation. I am of the view that complaint reports serve a public interest and public confidence function and should be made public, after editing for privacy and national security confidentiality concerns. Once it has given the Attorney General ten days to respond with respect to national security confidentiality issues under the *Canada Evidence Act*, ICRA should be able to publish complaint reports that have been edited to remove information subject to security confidentiality requirements and personal information (unless the subject of the personal information consents to release of that information). Publication of complaint reports should increase public trust and confidence in both ICRA and the RCMP.

2.20.1
Recommendation Powers

Several participants in the Policy Review suggested that the review and complaints body should have the power to make binding orders, such as orders for compensation, correction of files, and declarations that a complainant is not the subject of a national security investigation. In my view, giving the review body such power is not a good idea, as there is a risk of undermining the Commissioner's responsibility for the direction and control of the Force. It is clearly in the public interest that the complaints process be accepted within the RCMP. Giving ICRA the power to issue binding orders could provoke unnecessary resistance and opposition within the RCMP to the review and complaint process and could understandably thrust ICRA and the RCMP into an undesirable confrontational mode. Moreover, binding orders might ultimately impede ministerial accountability for the Force.

ICRA's power to issue non-binding reports should not be minimized. The fact of issuing a report, even one that is not binding, is a serious matter that will command attention from the head of the RCMP, the Commissioner. In addition, the fact that the Minister receives the non-binding report should affirm the importance of ministerial responsibility for the RCMP and add to the report's significance.

I note that the CPC, which has a long history of making recommendations, was not supportive of binding orders in its Policy Review submissions. It com-

mented as follows on the difference between the ability to offer recommendations and the making of binding orders:

> This represents the line of demarcation between review and oversight. An oversight mechanism that is capable of ordering the overseen body to do, or refrain from doing, something interferes with that body and undermines its accountability. By contrast, independence is preserved where the overseen body retains the ultimate right to decide if and how to act. Thus, the existence of the CPC as a recommendation-making body, even with enhanced powers, poses no threat to police independence.[35]

The complainant should generally be informed of both ICRA's recommendations and the Commissioner's reasons for accepting or diverging from them, where it is possible to do so without undermining national security confidentiality, interfering with ongoing police investigations or compromising sources and investigative methods. However, ICRA should be able to refuse to confirm or deny the existence of a complaint or any elements of a complaint where to do so would itself would result in a risk in any of these respects. The complainant has a clear interest in the outcome of a complaint and should be entitled to be informed of that outcome, subject to this exception.

A number of participants in the Policy Review indicated that the RCMP review body should have the power to recommend an award of compensation in cases involving national security. It was suggested that, in the absence of such a power, complainants may have nothing to gain by making a complaint and potentially something to lose in terms of time, adverse publicity or cost.

I am not inclined to recommend that ICRA be given this power. The expertise that I envision the review body will require does not include expertise for assessing damages or compensation. In my view, this proposal strays too far from the objectives of national security review identified above. Furthermore, doing so would create an anomalous situation, as only those making national security complaints would be potentially entitled to compensation. I think it best to maintain the status quo in this regard. Redress may be sought in the civil courts or from the Canadian Human Rights Commission, where appropriate.

2.20.2 Annual Reports

The *RCMP Act*[36] requires that the Chair of the CPC prepare and submit annual reports to the Minister outlining the activities of the CPC and making any recommendations. It also requires that the Minister cause a copy of the annual report to be laid before each House of Parliament. This reporting arrangement

appropriately places responsibility on the responsible minister and ensures that the legislature and the public are in an informed position to ask questions of that minister. Although the Act does not make provision for the Commissioner to receive a copy of the report, it would be advisable to have such a requirement embodied in the law in order to foster dialogue between ICRA and the Commissioner and ensure that the Commissioner is in a position to respond in an informed manner to any questions the Minister may have in relation to ICRA's reports and recommendations.

2.20.3
Transparency of Reports

Reports by ICRA will have to be edited to ensure national security confidentiality. The *CSIS Act* provides that SIRC is to consult with the Director of CSIS when preparing reports, to ensure respect for secrecy obligations.[37] Without question, such consultation is to be encouraged, and ICRA should similarly be required to consult with the Commissioner of the RCMP. At the same time, I am of the view that a more formal process is also required. This would include delivering an edited copy of the report to the Attorney General of Canada at the same time the report is submitted to the Minister of Public Safety and the Commissioner of the RCMP. Delivery of the edited report would constitute notice under section 38.01 of the *Canada Evidence Act* concerning the disclosure of sensitive or potentially injurious information, as defined in that act. The Attorney General would then have ten days[38] to inform ICRA and the Minister and Commissioner about his or her decision to allow or oppose disclosure of the report proposed by ICRA for public release.

I would expect that most, if not all, disputes about what can be released to the public would be resolved without litigation. Litigation is inevitably costly and lengthy and may undermine public confidence in the review body. One could well imagine that the public would lose confidence in a review body that was unable to comply with its statutory obligations to issue annual reports to the Minister (to be laid before Parliament) because of a dispute in Federal Court over claims of national security confidentiality. It is to be hoped that, in all cases, ICRA and the government will be able to agree to disclose as much information as is possible without jeopardizing ongoing investigations, sources and methods. Any temptation to make overly broad claims of national security confidentiality to prevent the release of information about embarrassing incidents should be resisted.

2.21 Recommendation 8

ICRA should have an adequate budget to fulfill its mandate in relation to the RCMP's national security activities, including for purposes of self-initiated review.

The above recommendations amount to a significant enhancement of the CPC. I have recommended a substantial increase in the review body's powers to obtain a wide range of information from the RCMP and have also recommended that it be given broad authority to conduct self-initiated reviews of the RCMP's national security activities. Implementation of these recommendations will require a transformation of the CPC from a body largely concerned with monitoring complaints to one with special responsibility for monitoring the RCMP's national security activities even in the absence of any complaint.

It will be important that ICRA members be given the training and expertise to fulfill the new mandate effectively. This may involve enhancing their national security and review expertise. In the short term, assistance may be required from people with experience in the review of national security activities at SIRC, the Office of the CSE Commissioner and the Office of the Inspector General of CSIS, for example. Secondments may even be required. I hasten to add that ICRA must develop its own unique expertise with respect to the review of national security policing, which is and should remain distinct from the review of security intelligence, given the RCMP's law enforcement and crime prevention mandate.

I would expect that ICRA's budget would be increased to account for its new responsibilities, should these recommendations be accepted. Even if all my recommendations were embraced in legislative reforms, they could be defeated by inadequate funding. Care should also be taken to ensure that additional resources are dedicated to the new responsibilities of ICRA and not diverted to other no doubt pressing needs within the CPC.

2.22 Recommendation 9

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.

2.22.1
Introduction

This recommendation flows from the mandate and the work of this Inquiry. My mandate directs that I make recommendations for an independent, arm's-length review mechanism for the RCMP's national security activities. It also directs that I make recommendations as to how that mechanism should interact with existing review mechanisms. My mandate is concerned with the relationship between agencies that review national security activities and, implicitly, with issues relating to the review of the national security activities of other entities when those activities are integrated[39] with those of the RCMP.

The importance of interaction among those reviewing the national security activities of the various federal agencies involved in the field is clear. It is apparent both from my research in the Policy Review and from the evidence I heard in the Factual Inquiry that integration of operations is a central feature of both the RCMP's approach to its national security mandate and the federal government's approach in general. In recent years, the government has increased emphasis on pursuing an integrated, broad and comprehensive national security policy. I have no doubt that integration of national security activities among the various federal entities involved is essential. The result, however, is that, increasingly, adequate review of the national security activities of one agency requires review of all the entities involved in the activities being reviewed.

The difficulty in this regard flows from the fact that many federal entities involved in national security activities have little or no independent review of the kind that exists for CSIS or the CSE, or the one that I am proposing for the RCMP. There is no federal ombudsman or review body that specializes in comprehensive review of the government's often secret national security activities. The review that is carried out is less extensive and very different in form. My concern is that, given the different types and levels of review, some independent and some not, some external and some not, there could be serious accountability gaps and incoherent or inconsistent results in the review of integrated activities. There is significant advantage to having the same or similar types of review for national security activities that are integrated, but conducted by different agencies.

I recognize that there are some independent review mechanisms within the federal arena that apply to all federal entities: the Canadian Human Rights Commission, the Privacy Commissioner, the Auditor General and the Information Commissioner. However, none have the broad mandate necessary to effectively and thoroughly review the national security activities of federal entities for

compliance with laws, policies and standards of propriety. These review mechanisms are focused on specific subject matters and do not provide the broad or overall accountability for national security activities that I consider necessary for the RCMP and the other five agencies and departments in question here.

If the interactions between ICRA and the review or accountability mechanisms for other national security entities are to be effective, it would be greatly beneficial to have the other entities reviewed by an independent review agency with powers similar to those of the review agency for the RCMP. Recommendation 11 concerns the enactment of statutory gateways among review agencies with respect to integrated national security activities. Such gateways are an effective and necessary means to review integrated activities. However, in cases where there is no independent review of an entity involved in national security activities, there is a risk that statutory gateways could be bridges to nowhere. The absence of independent review leaves open the potential for gaps in determining where accountability lies for integrated national security activities. In addition, different types of review mechanisms are more likely to apply inconsistent standards and obtain inconsistent results in relation to the same activities, including integrated activities involving the RCMP. Thus, to make recommendations for the effective review of RCMP national security activities that are integrated with the activities of other federal entities, it is very important to look at the review mechanisms for those other entities.

The need for effective independent review of the national security activities of federal entities other than those currently subject to independent review became a central issue in the Policy Review process. With the assistance of Policy Review legal counsel and the government, I did a survey of the national security activities presently carried out by over twenty separate federal agencies and departments. In Chapter V of this Report, I describe in some detail the mandates of those entities, their national security activities, and the amount of integration with the RCMP.

Throughout the Inquiry, there was a good deal of support for the extension of independent review to the national security activities of all federal national security actors not currently subject to such review. Many of the parties to the Inquiry suggested that I should recommend the creation of a "super agency" to conduct such review. In addition, during the public roundtables convened for this Inquiry, experts from Canada and abroad spoke of the need for independent review of the national security activities of a broad range of operational entities, not just the traditional law enforcement and security intelligence agencies currently subject to such review.[40]

Before final submissions were made in the Policy Review, the Inquiry sought comments on a range of options for addressing issues arising from the fact that many different federal entities are involved in the area of national security and the need for integrated or coordinated review. One of the options put forward for discussion, the "super agency," would extend independent review to all federal entities involved in national security activities. There was considerable discussion about the "super agency" model at the ensuing public hearings. No one, including the government, suggested that my recommendations should not address the issue of extending independent review to federal entities involved in national security activities other than the RCMP, if I considered it necessary to do so.

As a result of the Policy Review process and my observations during the Factual Inquiry, I have reached four conclusions with respect to the extension of independent review:

(i) The government should extend independent review to the national security activities of the CBSA, CIC, Transport Canada, FINTRAC and DFAIT.
(ii) ICRA is the most appropriate body to review the CBSA, given the latter's important law enforcement mandate.
(iii) SIRC is the most appropriate body to review the national security activities of the other four entities.
(iv) In five years' time, the government should appoint an independent person to conduct a review of the effectiveness of the review of the federal government's national security activities and to determine whether there are other federal government agencies or departments that, by virtue of their national security mandate, should also be subject to independent review.

2.22.2
Need for Independent Review

In general terms, I have two reasons for concluding that the government should extend independent review to the national security activities of the five entities mentioned above: the nature of their national security activities, which raise many of the same concerns that give rise to the need for independent review of the national security activities of the RCMP, CSIS and the CSE; and the degree of integration of the national security activities of each of the five entities with those of the other federal actors subject to independent review, including the RCMP.

Independent review is required to provide effective review of integrated activities, including integrated activities involving the RCMP. Without the

ability of an independent review body to make findings and recommendations about the five entities, there will be clear accountability gaps in the national security framework.

I provide a brief description of the national security activities of each of the five entities below. Greater detail is provided in Chapter V.

2.22.3 Canada Border Services Agency (CBSA)

The Canada Border Services Agency (CBSA) was created in December 2003. It has a mandate to manage the movement of goods and people into Canada and movement of goods out of Canada at all ports of entry. The RCMP is responsible for enforcing Canadian laws with respect to the flow of goods and people across Canada's borders between ports of entry. The role of the two agencies is thus highly complementary, as evidenced by the participation of both in Integrated Border Enforcement Teams (IBETs).[41] Similarly, the activities of the CBSA and CIC with respect to immigration issues are integrated with activities of both CSIS and the RCMP.

The branch of the CBSA that is most relevant to national security is the Enforcement Branch, which houses the CBSA's intelligence capability. It includes the Threat Analysis and Assessment Directorate, National Security Directorate and Border Intelligence Directorate. The Enforcement Branch also deals with immigration screening, fraudulent travel documents, investigations, detention, removals, counter-terrorism, counter-proliferation, strategic exports and contraband.

CIC and the CBSA share responsibility for administering Canadian immigration laws, which govern the movement of people into Canada and removal of non-citizens from Canada. Generally, the CBSA focuses on the security of Canada's borders and on threats and risks to the country. It prevents entry by people not legally allowed into Canada (inadmissible persons), collects intelligence, and detects, arrests, detains and removes people who are in Canada illegally.

The CBSA also enforces customs laws, which regulate the goods and currency that may enter Canada. This responsibility includes reporting certain cross-border financial transactions to FINTRAC and/or the RCMP. In enforcing customs laws, CBSA officers have the power to search individuals and baggage and seize certain goods, including currency. In addition, the CBSA has responsibility for enforcing restrictions on the export of strategic goods (goods that could be used to make sophisticated weaponry, etc.).

CBSA officers staff all points of entry into Canada, at which they screen people and goods and conduct interviews and secondary examinations that may involve issues of national security.

When performing their enforcement duties under customs and immigration legislation, CBSA officers generally have the same powers as police officers, including powers of arrest, detention, search and seizure. Under the *Customs Act*, CBSA officers may also take breath and blood samples. Under immigration laws, in defined circumstances, CBSA officers may issue arrest warrants and may detain and arrest without warrant. The CBSA has legal responsibility for immigration detention facilities, including the conditions of detention therein, even though Correctional Service Canada staffs the facilities.

The CBSA is also highly integrated into Canada's national security landscape. For instance, it works closely with CIC, the RCMP, CSIS and other Canadian and international agencies in its screening functions at points of entry. CBSA Intelligence is responsible for placing and maintaining "lookouts," electronic file records that flag or identify particular travellers or vehicles according to risk indicators or intelligence. Lookouts may relate to either customs or immigration issues, and they contain personal information. The information upon which lookouts are based is generally provided to the CBSA by other agencies, usually CSIS, the RCMP, the Department of National Defence (DND), the CSE or American law enforcement authorities. The CBSA participates in several multi-agency initiatives related to national security, including IBETs, INSETs and the Integrated Threat Assessment Centre (ITAC). The RCMP and the CBSA share responsibility for gathering criminal intelligence to assist investigations relating to cross-border national security issues. The CBSA screens travellers entering Canada for compliance with immigration and customs laws, and it maintains databases to assist in enforcement. It runs the National Risk Assessment Centre (NRAC), which receives and analyzes passenger information from airlines to identify individuals who pose security threats. This information may include any information in the air carrier's possession, such as frequent flyer history, emergency contact details, credit card billing information, addresses, email accounts and information about special health needs. NRAC shares Advance Passenger Information (API), including terrorism and serious crime-related lookouts, with the U.S. National Targeting Center. NRAC is the focal point for receiving terrorist watch-list information from the United States. It also receives and analyzes advance commercial information for risk and co-operates closely with U.S. authorities on cargo screening.

The CBSA plays a significant role in the security certificate process**.** It evaluates classified national security information, which may not be available to the person who is the subject of the certificate or to that person's counsel, and makes recommendations to the Minister of Citizenship and Immigration regarding the individual's participation in activities that would result in inadmissibility on grounds of national security or other grounds set out in the *Immigration and Refugee Protection Act*. The Minister considers these recommendations before signing the security certificate.

All of the reasons for recommending independent review of RCMP national security activities apply to the national security activities of the CBSA as well. As noted above, within the limits of its mandate, the CBSA often operates in a manner similar to that of a police force. There is a significant potential for the CBSA's activities to affect individual rights, dignity and well-being, and much of the national security activity undertaken is not disclosed to the public.

2.22.4
Citizenship and Immigration Canada (CIC)

Together with the CBSA, Citizenship and Immigration Canada (CIC) has responsibility for managing immigration and entry to Canada for non-citizens. It is involved in two principal types of national security activities: screening temporary visa, immigration and citizenship applicants and refugee claimants; and conducting pre-removal risk assessments and writing danger opinions, including in regard to persons subject to security certificates.

CIC, the CBSA, CSIS and the RCMP work closely together in the immigration and refugee screening process. If the CBSA is concerned that an individual may not be admissible to Canada, it places an electronic lookout in the immigration database shared by the CBSA and CIC. CIC officials who encounter a person regarding whom a lookout has been issued will gather more information about the person and transmit that information for further investigation either to CSIS, if there are concerns about threats to the security of Canada, or to the RCMP, in the case of concerns relating to serious or organized criminality or war crimes. If there are concerns, the results of the RCMP and CSIS investigations are reported, there may be CBSA involvement, and CIC makes the final decision with respect to admissibility.

CIC officials may interview non-citizens jointly with the RCMP and/or CSIS and receive advice and information from the CBSA, CSIS and the RCMP. Even where no suspicions about a foreign national arise, CIC is involved in interviewing individuals, gathering personal information and transmitting

that information to the RCMP and CSIS as part of routine criminality and security screening.

CIC officials also make decisions as to whether or not foreign nationals should be detained pending a determination of their admissibility to Canada.

In addition, CIC personnel are responsible for conducting pre-removal risk assessments for non-citizens ordered deported for reasons of national security or involvement in organized crime, war crimes or crimes against humanity, including persons subject to security certificates. As a result, CIC officials make decisions about whether individuals who pose serious threats to the security of Canada ought to be deported on the basis that such threats to Canada outweigh the risks they may face upon removal. Pre-removal risk assessments must be found to be reasonable by a Federal Court judge. Inadmissible persons are given the opportunity to make submissions, but may not have full access to information used by the CIC official to determine the threat posed to Canada.

CIC may share intelligence and personal information with the CBSA, CSIS, the RCMP, DFAIT and DND within Canada. It may also share information and intelligence with foreign governments and agencies. For example, it may share information with U.S. Customs and Border Protection authorities, who may in turn share the information with the FBI, the CIA and the U.S. Department of Defense.

In the national security context, there is significant interaction between CIC officials and the RCMP and CSIS. Indeed, CIC and the CBSA are building a common immigration database that will allow them to electronically transmit personal information, such as security or criminality screening information, directly to the RCMP and CSIS. RCMP immigration units will also have direct access to this database.

As with the CBSA, the national security activities of CIC require independent review because they can have a significant impact on individuals, and they lack transparency. While there is opportunity for judicial scrutiny of final decisions, this occurs on a case-by-case basis and under restricted conditions owing to both legislative provisions and secrecy concerns. There is no review of CIC's national security activities other than limited review by the Immigration and Refugee Board or the Federal Court in specific circumstances, and little opportunity for independent assessment of systemic issues.

2.22.5
Transport Canada

Transport Canada is responsible for safeguarding Canada's transportation system, which includes transportation by air, rail, road and water. It sets security standards for airports, surface transport, marine vessels, ports and marine facilities.

The department has an intelligence branch that regularly receives intelligence and transportation security information from CSIS, the CSE, DND, CIC, the CBSA, the RCMP, ITAC, the Canadian Coast Guard and other agencies. It analyzes information to identify threats to Canada's transportation infrastructure and may inform federal, provincial, municipal and private-sector transportation providers of credible national transport security threats.

Transport Canada also conducts security clearances for airport employees who require access to restricted or sensitive areas. It is in the process of developing a system of clearances for port and rail workers, as well as a background check program for truckers who transport dangerous goods across the Canada-U.S. border. The security clearance process may involve obtaining information related to national security from CSIS and the RCMP. Denial of a security clearance may mean termination or denial of employment.

The department also has an important marine security role, in the performance of which it shares information and co-operates closely with the CBSA, DND, the Coast Guard and the RCMP.

Transport Canada is also working in conjunction with Public Safety and Emergency Preparedness Canada to develop a Canadian no-fly list,[42] which will include the names of individuals the Minister of Transport believes pose "an immediate threat to aviation security." The development of this list will involve the exchange of information with a number of agencies, including the RCMP, CSIS and the CBSA.

For the purposes of transportation security, Transport Canada may request any information on airline passengers that is in the possession of the carrier, including personal information. The department may share this information with certain federal and, in some cases, foreign entities. It is also studying the feasibility of an air passenger risk assessment system. Further, legislation has been passed, though not proclaimed in force, that would allow significant sharing of airline passenger information by Transport Canada with CSIS and the RCMP.

In summary, Transport Canada is significantly involved in the collection, analysis and dissemination of information related to Canada's national security. Much of its work in this area takes place out of the public eye. In addition, its intelligence activities and activities related to national security are substantially integrated with those of other federal entities, particularly the RCMP and CSIS, as well as DND for maritime security matters.

Transport Canada's activities have the potential to affect individual rights, dignity and well-being to a significant extent. This is particularly so in the case of the security clearances it provides and the proposed creation of a no-fly list and passenger risk assessment program. Although the department has stated

that it will create internal reconsideration mechanisms, none of these activities are currently subject to independent scrutiny.

2.22.6
Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)

The Financial Transactions and Reports Analysis Centre (FINTRAC) collects, analyzes and discloses information on prescribed and suspicious financial transactions in Canada. Its main function is to support law enforcement and security intelligence investigations into terrorist financing and money laundering.

FINTRAC receives information from three main sources: Canadian federal government departments and agencies such as the CBSA, CSIS and the RCMP, foreign intelligence units, and private-sector reporting. Most of the information comes from private-sector reports.

In general, financial institutions are required to report on withdrawals or transfers involving more than $10,000, suspicious transactions, and property owned or controlled by or on behalf of a terrorist group included in the *Criminal Code* terrorist group listing. The CBSA is required to report on any cross-border movements of $10,000 or more in cash and monetary instruments.

FINTRAC analyzes data in order to identify patterns that suggest terrorist financing or money laundering activities. Where it has reasonable grounds to suspect that information is relevant to an investigation or prosecution of terrorist financing or money laundering activities, it must disclose that information to the RCMP or another police force. Where it has reasonable grounds to suspect that such information would be relevant to threats to the security of Canada, it must disclose it to CSIS. FINTRAC has information-sharing agreements with financial intelligence units in 30 foreign countries and may disclose information to those units for intelligence purposes relating to investigating money laundering, terrorist financing or substantially similar offences.

Presently, FINTRAC is permitted to disclose only certain designated information unless a judge orders further disclosure. It is required to keep records of its disclosures.

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.

2.22.7
Foreign Affairs and International Trade Canada (DFAIT)

Foreign Affairs and International Trade Canada (DFAIT) is responsible for the conduct of Canada's international relations. Among other things, it provides diplomatic and consular assistance to Canadians in foreign countries. It has responsibility for Canada's participation in and coordination with the anti-terrorism efforts of international organizations such as the United Nations and NATO. DFAIT plays the lead role in the listing of terrorist individuals, groups and organizations under the *United Nations Suppression of Terrorism Regulations* and *United Nations Afghanistan Regulations*.[43] The Security and Intelligence Bureau's Foreign Intelligence Division (ISI) provides intelligence to support operational and policy decision making and handles incidents abroad involving Canadian citizens.

DFAIT plays a significant role in Canada's national security operations. The department receives and analyzes intelligence relating to Canada's national security and disseminates it to other federal intelligence partners, principally CSIS, the CSE, DND, the RCMP and PCO and also, occasionally, others, including the CBSA, CIC and Transport Canada. The Factual Inquiry provided excellent insight into DFAIT's operations in the national security milieu. The department was involved with the RCMP and CSIS in making decisions about a visit to Syria by CSIS officials to meet with officials of the Syrian Military Intelligence (SMI), the body that had imprisoned Maher Arar. It was also involved in receiving and distributing the summary of a statement that Mr. Arar had given the Syrian officials. Foreign Affairs was moreover consulted by the RCMP regarding a decision to provide Syrian officials with questions for Abdullah Almalki, and it was centrally involved in Canada's efforts to obtain Mr. Arar's release from prison in Syria. It met and attempted to coordinate approaches with both the RCMP and CSIS.

The RCMP and DFAIT have secondment arrangements and significant information exchanges, which I discuss in Chapter V.

Implementation of my recommendations in the Factual Inquiry report would mean that DFAIT would play a lead role for Canada in addressing the situation of Canadians detained abroad in connection with terrorism and related matters. In that role, DFAIT would necessarily interact with Canadian investigative agencies in relation to their national security investigations. I note that other Canadian citizens detained in Syria in terrorism-related cases, such as Abdullah Almalki and Ahmad El Maati, have also complained of the involvement of Canadian officials abroad.

If DFAIT takes the lead any time a Canadian is detained abroad for a terrorism-related offence and its actions affect citizens or permanent residents, I am of the view that the actions of DFAIT employees should be subject to independent review. It should be borne in mind that the actions of Canadian representatives abroad are particularly difficult to review through Canadian courts, even though they are clearly subject to the *Canadian Charter of Rights and Freedoms*.[44] In making this recommendation for review of the actions of DFAIT employees and officials relating to national security, I recognize that the boundaries of review will have to be defined clearly, since some aspects of Crown prerogative should not be the subject of review.

At present, DFAIT's national security activities are subject to only limited independent review. Most of the concerns arguing for independent review of the RCMP's national security activities also apply to DFAIT's national security activities. Many of those activities have a significant impact upon individual rights and freedoms. As illustrated in the Factual Inquiry, many are not known publicly, and individuals affected may, in the ordinary course, never learn of the action taken. Moreover, DFAIT national security activities are highly integrated with those of the RCMP and other federal entities.

2.22.8
Rationale for Independent Review

It may be useful here to take a closer look at the two main reasons for my recommendation of independent review for these five departments and agencies: the nature of their national security activities and the degree of integration with other federal entities involved in national security activities.

2.22.8.1
Nature of Entities' National Security Activities

As is clear from the brief descriptions above, the nature of the national security activities of the five departments and agencies raises many of the same

concerns that give rise to the need for independent review of the national security activities of the RCMP, CSIS and the CSE.

Those concerns may be loosely grouped under three headings: potential for serious impact upon the lives of individuals, lack of transparency, and likelihood that they will not otherwise be subject to independent assessment.

Impact on Lives of Individuals

The potential to seriously affect the lives of individuals is shared by all of the departments and agencies described above. The police powers of the CBSA allow it to use intrusive methods, such as arrest, detention, search or seizure that are very much like those used by the RCMP. While the other entities do not have police powers, they have other powers that can harm individuals. These include powers to refuse entry into Canada or to deport from Canada on national security grounds (CIC and the CBSA), powers to restrict access to modes of transportation and employment on national security grounds (Transport Canada and the CBSA), powers relating to the treatment of Canadians by foreign governments in cases of national security (DFAIT) and powers to intrusively compel the disclosure of intimate financial information and provide such information to law enforcement, security and immigration authorities on grounds of national security (FINTRAC). These entities also all have the power that flows from the receipt and sharing of information about individuals in the context of national security. The collection, analysis, retention and dissemination of information can intrude in significant ways on privacy and other rights. For instance, the stigma suffered by an individual who is linked inappropriately or improperly to terrorism may be enormous. When that information is shared with agencies such as the RCMP, the CBSA or CSIS, it can have further intrusive impacts.

I have identified three particular features of RCMP national security activities that are of concern in terms of potential impact on individuals: information-sharing practices, interaction with other countries and the possibility of racial, ethnic and religious profiling. The five departments and agencies under discussion here share those features. They are important partners with the RCMP and other domestic and international actors in the information-sharing process related to national security. Consequently, concerns respecting the need to ensure that information is reliable, precise and accurate and that sharing is conducted in accordance with rules and policies so as not to impinge unfairly on the rights of individuals also apply to each of the five entities. Moreover, all of them may receive information from other countries, particularly the United States, and all have the power to provide information directly to agencies in

other countries and/or international organizations, depending on the statutory mandate. The risks associated with the possibility of discriminatory profiling identified in connection with RCMP national security activities arise primarily as a result of the nature of the current primary threats to national security. As such, they are not restricted to the RCMP and apply to other national security actors as well.

Lack of Transparency

Another critical factor underlying my recommendation for independent review of RCMP national security activities, the lack of transparency that accompanies those activities, is also shared by the other five agencies and departments. National security activities generally are characterized by requirements of secrecy, and secrecy means that public scrutiny of activities is seriously curtailed. It also means that individuals may never be made aware of the impact of an action on their lives. Review thus cannot rely upon the laying of complaints.

Lack of Independent Assessment

While all of the departments and agencies in question have internal policies and audit branches and are subject to ministerial direction and control, there is no comprehensive independent review of their national security activities.

Similarly, there is little judicial scrutiny of many of the decisions they make. While some of their activities are reviewed by the courts in criminal, immigration/refugee or administrative contexts, the courts cannot be expected to provide an assessment of the broad range of national security activities that impact upon individual rights or interests, including dignity, reputation and well-being. Judicial scrutiny generally only provides for a relatively narrow review of issues, restricted by the scope of activities raised in the particular case before the court. The courts are not ideally suited to provide broad systemic reviews of the activities of an organization. Courts are also constrained by the requirements of secrecy inherent in national security activities, which place significant restraints on the normal adversarial process.

There are also constraints on the other forms of independent review to which these agencies and departments are subject. Currently, such review, if it exists at all, is limited to review by entities such as the Office of the Auditor General and the Privacy Commissioner, whose role is not to provide reviews of national security activities for all aspects of lawfulness or propriety. While the Privacy Commissioner and Canadian Human Rights Commission may review for lawfulness, they do so within a very restricted statutory mandate.

2.22.8.2

Integrated Activity

The second reason I recommend that the national security activities of the CBSA, CIC, Transport Canada, FINTRAC and DFAIT be subject to independent review is that those activities are integrated to a considerable extent with those of the RCMP and CSIS. Including them in a regime of independent review will promote effective review of integrated activities by avoiding accountability gaps and inconsistent review standards and outcomes for the same integrated activities. In recommendations 1, 2, 11 and 12, I discuss the importance of integrated review of integrated operations. I will not repeat that discussion here, other than to point out that the reasons that underlie my recommendation for integrated review of the RCMP's national security activities apply in the main to the five entities in question in this recommendation. The amount of integrated activity of each is now sufficiently large for there to be a benefit to putting in place review mechanisms that facilitate integrated review. In my view, that can best be accomplished by subjecting each of the five entities to the same type of review mechanism as is currently available for CSIS and the CSE and as will be available for the RCMP if my recommendations are adopted.

It is precisely because the CBSA, CIC, Transport Canada, FINTRAC and DFAIT have the power to significantly affect the lives and rights of individuals, because their national security activities are not transparent, and because their activities are integrated with both CSIS and the RCMP, that the question of accountability is so important. Unless an independent, national security review body has the ability to make findings and recommendations about these agencies, the goals of national security review will be compromised. These are the five federal entities other than CSIS, the RCMP and the CSE whose national security activities have the greatest potential to intrude on the lives of individuals and that, accordingly, require the greatest degree of accountability.

SIRC and the CSE Commissioner were created as independent review agencies for CSIS and the CSE because of the same types of concerns. In her November 2003 report that I have described previously, the Auditor General addressed this issue in the following recommendation:

> The government should assess the level of review and reporting to Parliament for security and intelligence agencies to ensure that agencies exercising intrusive powers are subject to levels of external review and disclosure proportionate to the level of intrusion."[45]

The Privy Council Office's response to the recommendation read in part as follows:

> Any consideration of review mechanisms and reporting requirements must adequately consider the very important and, in some cases, fundamental differences in mandates and operations of departments and agencies."[46]

I have considered the mandates and operations of these departments and agencies and, for the reasons set out above, am satisfied that independent review is warranted in each case.

The Government of Canada is aware of the expanding nature of its national security activities and the need for review mechanisms to evolve to match. In its 2004 National Security Policy, the government recognized the general principle that "[a]s the legal authorities and activities of our security and intelligence agencies evolve to respond to the current and future security environment, it is vitally important that we ensure that review mechanisms keep pace."[47]

The government further indicated that it "will monitor progress in relation to enhanced intelligence collection and assessment as well as development and implementation of expanded review mechanisms relating to national security."[48]

The growth and integration of intelligence and information collection, assessment and dissemination by the five agencies and departments identified lead me to recommend their inclusion in an expanded national security review framework.

2.23
Recommendation 10

ICRA should review the national security activities of the Canada Border Services Agency, and the Security Intelligence Review Committee should review the national security activities of the other four entities.

2.23.1
Expanded SIRC

Having concluded that there is a need for an independent review mechanism for the national security activities of the five entities identified, I now turn to the issue of what bodies should perform such review. I have come to the conclusion that the national security activities of CIC, Transport Canada, FINTRAC and DFAIT should be reviewed by SIRC.

Limiting the number of independent review mechanisms for federal entities engaged in national security is a sensible approach. There is benefit

in restricting the number of organizations involved in the review of national security activities, given the sensitive nature of the information and activities, the special obligations that attach to review of such activities, and the necessity of retaining the confidence of foreign information-sharing partners. Moreover, it does not make sense and is not necessary to have a separate review agency for every operational entity. Such a situation would be unwieldy and could render the provisions for integrated or coordinated review unworkable. In addition, the national security activities of these other agencies and departments are relatively limited. A separate review mechanism for each would not be cost-effective.

SIRC is an established review agency with significant experience in the review of national security activities. It commands respect within the national security field. There is significant advantage to building upon its expertise and success rather than establishing a new review agency or agencies for other operational entities in the national security field.

When consideration was being given to where to locate the review mechanism for the national security activities of the RCMP, a number of participants in the Policy Review process suggested SIRC. The latter's experience and reputation made it a serious option. However, I chose not to recommend SIRC for review of the RCMP for reasons that centered around the RCMP's role as a law enforcement agency. I concluded that there is a real danger in blurring the important distinctions highlighted by the McDonald Commission between a law enforcement and a security intelligence agency, and that combined review could contribute to such blurring. My recommendation is also based on the critical need for law enforcement experience and expertise on the part of those reviewing law enforcement activities in the area of national security. These same considerations do not apply to CIC, FINTRAC or DFAIT for the obvious reason that they are not law enforcement agencies. And while Transport Canada has some enforcement functions in relation to transport safety and security, I am satisfied that its national security intelligence function is not oriented toward law enforcement.

The second reason for recommending that SIRC review the national security activities of these four entities is that, while there are important distinctions between the mandate and activities of CSIS on the one hand, and the national security activities of the four entities on the other, there are also important similarities. The national security activities of all four entities involve the collection, analysis, retention and dissemination of information and intelligence, including personal information, to varying extents. All four entities are involved in the collection of information, which is then analyzed or processed. Although CIC has

no independent intelligence analysis capability, it collects intelligence and raw information and receives intelligence analysis from other entities, such as the RCMP, the CBSA and CSIS. All four entities retain such information and intelligence and all are involved in the dissemination of such information to both domestic and foreign recipients. These functions are all similar to those that SIRC examines in connection with CSIS.

I am not downplaying the considerable differences in mandate among the entities. The review mechanism will have to take the different roles and mandates into account and apply different standards to assess conduct. However, my conclusion is that SIRC's expertise provides an excellent foundation on which to build an effective review mechanism for these bodies. SIRC will have to develop expertise with respect to their mandates and specific national security activities.

Concern was raised both by SIRC and other participants in this Policy Review that combining review of more than one national security actor within the same review body creates a risk of cross-contamination, in the sense that the "need to know" principle may be violated, wittingly or unwittingly, when information from one actor is taken and shared with another through the review body itself. This is also a risk at the operational level.

I think it is important to bear in mind that SIRC is well aware of the importance of placing safeguards upon information to ensure that it is communicated only to those who have a need to know in the course of an activity. As I cautioned in the Factual Inquiry report, we are moving into a world where "need to know" and "need to share" with respect to national security and intelligence information cannot simply be invoked. The *relevance* of information to any particular activity and the *purpose* of sharing or restricting information must be the overarching considerations. As the operational agencies work out limits in this regard, so, too, can the review bodies. I expect that SIRC will set up the appropriate "firewalls" — that it will have separate investigative staff to deal with the different departments and, in the case of integrated activities, will be mindful of the information coming from one organization or another. It will have the unique ability, however, to review trends and practices amongst a variety of security intelligence actors. In my view, such review can only strengthen the quality of the federal national security actors. The adverse consequences of potential cross-contamination might be greater if one review body were to examine both law enforcement and security intelligence activities, given the different legal and constitutional standards that apply to matters such as obtaining private information and warrants. My recommendations lessen this risk by confining review

of law enforcement agencies to ICRA and review of security intelligence bodies to SIRC.

There is a legitimate concern that expanding SIRC's mandate as I recommend might interfere with SIRC's capacity to effectively review the activities of CSIS. Below, I recommend that a review be conducted in five years' time. That review should specifically address how SIRC is managing its increased responsibilities. It will provide an opportunity to examine SIRC's capacity to handle the expanded mandate recommended in this Report and also determine whether that expanded mandate is affecting its ability to conduct the effective review of CSIS.

2.23.2
Review of CBSA

As I noted above, in certain situations CBSA officers have powers similar to those of a police officer, including the power to detain, arrest and search individuals. A CBSA immigration officer may issue an arrest warrant for a permanent resident or a foreigner if the officer suspects the person poses a threat to the public or is in Canada illegally. Foreign nationals other than refugees may also be arrested and detained by CBSA officers without a warrant, on the same grounds. At border posts, CBSA officers may detain foreigners and permanent residents for further questioning if they suspect that an individual poses a national security risk. There are also search and seizure powers in the customs area.

Since the CBSA has some law enforcement powers, the question arises as to whether SIRC is the appropriate body to review its national security activities. Above, I conclude that one of the compelling reasons for the need for a review body for the RCMP other than SIRC is the need for that body to have specialized expertise in reviewing law enforcement activities. Thus, there is an argument that the national security activities of the CBSA would also be most effectively reviewed by a review body with special expertise in reviewing law enforcement activities. The separate review body for the RCMP immediately comes to mind.

I note that, in the United Kingdom, the Independent Police Complaints Commission was recently given jurisdiction to investigate complaints in respect of the law enforcement activities of agencies other than the police, including the UK Customs service, and jurisdiction over immigration enforcement activities is expected to follow shortly.

There are differences between the CBSA and the RCMP, however. The CBSA is not a police force and not all of its officers have police powers. Unlike

the RCMP, it carries out some activities related to national security that do not involve law enforcement. Further, the CBSA collects both criminal and security intelligence. It has an extensive intelligence network, shares information and intelligence with American and other foreign agencies under a variety of agreements, and releases information to other parts of the federal government for national security purposes. In contrast, all of the RCMP's national security activities are conducted in furtherance of its law enforcement mandate to prevent, investigate and prosecute crime.

The CBSA consequently does not fit neatly under the mandate of SIRC or that of the review body for the RCMP. Nevertheless, I think it makes sense that independent review of the CBSA be carried out by one or the other of those bodies.

It would be difficult to separate the CBSA's law enforcement activities related to national security from those that are not. For example, an investigation of tobacco smuggling can turn into a terrorism investigation if the proceeds are directed to a terrorist group. In any event, having two review bodies for the national security operations of the CBSA would be unduly complicated and cumbersome. As I indicate above, there is significant advantage to limiting the number of independent review bodies in the national security field and building upon existing institutions.

On balance, I am of the view that responsibility for reviewing the CBSA should fall to ICRA, in view of its law enforcement expertise, but statutory gateways should be established to allow ICRA to exchange information, refer investigations, conduct joint investigations and coordinate the preparation of reports with SIRC when reviewing activities that involve security intelligence. Although the fit is not perfect, in the end, ICRA appears to be the better suited of the two review agencies, given the CBSA's law enforcement mandate, combined with its coercive powers.

2.23.3
Resources

One of the advantages, from a resource standpoint, to using SIRC and ICRA to review the five bodies is that the infrastructure is already in place. The new resource requirements will be incremental and, I think it is fair to say, far less than if new review bodies were to be established. The government should ensure that SIRC and the review body for the RCMP have the resources necessary to perform the mandates I recommend.

2.23.4 Amendment to SIRC Powers

Currently, SIRC does not have the extensive investigative powers that are held by the CSE Commissioner or that I recommend for the review body for the RCMP. It does not have the authority to subpoena documents or compel testimony from entities or persons outside CSIS. I recommend that it be given those powers, for the same reasons I recommend they be given to ICRA. Considering the degree of integration of the activities that SIRC would review, it is essential that SIRC's powers be expanded to enable it to obtain information outside CSIS or outside other entities it may have a mandate to review.

2.23.5 Other Issues

I have not examined all the details involved in expanding SIRC's mandate to encompass other federal entities. The comments I make above are therefore general in nature. However, my examination of the need for a review of the national security activities of other federal entities has brought to light several issues that will have to be addressed. The following are my comments in that regard.

2.23.5.1 Identifying National Security Activities

None of the other five departments and agencies regarding for which I recommend independent review are dedicated solely to conducting national security investigations. Indeed, in most cases, national security activities form a relatively small part of the overall mandate and workload. In order for SIRC or ICRA to conduct reviews of their national security activities, it will be necessary to consider, on an entity-by-entity basis, how best to determine what activities fall within the realm of national security. In some cases, the internal organizational structure, relevant databases or specific functions may make the dividing lines clear. Whatever the case, however, the review body must have access to all of the information necessary to make an informed decision about what needs to be reviewed and what falls outside its mandate.

2.23.5.2 CSE Commissioner

I am not recommending that SIRC's mandate be expanded to include the CSE, as I understand that the Office of the CSE Commissioner functions very well and I see no reason to interfere with that operation. That said, I recommend

below that the government establish statutory gateways and a coordinating committee to ensure that there is effective, independent review of integrated national security operations involving the CSE.

2.23.5.3
Department of National Defence

The Department of National Defence (DND) and the Canadian Forces (CF) are key federal intelligence gatherers. While much of their security intelligence capability involves foreign intelligence, they have a domestic intelligence capability, particularly in relation to marine security. In addition, the Canadian Forces' signals intelligence capability is closely integrated with the CSE. DND/CF representatives have been attached as liaisons to IBETs and INSETs. DND/CF also may provide armed assistance or intelligence assistance within Canada. For example, DND/CF personnel and assets were deployed for the 2002 G-8 Summit in Kananaskis, Alberta. I make no recommendations with respect to review of DND intelligence activities, for a number of reasons. I have heard evidence and conducted research on the national security role of a number of civilian agencies and departments, including the differences between civilian security intelligence and police criminal intelligence. I have not considered the nature of military intelligence. The distinction between military intelligence activities and civilian activities would have required extensive study outside my mandate. I note that there are two accountability bodies in relation to DND/CF: the Ombudsman for the Department of National Defence and Canadian Forces and the Military Police Complaints Commission. I recommend that the government consider issues of integration and information sharing between military and civilian federal agencies and, in particular, whether a statutory gateway to the two existing military review bodies would be desirable.

2.23.5.4
Other Federal Agencies and Departments

In Chapter V, I discuss all the federal departments and agencies that are in some way involved in national security activities. The involvement of the remaining entities does not at this time appear to be of such a nature as to warrant independent review. The review I recommend be conducted in five years' time should include consideration of whether other federal entities involved in national security activities should be subject to independent review.

2.23.5.5
Other Countries

Some of the eight countries examined in Chapter VII have review models that are function-based, as SIRC would have with its expanded mandate. Norway has perhaps the purest form of a function-based review model. The United Kingdom also makes use of function-based review for certain specified activities.

Officials in the various countries were very co-operative in providing information and suggestions to Commission staff with respect to the design of a review body for national security activities. I raise this point to suggest that those considering issues related to the expansion of the SIRC mandate would benefit from speaking directly to officials in countries where similar issues of integration and accountability have arisen.

2.24
Recommendation 11

The government should establish statutory gateways among the national security review bodies, including ICRA, in order to provide for the exchange of information, referral of investigations, conduct of joint investigations and coordination in the preparation of reports.

The RCMP's national security activities are increasingly integrated with those of other agencies. Some are federal entities engaged in the national security field and some, provincial or municipal police forces. In this recommendation, I address the need for integrated or co-operative review[49] between ICRA and the review bodies for other federal entities.

2.24.1
Integrated Activities

Since 9/11, the RCMP has significantly increased its integrated activity with other federal entities involved in the national security field. For example, Integrated National Security Enforcement Teams (INSETs) include representatives of agencies such as the CBSA, CIC and the Canada Revenue Agency. In Chapter V of this Report and in recommendations 9 and 10, I discuss the national security landscape, emphasizing the links between a variety of federal national security actors and both the RCMP and CSIS.

The events of 9/11 underlined the importance of integrated operations between the RCMP and CSIS. The two agencies engage in extensive co-operation and integration of their national security activities, and I expect that integrated

activity between them will increase in the future. Indeed, in the Factual Inquiry report, I recommended that the two agencies explore ways to promote further co-operation.

As I point out under Recommendation 9, the subject matter of the Factual Inquiry report provides an example of the nature of integrated national security operations among four federal agencies: the RCMP, CSIS, Canada Customs (now the CBSA) and DFAIT. Shortly after 9/11, CSIS transferred prime responsibility for a number of its national security investigations to the RCMP. One of those investigations was the one in which Maher Arar eventually became a person of interest. From time to time, CSIS provided the RCMP investigators with further information. For its part, the RCMP kept CSIS fully informed about the progress of its investigation by sharing its daily situation reports describing all of the investigative steps taken. For a time, a CSIS official was assigned to Project A-O Canada, the RCMP unit that conducted the investigation that involved Mr. Arar.

The RCMP investigation in question also involved considerable interaction with Canada Customs. A Canada Customs intelligence officer was assigned to Project A-O Canada. At the request of the RCMP, Canada Customs posted border lookouts for Maher Arar and Dr. Monia Mazigh, his wife. Canada Customs conducted two secondary examinations of Mr. Arar and forwarded the information obtained from them to the RCMP. Some of that information was provided to American authorities when Mr. Arar was detained in New York.

During the time Mr. Arar was imprisoned in Syria, the RCMP had frequent contact with DFAIT officials, particularly those in the Foreign Intelligence Division, or ISI. DFAIT provided the RCMP with the *bout de papier* that Canada's ambassador to Syria had received from Syrian Military Intelligence setting out a summary of a statement that Mr. Arar had made to Syrian officials. As it turned out, the statement had been made under torture.

Moreover, officials from the RCMP, CSIS and DFAIT discussed the advisability of CSIS officials travelling to Syria to meet with Syrian Military Intelligence during Mr. Arar's detention. DFAIT and RCMP officials also discussed the advisability of sending questions to Syria to be posed to Abdullah Almalki, who had been linked to Mr. Arar in the RCMP investigation and was detained in Syria at the same time as Mr. Arar. In the end, Canada's ambassador to Syria arranged for delivery of those questions to the Syrians. In addition, DFAIT provided some reports of its consular visits with Mr. Arar to the RCMP and CSIS. Further, there were extensive discussions among officials of DFAIT, the RCMP and CSIS about DFAIT's efforts to obtain Mr. Arar's release from Syrian custody. In brief, there was an enormous amount of interaction between the RCMP and DFAIT

concerning Mr. Arar's case. Their activities were integrated and, for review purposes, needed to be considered together.

At present, there is no body empowered to conduct a comprehensive review of integrated national security activities. Integrated review of integrated activities is essential, and statutory gateways linking review bodies are an important means of achieving effective review.

2.24.2
Need for Integrated Review

It is essential that there be institutional co-operation among review bodies where there is institutional co-operation among the bodies being reviewed, for four specific reasons: to avoid gaps in accountability, to attempt to avoid reaching inconsistent or differing conclusions about the co-operative activities, to provide a unified intake system for national security complaints, and to avoid the burden on agencies of duplicative review.

When different review bodies investigate the same or overlapping activities separately, there is a potential for gaps in findings regarding which operational agency or individual is accountable for what may be found to be illegal or improper actions. In an extreme case, a review body might conclude that ultimate responsibility for a problem lies with an agency outside its mandate rather than with the agency it reviews. As a result, all agencies involved in a flawed activity could avoid accountability. Less drastically, there is a risk that officials in an agency under review would point to others outside that agency as being responsible for impugned activities. Moreover, where there is no integrated or coordinated review, the potential exists for officials to structure operations so as to avoid review by their home review body.

In addition, when different review bodies review integrated or coordinated activities separately, there is a risk that inconsistent or differing conclusions about those same activities will be reached. Separate review bodies may receive different evidence or information about the activities, for a variety of reasons. For example, witnesses may give different versions of events, or the review bodies may not obtain all of the same documents. Whatever the reasons, separate factual investigations into the same events may produce different factual conclusions about what occurred — obviously an unsatisfactory outcome.

Further, there is a risk that review bodies acting separately may apply inconsistent standards to the same activities. While the mandates of the agencies being reviewed may be different and, thus, standards may in some circumstances differ, those standards are unlikely to be inconsistent with one another.

However, separate reviews create the potential for inconsistent application of standards to the same activity.

The need for coordinated review was made abundantly clear by the Factual Inquiry. Neither SIRC nor the CPC, the independent review bodies for CSIS and the RCMP respectively, were able to adequately review the full breadth of the actions of Canadian officials with respect to Mr. Arar, and there are no formal links for coordinating reviews between SIRC and the CPC. Thus, while the two bodies had jurisdiction to conduct reviews, there were no provisions or practices to prevent gaps in accountability for the integrated activities of CSIS and the RCMP or to attempt to prevent different or inconsistent conclusions by the two bodies about the same activities. The practice has been for the two review bodies to conduct independent reviews, even where there is overlap in the activities under examination. In the Factual Inquiry, there was the additional problem that neither SIRC nor the CPC had jurisdiction over Canada Customs or DFAIT, entities with considerable involvement in some aspects of the activities being reviewed.

Another problem in the Arar case was that neither SIRC nor the CPC had the power to compel the production of documents or testimony from agencies or individuals outside the agency being reviewed. The jurisdiction of each review body stops with the activities and employees of the agency it reviews. Although SIRC and the CPC may read one another's reports or at least the public portion of such reports after completion of a review, the potential for accountability gaps and inconsistent results is obvious. Coordination of independent reviews is fundamental where coordinated activities are involved.

Not surprisingly, many countries that have independent review mechanisms for different entities involved in the same activities have enacted provisions to address the potential for accountability gaps and inconsistent reviews. These provisions are frequently referred to as "statutory gateways."

Belgium has two parliamentary review committees. Committee P is responsible for reviewing all of Belgium's police agencies, and Committee I, for reviewing the country's two security intelligence agencies. Each of these committees is required by its governing statute to exchange information with the other regarding its activities, to submit its reports and conclusions to the other, to hold joint meetings where complementary information can be exchanged, and to discharge its mandate jointly with the other committee in certain circumstances. These provisions have led the two committees to carry out several joint investigations, including one on police and intelligence coordination and another on terrorism coordination among police and intelligence agencies. In interviews with Policy Review legal counsel, both committees spoke favourably

about the potential benefits of such co-operation. Indeed, as Committee P stated, institutional co-operation among review bodies is vital where there is institutional co-operation among the bodies being reviewed. Otherwise, there is too great a risk of escape from scrutiny by one body or the other.

In England and Wales, the Independent Police Complaints Commission (IPCC) has jurisdiction over all local police forces, as well as specialized police forces with national scope, including those that deal with national security investigations and Her Majesty's Revenue and Customs enforcement activities. Its jurisdiction will soon be extended to cover immigration enforcement activities as well. The IPCC's jurisdiction includes police forces that have activities that are integrated with several other agencies.

The IPCC's jurisdiction overlaps with that of a number of other public authorities, including authorities responsible for access to information and human rights matters, as well as several commissions and ombudsmen. England and Wales have provided for statutory gateways to address overlapping jurisdictions, the potential for duplication and the diminished observation and accountability that can result when multiple review bodies have "silo" vision. Statutory gateways allow information sharing between public bodies, among other things, and the Department for Constitutional Affairs has published guidance on the applicable laws and protocols that various bodies may establish. A statutory gateway was recently created to allow for information exchange and co-operation between the IPCC and the Parliamentary Ombudsman, which both have review jurisdiction over certain aspects of the new Revenue and Customs Department. The gateway allows the two bodies to disclose information to each other for purposes of the exercise of their respective mandates and to "jointly investigate" certain matters. Where an impugned matter or course of conduct has involved more than police forces, the IPCC has sometimes engaged in joint investigations with other accountability bodies.

Clearly, providing for integrated review of integrated national security activities goes a long way towards eliminating any potential "accountability gaps" and ensuring a consistent review process and concordant outcomes. However, there is a further reason for integrating the review of national security activities: to avoid the need for complainants to make multiple complaints. This is extremely important. Complainants should not be required to go to more than one review body to file a complaint about national security activities simply because those activities were conducted by more than one agency and those agencies are subject to the jurisdiction of separate review bodies. I come back to this issue of the need for a unified complaint intake system under Recommendation 12.

Integrated review can also avoid the burden of duplicative reviews, which may occur when different review agencies conduct investigations into the same or related matters at different times, thus requiring agencies to respond to demands for information two or more times. Duplicative review may occur unintentionally or as a response to inconsistent findings by different review agencies. Integrated review should allow the important work of review to be done only once in a cost-effective manner that produces a thorough report which is based on investigations of all relevant national security actors.

2.24.3
Statutory Gateways – General

As the name suggests, the gateways that I recommend should be established by statute. Providing for the mechanisms by which integrated review may take place in statutes emphasizes the importance of using such mechanisms. It should also eliminate or greatly reduce any jurisdictional arguments about whether an investigation falls within the statutory mandate of a particular review body.

I recommend that the statutory gateways apply to the three independent review bodies for federal entities engaged in national security activities: ICRA, the expanded SIRC and the CSE Commissioner. These review bodies have similar mandates, to review the activities of entities within their jurisdiction for conformity to law and standards of propriety; they would have similar powers if the recommendations in this Report are implemented; and they can be expected to conduct investigations and review processes in similar fashion. I am therefore satisfied that it would be feasible and practical to provide for a significant level of integration of review among them where the activities of the underlying agencies being reviewed are integrated.

Despite the relative lack of integration between the RCMP's national security activities and those of the CSE at present, I am of the view that it still makes sense to include the CSE Commissioner within the statutory gateway regime. I make this recommendation because of the similarity between the CSE Commissioner's review functions and those of the other review agencies, and because in the future there may be some cases of integrated activities. Moreover, I note that the CSE has a statutory mandate to provide technical and operational assistance to the RCMP and CSIS. In addition, as I point out under Recommendation 12, I envision an important role for the CSE Commissioner in a newly established integrated national security coordinating committee with responsibility for ensuring that the statutory gateway regime is functioning properly.

I do not recommend that the statutory gateways be extended beyond the three independent review bodies I mention above. The mandates of other federal review mechanisms, such as the Canadian Human Rights Commission, Privacy Commissioner, Information Commissioner and Auditor General, are significantly different from those of the three independent bodies to which I refer. While the jurisdictions of other bodies may overlap in some cases, the fundamental purpose of those other review bodies is either so much narrower or so different from the mandates of ICRA, SIRC and the CSE Commissioner that the type of integrated review that I propose flow from the statutory gateways would be impractical in their respect.

Moreover, if the statutory gateways I propose operate as intended, the resulting integrated review should avoid accountability gaps and inconsistent outcomes for matters falling within the mandates of the review bodies. Given the breadth of those review mandates, I do not see a need to establish formalized statutory gateways to the other review mechanisms mentioned above. It would do nothing to further these objectives.

That said, in Recommendation 5 (i), I propose that ICRA have the power to exchange information with and seek advice and assistance from other review and accountability bodies. I think that SIRC and the CSE Commissioner should have the same power, so that there can be informal co-operation with other review mechanisms as warranted. Moreover, the three review bodies under the gateway regime should develop the capacity to identify complaints that should be directed to one of these other agencies and make the necessary referrals. I repeat, however, that the statutory gateways should not be extended to other review or accountability bodies, at least not initially. It may be that, as matters evolve and experience is gained in the independent review of integrated national security activities, it will make sense to formalize gateways with the other review agencies. That is an issue that the review in five years' time should address.

I recognize that there are some federal entities involved in integrated national security activities that will not, for the time being, fall within the mandate of one of the three review bodies subject to statutory gateways. In Recommendation 10, I propose that ICRA be mandated to conduct independent review of the CBSA and that the mandate of SIRC be expanded to encompass four entities beyond CSIS. In the future, the government should consider whether to add other federal agencies to SIRC's review jurisdiction and whether the creation of additional statutory gateways is necessary. One of the primary factors in these future decisions should be the degree of integration between

agencies that already fall within SIRC's mandate and other government agencies or departments. The same might also be said of ICRA.

Finally, I note that the statutory gateways will require the exchange of information, some of which will be subject to national security confidentiality. It will be necessary to ensure that those receiving information have the required security clearances and that proper systems are in place in the recipient review bodies to maintain security of information. However, I do not envision that maintaining security of information should be a particular problem. By their very nature, the three review bodies subject to the statutory gateways recommended above will be required to have proper processes for maintaining confidentiality of information. Moreover, dissemination of confidential information within a review body can be limited to that information that is necessary and relevant to the review being undertaken.

2.24.4
Statutory Gateways – Specific Goals

I recommend that the statutory gateways be designed to achieve four goals: exchange of information, referral of investigations, joint investigations and coordination in the preparation of reports. I propose that they be permissive, conferring the authority to carry out the designated function.

2.24.4.1
Exchange of Information

Exchanging information about integrated operations is an important first step for integrated review. The three review bodies should be authorized to exchange all information, to enable the others to fully fulfill their mandates. Information should be provided both in response to requests from another review body and on the initiative of the review body providing the information. For example, if ICRA becomes aware that activities being investigated were conducted in an integrated or co-operative fashion with another entity subject to review by SIRC, it should determine whether there is a potential need for review of the integrated activities. If there is, ICRA should contact SIRC and provide it with the relevant information.

The underlying premise for the exchange of information should be that information available to one review body should be available to another insofar as it is connected to integrated or co-operative activities or to the mandate of the recipient body. There should be no jurisdictional barriers to the flow of information that needs to be shared to prevent gaps in accountability and avoid inconsistent outcomes when integrated activities are reviewed. Having said that,

I stress that only information that is necessary and relevant to a review should be exchanged.

2.24.4.2 Referral of Investigations

Given the level of integration of national security activities, there will be times when a complaint is made to a review body that, on examination, turns out to be the wrong body. In such circumstances, the review body should be authorized, at any stage of an investigation, to transfer the investigation, together with its investigative product, to the appropriate body and to provide whatever assistance is necessary to avoid duplication of investigative efforts and enable the other body to continue the investigation as expeditiously as possible.

In some instances, the referring review body may continue with all or part of its own investigation or, as I indicate in the next section, the two bodies may decide to conduct a joint investigation.

The three review bodies under the statutory gateway regime should have the capacity to identify complaints that fall outside their collective mandates, along with the appropriate review/accountability mechanism. It is important that, when appropriate, they refer complaints to other accountability bodies not under the regime, such as the Canadian Human Rights Commission, the Privacy Commissioner, the Ombudsman for the Department of National Defence and Canadian Forces, the Military Police Complaints Commissioner, or the Office of the Correctional Investigator (the ombudsman for federal corrections), for matters involving conditions of immigration detention. Referral of complaints to the proper body is a relatively simple matter and clearly in the public interest, so that complainants are not left on their own to sort out the maze of federal accountability mechanisms.

2.24.4.3 Joint Investigations

The authority to conduct joint investigations of integrated operational activities is vital to successful integrated review. It is not practical to set out here all of the possible ways that joint investigations might be conducted. When a joint investigation is being considered, those responsible within the review bodies should prepare an investigation plan, clearly delineating which body is responsible for which aspects of the investigation and what investigative steps must be taken. The objective should always be to provide the most effective review of the integrated activities, so as to avoid accountability gaps and conclusions or recommendations based on different factual determinations. A joint investigation

should be aimed at ascertaining all of the facts relating to integrated activities in order that each review body can make the assessment required by its mandate on a commonly understood factual basis.

In addition, joint investigations should be directed at avoiding duplication of investigative effort. It makes little sense, for example, to have SIRC and ICRA each conduct separate investigations into a factual situation relating to integrated CSIS and RCMP activities.

Decisions relating to personnel and resources for joint investigations are best approached on a case-by-case basis. Relevant factors will include the level of involvement of an underlying agency and the expertise and available resources of the respective review bodies. As discussed under Recommendation 12, any disputes about joint investigations will be referred to a coordinating committee, the Integrated National Security Review Coordinating Committee (INSRCC), for resolution.

Developing joint investigation plans undoubtedly will require a good deal of co-operation between review bodies and a conscious effort to avoid jurisdictional disputes. I would hope that, over time, the review bodies would jointly develop expertise in working co-operatively, so that the prospect of joint investigations would not be viewed as a threat to jurisdictional interests.

A successful joint investigation should result in a common understanding about the facts relating to the integrated activities. It should also produce coordinated recommendations about how the agencies subject to review should respond to the findings.

Some investigations, particularly those involving complaints, may require hearings in which the agency being investigated and the complainant are entitled to participate. Clearly, joint hearings will be more challenging than joint investigations. Although I do not envision that there will be many cases where joint hearings are required, I would not exclude the possibility. If a joint hearing makes sense, it should be held. I am satisfied that, with co-operation between review bodies, a process can be established to coordinate such hearings. By way of example, I point to the practice of the Ontario and Quebec securities commissions of holding joint hearings on occasion. Although the two commissions were established under separate provincial statutory schemes, they have been able to co-operate and conduct effective joint hearings. If two provincial bodies can achieve that level of co-operation, one would expect that federal review agencies would also be able to do so.

The outcome of a joint hearing should be the same as the outcome of a joint investigation: a common factual basis upon which each of the review bodies can make its own assessment and prepare its own report in accordance with its mandate.

2.24.4.4
Coordination in the Preparation of Reports

Statutory gateways do not alter or intrude upon the exercise of each review body's responsibility for preparing and submitting reports as described in its constituting legislation. However, for purposes of producing such reports, when more than one review body has investigated or reviewed integrated activities, there is significant advantage to consultation among the review bodies to discuss assessments on the basis of the commonly understood underlying facts. While each review body must reach its own conclusions, prior consultation can minimize the potential for gaps in accountability for the integrated activities and for inconsistent conclusions.

I envision that, in some cases, the conclusions of more than one review agency could be included in consolidated reports, which would then be provided to the appropriate minister(s).

While statutory gateways cannot ensure that there will be no accountability gaps or inconsistent conclusions, I think that, if they are properly applied, the potential for such undesirable results can be significantly reduced.

2.25
Recommendation 12

The government should establish a committee, to be known as the Integrated National Security Review Coordinating Committee, comprising the chairs of ICRA and the Security Intelligence Review Committee, the Communications Security Establishment Commissioner and an outside person to act as Committee chair. INSRCC would have the following mandate:

- **to ensure that the statutory gateways among the independent review bodies operate effectively;**
- **to take steps to avoid duplicative reviews;**
- **to provide a centralized intake mechanism for complaints regarding the national security activities of federal entities;**
- **to report on accountability issues relating to practices and trends in the area of national security in Canada, including the effects of those practices and trends on human rights and freedoms;**
- **to conduct public information programs with respect to its mandate, especially the complaint intake aspect; and**
- **to initiate discussion for co-operative review with independent review bodies for provincial and municipal police forces involved in national security activities.**

2.25.1
Operation of Statutory Gateways

The statutory gateways that I propose are permissive. Their success in meeting their objectives will depend almost entirely on co-operation among the three review bodies.

Because co-operation is so important to the success of integrated review, I think it would be prudent for a coordinating committee — which would include among its members the chairs of ICRA and SIRC and the CSE Commissioner — to provide a formal and effective mechanism for coordination of review of integrated activities. I envision that this aspect of INSRCC's mandate need be nothing more than a formalized process of consultation and co-operation. Indeed, if this function of INSRCC proves unnecessary because the required co-operation will take place in any event, then that will be an excellent outcome. If the review bodies are able to address all of the issues required to achieve effective integrated review of integrated activities, there will be no need for INSRCC to take any action in terms of overseeing the effectiveness of statutory gateways.

INSRCC will need to take action in relation to its oversight of statutory gateways only when the review bodies, at the operational level, are not functioning as intended.

To fulfill this part of its mandate, INSRCC should be informed on a regular basis by the chairs of ICRA and SIRC and the CSE Commissioner about reviews or investigations involving integrated activities, parallel reviews that may be taking place with respect to the same activities, and cases being reviewed pursuant to statutory gateways. In particular, INSRCC should be informed of any difficulties or disagreements with respect to integrated review. It should determine whether reviews of integrated activities are being conducted in ways that will avoid the potential for accountability gaps and inconsistent outcomes, and whether any additional steps should be taken in order to achieve the objectives of integrated review.

In those instances where INSRCC determines that different or additional steps should be taken to provide effective integrated review, it should issue an investigation plan setting out the responsibilities of the review bodies involved and the investigative steps it considers appropriate. An investigation plan could involve some or all of the co-operative actions contemplated by the statutory gateways. INSRCC's authority in this regard would not undermine the independence of the review bodies, as INSRCC itself will be independent and at arm's length from government.

I expect that, in most, if not all cases, INSRCC members would be able to agree on the most effective and appropriate course of action for integrated review. In those cases where members of INSRCC are unable to reach a consensus regarding a course of action, INSRCC should determine the course to be followed for integrated review by majority vote, with the independent chair casting an additional deciding vote where necessary**.**

Some have suggested that giving a coordinating committee the authority to direct investigation plans would result in an atmosphere of confrontation among the review bodies. I find this suggestion rather surprising and disappointing. The Canadian public should be able to expect that those responsible for the independent review bodies in respect of Canada's national security activities could reach agreement on the most effective approach for integrated review. All of the review bodies should have the same objectives: to ensure that integrated reviews are effective, there are no gaps in accountability and review outcomes are consistent, and to avoid duplicative review. I have more optimism about the capacity of review bodies to cooperate fully than those who put forward this rather pessimistic outlook.

Finally, I recommend that INSRRC be authorized to direct the underlying review bodies to conduct an integrated investigation or review upon request of the Minister of Public Safety, Minister of National Defence or Attorney General, or upon direction by Order in Council. I envision that this power will be used only rarely, but it could be useful in dealing with another case similar to Mr. Arar's, involving pressing issues and multiple national security agencies.

2.25.2
Avoiding Duplication

INSRCC's mandate should include responsibility for preventing duplication of review of the same activities, which is a waste of time and resources. Potential for duplicative review looms large when the operational activities of two agencies with separate review bodies are not coordinated or integrated.

INSRCC should be able to perform this aspect of its mandate with little difficulty. On receipt of the information from the ICRA and SIRC chairs and the CSE Commissioner, INSRCC should identify situations with a potential for duplication and, in a co-operative manner if possible, develop an investigation plan to avoid the problem. Again, where agreement cannot be reached, the committee should proceed by majority vote. The review bodies involved would then be required to implement the investigation plan as directed.

INSRCC could also provide a forum for coordinating review among its members and other federal review agencies such as the Privacy Commissioner, Information Commissioner, Canadian Human Rights Commission and Auditor General. Although not represented on INSRCC, those other review agencies could be encouraged to inform INSRCC of plans to conduct reviews of national security activities, thereby enabling INSRCC to inform the relevant independent review agency of ongoing or planned reviews or of the possibility of pooling resources and information. Such a coordinating role could be helpful both to avoid wasteful duplication and thus conserve limited review resources and to ensure that no one federal agency with national security responsibilities is overwhelmed and overburdened with multiple reviews conducted by different review agencies at any one point in time.

INSRCC's mandate with respect to avoiding duplication need not be onerous. Nevertheless, as integrated operations in the national security field increase, so, too, will the need to avoid duplication in review.

2.25.3
Centralized Complaint Intake

INSRCC should establish a complaint intake system with the capacity to receive complaints related to the national security activities of any federal entity. When it receives a complaint, INSRCC should assess it to determine which review or accountability agency has jurisdiction to address it and then direct the complaint to the appropriate agency. Here, I envision that complaints would be directed not only to the review bodies represented by INSRCC (ICRA, SIRC or the CSE Commissioner), but also to any other review body or accountability mechanism within the federal government.

In order to fulfill this role, INSRCC will have to set up a process for receiving and triaging complaints. It will need the capacity to review the substance of a complaint, identify the entities that might be involved in the activities complained of, and assess what review or accountability mechanism has jurisdiction to address the matter.

I am satisfied that there is a compelling need for a unified processing function for complaints relating to national security activities within the federal government. Throughout this Report, I speak frequently of the large increase in national security activities undertaken by federal entities and in integration among those entities. The result of that increase is that it has become more and more difficult for individuals with complaints to know where to lodge them. The problem is compounded by the fact that so many national security activities are cloaked in secrecy.

Thus, for example, when an individual becomes aware that a government entity has collected and stored information about him or her that is inaccurate, the individual may have no idea what entities were involved in the information collection or dissemination process, or where to complain. Potential complainants should not have to go from one review body or accountability mechanism to another until they find the right one. Being turned away and told to try somewhere else creates frustrations, impedes effective review, and can undermine public confidence in the review process. At the Policy Review hearings, a number of intervenors made persuasive submissions concerning the desirability of having a single agency able to receive all complaints relating to national security activities.

It makes abundant sense for the government to establish a single agency to take complaints, sort them out and direct them to the bodies with jurisdiction to address them. As I point out above, some complaints may involve entities not within the jurisdiction of the review bodies represented by the INSRCC.

However, INSRCC, constituted as I propose, is a sensible choice for handling the complaint-receiving function, regardless of the entity to which a complaint relates. In many cases, the agency or department that is the subject of a complaint will be readily identified. Moreover, many complaints will probably be channeled to one or more of the three review bodies represented by INSRCC, as they are responsible for the review of the most significant actors in the national security field.

In addition, the combined expertise of the ICRA and SIRC chairs and the CSE Commissioner in assessing complaints and conducting investigations should be invaluable in guiding the complaints intake function. If one accepts the notion that there is a significant public interest in having a unified complaints-receiving mechanism for all federal entities, it seems to me that INSRCC is ideal for carrying out that task. The triaging undertaken by INSRCC should also assist it in identifying both accountability trends and gaps in the dynamic national security environment.

I do not envision that establishing a unified complaints intake process within INSRCC will remove the need for separate complaint intake systems within each of the three review bodies represented by INSRCC. I propose that those bodies continue to receive complaints from the public as well as those referred to them by INSRCC and to handle them in much the same way they have in the past. When INSRCC receives a complaint and determines that integrated review is necessary, it may direct the manner in which the integrated review is to be conducted when it refers the complaint to the appropriate review body.

INSRCC's complaint processing function will involve creating an infrastructure with appropriate capacity to fulfill this aspect of INSRCC's mandate. The government should ensure that INSRCC has adequate resources in this regard.

2.25.4
Reports on Accountability Issues

The complexity of Canada's national security activities has grown enormously in recent years. The ways in which national security activities may run afoul of the law or standards of propriety have also increased, as have the potential impacts on individual rights and freedoms.

Canada has an important interest in monitoring the way national security activities are evolving and in keeping abreast of practices or trends that create accountability problems. The independent agencies responsible for reviewing the national security activities of the major federal participants in the national security field are ideally situated to observe the types of practices or trends that warrant consideration by the government. Most of what the review bodies learn

will be contained in reports on reviews and complaint investigations. However, the advantage of INSRCC is that its members will have the opportunity to examine both the reports of the three review bodies and the information derived from its own complaints processing function in a coordinated and cohesive way. As a result, INSRCC will be in an excellent and perhaps unique position within the Canadian national security milieu to report to government about practices and trends that warrant observation and comment. In short, INSRCC will be able to see the "big picture" with respect to independent review of the government's national security activities. I recognize that a committee of parliamentarians on national security or a legislative committee, should one be created, would also have the capacity to see the "big picture" with respect to the government's national security activities, but I note that it might be concerned more with the efficacy of these activities than their propriety. INSRCC, like its constituent independent review agencies, will be primarily concerned with issues relating to propriety and accountability, as opposed to efficacy.

I suggest that INSRCC be authorized to receive submissions from the public and to consult with other agencies within and outside government as it deems appropriate in furtherance of its mandate to report on accountability and the effects of national security practices on human rights and freedoms. I also suggest that INSRCC prepare a report on matters relating to this part of its mandate on an annual basis. The report should be submitted to the Minister of Public Safety, Minister of Defence and other ministers of agencies subject to review by SIRC, and should be tabled in Parliament within 15 sitting days, as is done for the annual reports of SIRC, the CPC and the CSE Commissioner.

2.25.5
Public Information Role

INSRCC should also conduct a public information program to inform Canadians about its mandate. In particular, it should ensure that the public is informed of its complaint intake function and responsibility to report on accountability issues in respect of Canada's national security practices and trends.

An effective public information program will greatly assist INSRCC in carrying out these important responsibilities.

2.25.6
Provincial and Municipal Police Forces

The evidence in this Inquiry indicates that provincial and municipal police forces are becoming increasingly involved in law enforcement investigations relating to national security. Integration of national security activities is important and

should continue. However, it is essential that integrated operations take place within a clearly established framework in order that there be a common understanding of the roles and responsibilities of those involved.

The Canadian Association of Chiefs of Police has endorsed the concept of an overarching federal statute to provide a framework for integrated policing across Canada. This strikes me as a good idea. However, I have not looked at that issue sufficiently to make a specific recommendation.

That said, when there are integrated activities among federal entities and provincial or municipal police forces in the national security area, there is merit in ensuring co-operative independent review of those activities. I am referring here to consultation and coordination of activities between the independent review bodies for the federal entities and their provincial or municipal counterparts, to the extent appropriate. Since provisions for independent review may vary depending on the provincial and municipal police force, arrangements would have to be tailored to different situations.

There are two points worth keeping in mind here. First, the RCMP is not the only federal body to conduct integrated activities relating to national security with provincial and municipal police forces. INSETs and IBETs are good examples of bodies in which provincial and municipal police officers operate on an integrated basis with federal agencies other than the RCMP. For that reason, the need for co-operative review extends beyond the review body that I propose for the RCMP.

Second, given its coordinating role, INSRCC is ideally placed to initiate discussions between independent federal review agencies and independent provincial review agencies for coordination of review of integrated activities when warranted. INSRCC represents three key independent review bodies and, as such, should have the expertise to initiate and lead the necessary discussions. If arrangements are to be formalized, then the respective governments — federal, provincial or municipal — will need to be involved.

Finally, I would suggest that the initiative to develop a co-operative approach to independent review involve the Canadian Association of Chiefs of Police. This organization has obviously given a great deal of thought to issues arising from integrated policing and would make a valuable contribution to the discussions.

2.25.7 Composition

I propose that INSRCC initially have four members: the chairs of ICRA and SIRC, the CSE Commissioner and an outside person to act as an independent committee chair. I do not see the need for a larger committee at this stage.

The chair of INSRCC should be someone who has expertise in the national security field and who would not only be, but also be perceived to be, independent of government and of the agencies involved in national security activities. The position of chair would be part-time. In the event of votes, the chair would have an additional deciding vote.

It may be that, as experience is gained, there will be an advantage to adding another member. It has been suggested that there should be a member to represent all of the other federal review or accountability bodies. It has also been suggested that the Privacy Commissioner would be a particular asset to INSRCC, as so many of the national security activities that may be the subject of complaints relate to the collection, storage and dissemination of personal information. There is merit to this suggestion. However, for the time being, it should be sufficient to ensure that INSRCC has the capacity to consult with and seek the advice of others (such as the Privacy Commissioner) who have special expertise in matters that might fall within its mandate.

2.25.8 Staffing

INSRCC will be required to hire qualified staff to fulfill its mandate. However, I do not envision a large bureaucracy or infrastructure. The committee will not be conducting reviews. It will consider the need for and adequacy of integrated reviews by the three independent review bodies and will serve as a clearing house and coordinating mechanism for complaints. Nevertheless, the process for handling complaints and perhaps making reports on accountability issues relating to Canada's national security activities will require staff with appropriate expertise and adequate resources. I expect that, in some cases, staff could be seconded to INSRCC from ICRA, SIRC, the CSE Commissioner and other federal review agencies, thereby providing INSRCC with the benefits of existing expertise, while at the same time broadening the experience of those seconded to the committee.

2.25.9
Reporting

In my view, INSRCC should report to a responsible minister, as the review bodies do. The reason is that all elements of the security and intelligence landscape need to be accountable to the executive rather than the legislative branch of government. The latter can review reports, but cannot act on recommendations. In the event of improper national security activities, the responsible minister is in the best position to take corrective action. Ultimately, it is the executive branch, in the form of responsible ministers, that is responsible for the propriety of the actions of the operating agencies being reviewed.

INSRCC should report to the ministers with responsibility for the independent review agencies represented on it: the Minister of Public Safety for the RCMP and SIRC review bodies, and the Minister of National Defence for the CSE Commissioner. It should also report as appropriate to the minister(s) responsible for the agencies whose activities are being reviewed in a given report.

2.25.10
Arguments Against INSRCC

The concept of INSRCC was put forward as an option during the Policy Review hearing process. Several of the parties made submissions opposing the idea, some strongly. The parties against INSRCC can be divided into two broad categories: those who do not think it is necessary, and those who would prefer a super agency that would conduct reviews of the national security activities of all federal entities in the field. I have already made the case for the necessity of INSRCC. Below, I address the arguments in favour of a super agency.

2.25.10.1
Super Agency

Many from outside government have submitted that setting up a body such as INSRCC does not go far enough in addressing accountability concerns that arise from integrated national security activities. They advocate the creation of a super agency, which would review all of the national security activities of federal entities. Some have suggested that the super agency would apply only to the "main players," but that the RCMP would be one of those players.

The single most important factor underlying these submissions is the need to extend independent review to government agencies not now included within the mandate of existing review bodies. A secondary concern is the need to avoid problems with accountability gaps and inconsistent reviews of integrated

operational activities. It has also been argued that a super agency would provide a convenient single intake point for all complaints related to national security and an excellent observation point for discerning problems or trends in the accountability mechanisms for Canada's national security activities.

I am satisfied that the model I propose addresses all of these concerns. In addition, it avoids what, by any measure, would be the huge and potentially unwieldy step of creating a massive new review body. A super agency also runs the risk of blurring the important differences in the roles of the numerous national security actors — in particular, the distinctions between national security intelligence gathering and law enforcement.

Finally, Recommendation 13 concerns an independent review of the recommendations in this area in five years' time. The national security landscape in Canada is growing and changing. If it is determined that changes are needed to achieve the objectives of the super agency, then those changes may be adopted at that time.

2.26
Recommendation 13

In five years' time, the government should appoint an independent person to re-examine the framework for independent review recommended in this Report, in order to determine whether the objectives set out are being achieved and to make recommendations to ensure that the review of national security activities keeps pace with changing circumstances and requirements.

2.26.1
Need for Review

I recommend an independent review after five years for two reasons. The first is that the proposed models for integrated review adopt a novel approach in Canada for the review of national security activities and may require modification based on experience with them. The second is that Canada's national security activities are evolving at a rapid pace and changes may be required to keep up with changing circumstances.

The proposals for integrated review in this Report attempt to make use of existing institutions to the extent possible and minimize the creation of new complex structures. I expect that, with appropriate effort and support, the models I propose will ensure an appropriate level of review for Canada's national security activities. However, the problems that these proposals are designed to address are complex and will be difficult to overcome. In particular, the success

of ICRA, the approach to reviewing integrated activities, the expanded SIRC, the statutory gateways and the role of INSRCC will be dependent to a considerable extent on co-operation among the review bodies involved. At this time, one can not be certain that the required co-operation will occur. Therefore, after some time has elapsed, it will be important to assess whether the structures proposed in this Report are functioning as intended.

The second reason for a review after five years is the fact that Canada's national security activities are evolving quickly. It is fair to assume that, over a period of five years, there will be an increase in the number of Canadian agencies involved in national security activities and in the level of integrated activities among those agencies. Sharing of national security information with other agencies, particularly internationally, is also likely to be stepped up. Further, those responsible for protecting Canada's national security may face new threats not presently contemplated and some federal entities may become involved in the national security field in new ways. In five years' time, additional agencies or persons may have been assigned to coordinate the government's national security activities and a national security committee of parliamentarians may have been established.

It is essential that Canada's review mechanisms for national security activities keep pace with the evolution of the activities being reviewed, in order that the objectives of review that I discuss in this Report may be achieved.

In its 2004 National Security Policy, the Government of Canada captured this idea when it said, "as legal authorities and activities of our security and intelligence agencies evolve to respond to the current and future security environment, it is vitally important that we ensure review mechanisms keep pace."[50]

2.26.2
Review Process

The review at the end of five years should be conducted by a person independent of the agencies to be reviewed, the review bodies, and government. The review bodies and agencies being reviewed could be perceived as having an interest in the outcome of the review. They might have different views about how integrated review has proceeded and what should be done in future, particularly if there have been difficulties. Similarly, the government, which is responsible for providing direction to the agencies being reviewed and for receiving and acting upon recommendations of the review bodies, may be seen to have an interest in one approach or another. Given the great importance of public confidence and trust in the effective review of national security activities, it would be prudent to appoint an independent person to conduct the review.

I do not envision the review in five years' time being a public inquiry. That is not necessary. The research done for this Inquiry and Report should provide a platform for conducting the review. It should not need to be repeated. The review could simply build on the work done to date.

The person responsible for the review should have the scope to adopt the process he or she considers appropriate. The reviewer will require proper security clearance, to be able to examine the necessary information in order to determine how effectively review models have been able to address integrated activities.

Finally, without being prescriptive, I envision that the review in five years' time would assess and report on each of the following matters:

(a) the effectiveness of the RCMP review body in reviewing the RCMP's national security activities;
(b) the effectiveness of the expanded SIRC in reviewing the national security activities included within its mandate;
(c) whether SIRC's expanded mandate is interfering with the effective review of CSIS;
(d) whether INSRCC is fulfilling its mandate;
(e) the efficacy of the statutory gateways in carrying out their intended objectives and the possibility that the gateways should be extended to other federal accountability mechanisms; and
(f) whether there are other federal entities engaged in national security activities that require independent review.

The reviewer should make recommendations to the Governor in Council for modifications to the review system as he or she deems necessary, and a copy of the reviewer's report should be made public and tabled in Parliament.

3.
SUMMARY LIST OF RECOMMENDATIONS ARISING FROM POLICY REVIEW

Recommendation 1

Existing accountability mechanisms for the RCMP's national security activities should be improved by putting in place an independent, arm's-length review and complaints mechanism with enhanced powers.

Recommendation 2

The review and complaints body should be located within a restructured Commission for Public Complaints Against the RCMP, and be renamed the Independent Complaints and National Security Review Agency for the RCMP (ICRA for short) to reflect its expanded role.

Recommendation 3

ICRA's mandate should include authority to:

(a) conduct self-initiated reviews with respect to the RCMP's national security activities, similar to those conducted by the Security Intelligence Review Committee (SIRC) with respect to CSIS, for compliance with law, policies, ministerial directives and international obligations and for standards of propriety expected in Canadian society;
(b) investigate and report on complaints with respect to the RCMP's national security activities made by individual complainants and by third-party groups or individuals;
(c) conduct joint reviews or investigations with SIRC and the CSE Commissioner into integrated national security operations involving the RCMP;
(d) conduct reviews or investigations into the national security activities of the RCMP where the Minister of Public Safety so requests;
(e) conduct reviews or investigations into the activities related to national security of one or more government departments, agencies, employees or contractors, where the Governor in Council so requests; and
(f) in exercising its mandate with respect to the matters in paragraphs (a) to (d) above, make recommendations to the Minister of Public Safety, and with respect to matters in paragraph (e), to make recommendations to the relevant Ministers.

Recommendation 4

ICRA should have the following powers:

(a) extensive investigative powers, similar to those for public inquiries under the *Inquiries Act*, to allow it to obtain the information and evidence it considers necessary to carry out thorough reviews and investigations; those powers should include the power to subpoena documents and compel testimony from the RCMP and any federal, provincial, municipal or private-sector entity or person;
(b) power to stay an investigation or review because it will interfere with an ongoing criminal investigation or prosecution;
(c) power to conduct public education programs and provide information concerning the review body's role and activities; and
(d) power to engage in or to commission research on matters affecting the review body.

Recommendation 5

ICRA's complaints process should incorporate the following features:

(a) in the first instance, ability on the part of ICRA to refer a complaint to the RCMP for investigation or to investigate the complaint itself, if deemed appropriate;
(b) ability on the part of the complainant to request that ICRA review the complaint if the complainant is not satisfied with the RCMP's investigation and disposition of it;
(c) ability on the part of ICRA to dismiss a complaint at any stage of an investigation as trivial, frivolous or vexatious, or made in bad faith;
(d) establishment of a program providing opportunities for the use of mediation and informal complaint resolution, except where the complainant does not have the information about the RCMP activities that are relevant to the complaint;
(e) with respect to complaints, opportunity for the Commissioner of the RCMP and affected members of the RCMP to make representations to ICRA and, where a hearing is commenced, to present evidence and be heard personally or through counsel;
(f) opportunity for the complainant to make representations to ICRA and to present evidence and be heard personally or through counsel at a hearing;

(g) open and transparent hearings of a complaint, to the extent possible, but authority for ICRA to conduct all or part of a hearing in private when it deems it necessary to protect national security confidentiality, ongoing police investigations or the identity and safety of sources;
(h) for purposes of hearings of complaints, discretion by ICRA to appoint *security-cleared* counsel independent of the RCMP and the government to test the need for confidentiality in regard to certain information and to test the information that may not be disclosed to the complainant or the public;
(i) ability for ICRA to seek the opinions or comments of other accountability bodies, such as the Canadian Human Rights Commission, the Privacy Commissioner of Canada and the Information Commissioner of Canada.

Recommendation 6

ICRA should be structured so that complaints and reviews related to the RCMP's national security activities are addressed only by specified members. Appointments of such members should be aimed at inspiring public confidence and trust in their judgment and experience. Appointees should be highly-regarded individuals with a stature similar to SIRC appointees.

Recommendation 7

CRA should prepare the following reports to the Minister of Public Safety (the Minister) and the Commissioner of the RCMP:

(a) Reports arising from self-initiated reviews and investigations of complaints, which should include non-binding findings and recommendations.
(b) Annual reports on its operations to the Minister, who should lay an edited version of the report, omitting national security information, before each House of Parliament.

All of the above reports may include confidential information (including information subject to national security confidentiality) and should also include an edited version that ICRA proposes for public release.

Recommendation 8

ICRA should have an adequate budget to fulfill its mandate in relation to the RCMP's national security activities, including for purposes of self-initiated review.

Recommendation 9

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.

Recommendation 10

ICRA should review the national security activities of the Canada Border Services Agency, and the Security Intelligence Review Committee should review the national security activities of the other four entities.

Recommendation 11

The government should establish statutory gateways among the national security review bodies, including ICRA, in order to provide for the exchange of information, referral of investigations, conduct of joint investigations and coordination in the preparation of reports.

Recommendation 12

The government should establish a committee, to be known as the Integrated National Security Review Coordinating Committee, or INSRCC, comprising the chairs of ICRA and the Security Intelligence Review Committee, the Communications Security Establishment Commissioner and an outside person to act as Committee chair. INSRCC would have the following mandate:

- to ensure that the statutory gateways among the independent review bodies operate effectively;
- to take steps to avoid duplicative reviews;
- to provide a centralized intake mechanism for complaints regarding the national security activities of federal entities;
- to report on accountability issues relating to practices and trends in the area of national security in Canada, including the effects of those practices and trends on human rights and freedoms;
- to conduct public information programs with respect to its mandate, especially the complaint intake aspect; and
- to initiate discussion for co-operative review with independent review bodies for provincial and municipal police forces involved in national security activities.

Recommendation 13

In five years' time, the government should appoint an independent person to re-examine the framework for independent review recommended in this Report, in order to determine whether the objectives set out are being achieved and to make recommendations to ensure that the review of national security activities keeps pace with changing circumstances and requirements.

Notes

1 In this chapter, unless I state otherwise, I use the term "review" broadly to encompass both self-initiated review and complaint investigation functions.

2 Germany has an intelligence review committee in parliament, but no body that reviews the police.

3 [2004] F.C.J. No. 1029, aff'd [2005] F.C.J. No. 1011.

4 *Report of the Auditor General of Canada to the House of Commons* (Ottawa: Minister of Public Works and Government Services Canada, 2003), para.10.161 [Auditor General's 2003 report].

5 R.S.C. 1985, c. C-46 (as am. by the *Anti-terrorism Act,* S.C. 2001, c. 41).

6 "Policy Review Submissions," Canadian Arab Federation and Canadian Council on American-Islamic Relations (Written submission, Arar Commission Policy Review Public Submissions), February 21, 2005, p. 26**.**

7 R.S.C. 1985, c. R-10, s. 45.35(1).

8 Hon. Patrick J. LeSage, *Report on the Police Complaints System in Ontario,* April 22, 2005, online, Ontario Ministry of the Attorney General, http://www.attorneygeneral.jus.gov.on.ca/english/about/pubs/LeSage/en-fullreport.pdf (accessed August 14, 2006) [LeSage].

9 Bill 103, *Independent Police Review Act*, 2nd Sess., 38th Leg.**,** Ontario, 2006, s. 58(1).

10 R.S.C. 1985, c. R-10, s. 45.37.

11 Ibid., s. 5(1).

12 R.S.C. 1985, c. C-23, s. 54.

13 *Babcock v. Canada (Attorney General)*, [2002] 3 S.C.R. 3 at para. 18 (internal citation omitted).

14 Ibid. at paras. 22, 32.

15 *Canada Evidence Act*, R.S.C. 1985, c. C-5, s. 39(2).

16 *Babcock v. Canada (Attorney General)*, [2002] 3 S.C.R. 3 at paras. 22, 25, 36, 39, 41, 42.

17 *RCMP Act*, ss. 45.36, 45.39, 45.4.

18 Ibid., ss. 45.41, 45.42.

19 Ibid., s. 45.43.

20 Ibid., s. 45.46.

21 "Submissions of the Commission for Public Complaints Against the RCMP Regarding the Policy Review of the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar" (Written submission, Arar Commission Policy Review Public Submissions), February 21, 2005, p. 49.

22 LeSage (see note 16), p. 66.

23 *RCMP Act*, s. 45.36

24 Canada, Commission for Public Complaints Against the RCMP, *Review 2004/2005 – Annual Report* (Ottawa: Minister of Public Works and Government Services, 2005), pp. 29–31 (Chair: Shirley Heafey).

25 *RCMP Act*, s. 45.36(6).

26 Ibid., ss. 44.42(2), 45.46(3).

27 Ibid., ss. 45.45(2), 45.45(5).

28 *CSIS Act*, s. 48(2).

29 Ibid., s. 48(1).

30 *RCMP Act*, s. 45.45 (11).

31 See, e.g., *Toronto Star Newspapers Ltd. v. Ontario*, [2005] 2 S.C.R. 188; *Vancouver Sun (Re)*, [2004] 2 S.C.R. 332; *Sierra Club of Canada v. Canada (Minister of Finance)*, [2002] 2 S.C.R. 522; *R. v. Mentuck*, [2001] 3 S.C.R. 442; *Canadian Broadcasting Corp. v. New Brunswick (Attorney General)*, [1996] 3 S.C.R. 480; *Ottawa Citizen Group Inc. v. Canada (Attorney General)* 2005, 75 O.R. (3d) 590 (Ont. C.A.) and 2005, 75 O.R. (3d) 607 (Ont. C.A.).

32 *Chahal v. United Kingdom* (1996), 23 EHRR 413.

33 U.K., H.C., Constitutional Affairs Committee, *The operation of the Special Immigration Appeals Commission (SIAC) and the use of Special Advocates: Seventh Report of Session 2004–05*, vol. 1 (London: Her Majesty's Stationery Office, 2005) [CAC Report]. Specifically, the European Court found that the procedure breached article 5, para. 4 of the Convention, which provides that "[e]veryone who is deprived of his liberty by arrest or detention shall be entitled to take proceedings by which the lawfulness of his detention shall be decided speedily by a court and his release ordered if the detention is not lawful."

34 CAC Report (see note 33), p. 22.

35 "Submissions of the Commission for Public Complaints Against the RCMP Regarding the Policy Review of the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar" (Written submission, Arar Commission Policy Review Public Submissions), February 21, 2005, p. 47.

36 *RCMP Act*, s. 45.34

37 *CSIS Act*, s. 55.

38 Under s. 38.03(3) of the *Canada Evidence Act*.

39 In this section, I use the term integration in a broad sense to cover coordinated operations and co-operation between agencies.

40 See transcript of Roundtable of International Experts on Review and Oversight, Arar Commission Policy Review (May 20, 2005), online, http://www.stenotran.com/commission/maherarar/2005-05-20%20International%20Roundtable.pdf; Transcript of Roundtable of Canadian Experts on Review and Oversight, Arar Commission Policy Review (June 10, 2005), online, http://www.stenotran.com/commission/maherarar/2005-06-10%20Canadian%20Roundtable.pdf (both accessed Aug. 14, 2006). These transcripts are also available on the CD that accompanies this Report.

41 See discussion in Chapter V.

42 Under the "Passenger Protect" program, which emerged from the *Public Safety Act, 2002*, S.C. 2004, c. 15.

43 S.O.R./2001-360 and S.O.R./99-444, discussed in Chapter V.

44 *R. v. Cook*, [1998] 2 S.C.R. 597.

45 Auditor General's 2003 report (see note 4), para.10.162.

46 Ibid., p. 41.

[47] Canada, Privy Council Office, *Securing an Open Society: Canada's National Security Policy* (Ottawa: Privy Council Office, 2004), p. 19, online, http://www.pco-bcp.gc.ca/docs/Publications/NatSecurnat/natsecurnat_e.pdf (accessed Aug. 9, 2006) [*Securing an Open Society*].

[48] Ibid., p. 20.

[49] For simplicity, I use the term "integrated review" rather than "integrated or co-operative review." Although I recognize that some of the procedures I recommend are arguably more in the nature of co-operation than integration, I do not think it is necessary to distinguish between the two.

[50] *Securing an Open Society,* p. 19.

XII
Policy Review Process

1.
INTRODUCTION

The Policy Review mandate requires me to make recommendations ". . . on an independent, arm's-length review mechanism for the activities of the Royal Canadian Mounted Police with respect to national security based on (i) an examination of models, both domestic and international, for that review mechanism, and (ii) an assessment of how the review mechanism would interact with existing review mechanisms. . .."

At the outset, I determined that I would benefit from a research-based, consultative process for this mandate. Clearly, the process required for the Policy Review was different from that necessary for the Factual Inquiry, the part of my mandate relating to what happened to Mr. Arar. For the Policy Review, it made sense to proceed in a much more informal and consultative manner. It was necessary to obtain information and submissions from a broad range of sources, including the institutions that would be affected by my recommendations, individuals with expertise in the area of national security, and public interest groups.

2.
GUIDING PRINCIPLES

In establishing the process for the Policy Review, I used four guiding principles and a variety of procedural mechanisms in order to gather as much information as possible and to involve all of those who were interested in participating in the process.

The four guiding principles were: openness/accessibility, thoroughness, fairness and expedition.

2.1 OPENNESS/ACCESSIBILITY

This is a public inquiry and it was essential that the proceedings be as transparent and open to the public as possible. With that in mind, my counsel and I developed a process that at each stage kept the public fully informed and involved. We did this by publishing background and consultation papers and by maintaining regular communications with the various parties who expressed an interest in participating in the process. We made extensive use of our website and e-mail correspondence.

In addition to keeping the public informed, we also invited public participation throughout the process. We regularly invited comment on our research and on our background and consultation papers, and received many helpful observations and submissions.

In the end, I am satisfied that the Policy Review process was fully transparent and open to the public and that all of those agencies, institutions and individuals who wished to participate in the process were given an opportunity to do so.

2.2 THOROUGHNESS

There were a number of challenging questions that were integrally linked to the Policy Review mandate. These questions required extensive information-gathering and analysis in order to thoroughly address the mandate and to make considered recommendations to the Government.

These questions included the following:

1. What are the RCMP's national security activities?
2. What are the characteristics of the RCMP's national security activities that could lead to a conclusion that they require a review mechanism?
3. What is a review mechanism, and how does it differ, if at all, from an oversight or other accountability mechanism?
4. What review, oversight and/or other accountability mechanisms currently apply to the RCMP's national security activities, and how adequately do they achieve their objectives?
5. With whom and to what extent are the RCMP's national security activities integrated?
6. What impact could the integration of the RCMP's activities have on the conception and design of a review mechanism?
7. How are other police forces in Canada reviewed?

8. How are security intelligence agencies in Canada reviewed?
9. How are police forces and security intelligence agencies in other countries reviewed?
10. What can we learn from these domestic and international review models?

Certain of these questions derived directly from the Government's direction that I base my recommendations in part on an examination of domestic and international review models. This examination was necessarily wide-ranging, as Canadian and foreign jurisdictions offer many different review models and features.

The Government also directed that I base my recommendations on an assessment of how a review mechanism for the RCMP's national security activities would interact with existing mechanisms. Given the integration of the RCMP's national security activities with those of other federal and provincial actors, and the number of review and other accountability mechanisms in the federal and provincial spheres in Canada, this direction necessarily entailed extensive information gathering.

Certain of these questions also reflected the fact that the RCMP's national security activities are policing activities that have some features in common with security intelligence activities, but that also have features that are unique to a law enforcement agency. It was therefore important that I not only learn about these activities in detail, but also that I consider the applicability of review mechanisms for both law enforcement and security intelligence agencies.

2.3
FAIRNESS

The principle of fairness is inextricably linked to the principle of openness and accessibility. I wanted to ensure that any individual or organization that wished to contribute to the Policy Review had a meaningful opportunity to do so. I therefore permitted written submissions in any format,[1] and I extended submission deadlines, both formally and informally. By "informally," I mean that I did not reject any submissions because they were received beyond a deadline. Indeed, I gave careful consideration to all submissions.

I also endeavoured to keep the public informed of the material information and issues that I was considering, not only to solicit comments, but also in the interest of fairness to the public. The "public" I refer to includes a number of organizations that could be affected by my recommendations. I considered it important that these organizations had a full opportunity to present any information or viewpoints as they saw fit.

Finally, I provided everyone involved with opportunities to respond to the comments and submissions of others.

2.4 EXPEDITION

To be effective, a public inquiry must be expeditious. Expedition in the conduct of a public inquiry makes it more likely that members of the public will be engaged by the process and that they will feel confident that the issues are being appropriately addressed. Since public inquiries typically involve pressing and substantial public-policy questions, the public is also better served by an inquiry that proceeds in a timely manner.

With this principle in mind, I decided to proceed with the Factual Inquiry and the Policy Review simultaneously. I established two distinct processes, largely with separate staff. I made this decision to proceed concurrently with both parts of the Inquiry for another reason as well. The substantive scope of the issues in the Policy Review differed from the Factual Inquiry's examination of a specific set of events. The Policy Review was a broad-ranging inquiry into the objectives of designing a review mechanism, the characteristics of national security policing by the RCMP, the interaction between Canadian accountability actors, the implications of Canada's constitutional division of powers, and many other subjects. There was no compelling reason, in my view, to delay information gathering and consideration of these substantial issues until I had completed my Factual Inquiry. While portions of the evidence in the Factual Inquiry were relevant to my Policy Review mandate, I viewed that an ongoing Policy Review process could take account of this evidence while it continued gathering information. Indeed, as the Factual Inquiry proceeded, it became clear to me that any information that was relevant to the Policy Review was being heard in public, and could therefore inform the public's contributions. In the end, the Factual Inquiry's evidentiary proceedings ended before the Policy Review's final hearings and final reply submissions. I am confident that there was ample opportunity for consideration in the Policy Review of any relevant Factual Inquiry evidence.

3.
PROCESS

3.1
APPOINTMENT OF ADVISORY PANEL

Early in the Policy Review process, I appointed an Advisory Panel of leading academics and former practitioners in the fields of law enforcement, security intelligence and government policy. In selecting members of the Panel, I tried to ensure that they would represent a diversity of expertise and perspective to help me in fulfilling my Policy Review mandate.

I met with the Advisory Panel regularly. I consulted them on the planning and content of all Policy Review publications, and on my continuing analysis of the questions posed by the Policy Review mandate. My counsel and I also drew on their expertise to carry out and assess the results of our extensive information gathering, the Expert Roundtables and the public hearings (all described below). Near the end of the Policy Review process, my counsel and I also held a two-day workshop with the Advisory Panel to gather their observations and views on the direction that my recommendations should take.

The thoughtful contributions of the Advisory Panel informed both my procedural and substantive decision making in the Policy Review. I am deeply appreciative of their expert assistance, and of the time and effort that they dedicated to the Policy Review.

The Advisory Panel consisted of the following individuals:

Monique Bégin was Minister of Health and Welfare between 1977 and 1984. Prior to that she served as Minister of Revenue, and in that capacity she dealt with the issue of money laundering in Canada. A sociologist by training, Ms. Bégin was from 1990 to 1997 Dean of the Faculty of Health Sciences at the University of Ottawa. She also served as co-Chair of the Ontario Royal Commission on Education from 1993 to 1994. Currently she is Professor Emeritus, and visiting professor at the University of Ottawa School of Management. She is an officer of the Order of Canada.

Alphonse Breau was Assistant Commissioner in the Royal Canadian Mounted Police. During his distinguished career, which spanned 38 years, Mr. Breau served as commanding officer in "C" Division of the Force in Québec (1988 to 1994), focusing on organized crime, drugs, customs and excise, and criminal intelligence. From 1995 until 1997, Mr. Breau was Chief Investigator for the International Criminal Tribunal for Rwanda.

Kent Roach teaches law and criminology at the University of Toronto. A graduate of Yale University and the University of Toronto, Professor Roach's teaching and research include the criminal process, the Charter, Aboriginal rights, the role of the courts, anti-terrorism and the legal profession. He is the author of *September 11: Consequences for Canada* published in 2003, as well as co-editor of *The Security of Freedom: Essays on Canada's Anti-terrorism Bill*, published in 2001.

Martin Rudner is a professor at The Norman Paterson School of International Affairs, Carleton University, Ottawa, and Director of its Canadian Centre of Intelligence and Security Studies. A graduate of McGill, Oxford and Jerusalem universities, Professor Rudner's current research interests include intelligence studies and international terrorism. He has served as a consultant and advisor to several government departments and agencies. Among his many scholarly publications is his article, "Challenge and Response: Canada's Intelligence Community in the War on Terrorism."[2]

Reg Whitaker is Distinguished Research Professor Emeritus at York University, where he taught political science from 1984 to 2001. He is currently Adjunct Professor of Political Science at the University of Victoria. He received a PhD in political economy from the University of Toronto and has since received several academic honours, including an Isaac Walton Killam Research Fellowship. He has authored several books, most recently *Canada and the Cold War*, published in 2003, and *The End of Privacy: How Total Surveillance is becoming a Reality,* published in 1999. He has authored several scholarly articles on issues of security and intelligence, and he is often called upon to comment on public affairs for the media.

3.2
INFORMATION GATHERING AND PUBLIC CONSULTATIONS

3.2.1
Initial Information Gathering and Publications

With the assistance of my Advisory Panel and counsel, I identified the many questions that my Policy Review mandate posed, and the areas in which I would need to gather information and seek public input.

In June 2004, the Commission published a List of Issues and an Outline for a Consultation Paper, in order to initiate a public discussion about the Policy Review. We solicited public comment on these documents, and published amended versions based on those comments, which are included in the CD that accompanies this Report; they are also available on the Commission's website,

www.ararcommission.ca, which I understand the Government will maintain for several years after the release of this Report.

Our first major step was the publication of a Consultation Paper in October 2004 to promote and assist public discussion. The Consultation Paper summarized the principal issues and relevant information in the Policy Review, and was based on much more detailed information and analysis provided in eight Background Papers. It also set out a number of options for review of the RCMP's national security activities, which included possibilities ranging from the status quo, to an enhanced Commission for Public Complaints Against the RCMP or Security Intelligence Review Committee (SIRC), to a SIRC-style agency for all federal national security activities.

The Background Papers on which the Consultation Paper was based were published in December 2004, and are available on the Commission's website. Those papers canvassed a broad array of topics, including the RCMP's national security activities, domestic and international review models for law enforcement and security intelligence, theories of accountability and police independence, and national security and human rights and freedoms. The papers were based on research and on extensive direct information gathering with a number of Canadian departments, agencies and groups, which I have listed in Appendix A. The information gathering included meetings, written questions and answers, and document requests.

This information gathering continued throughout the duration of the Policy Review. It informed my deliberations and my public consultations, periodically leading to the publication of further documents, discussed below.

I wish to thank the representatives of all of the agencies and organizations with whom the Policy Review conducted its information gathering. Some of these agencies, including the RCMP, CPC, CSIS, SIRC and the Office of the CSE Commissioner, met with my counsel and members of the Advisory Panel several times, and provided many documents and written answers to our questions. Their efforts were of great assistance to this Inquiry.

The initial Consultation Paper of October 2004 was republished, with amendments, in December 2004. The Consultation Paper is included on the CD which accompanies this Report; it is also available on the Commission's website.

3.2.2 Public Input

In response to my call for comments on the Consultation Paper and Background Papers, I received numerous written submissions from various government agencies and institutions and the public throughout the winter and spring of 2005.

Some of these submissions addressed discrete Policy Review issues; others included comprehensive proposals for a review mechanism; and others concentrated on communicating valuable operational information or matters of principle to me. I also received several supplementary and reply submissions through the end of 2005, often in response to detailed questions that I posed to the public. These questions were set out in several Policy Review documents published in 2005; they are included on the accompanying CD and are also available on the Commission's website.

I thank each of the Policy Review participants who made these submissions. These individuals and organizations are listed in Appendix B.

3.3
FURTHER INFORMATION GATHERING AND PUBLICATIONS

3.3.1
Integrated Nature of the RCMP's National Security Activities

Commission counsel held several meetings with the RCMP, including the Force's integrated teams, to advance our understanding of the integrated nature of their national security operations. We also held a number of meetings with other national security actors whose activities are integrated with those of the RCMP. These agencies included CSIS, the CBSA, FINTRAC, ITAC, Transport Canada, CIC, DFAIT and the municipal police forces.

On June 14, 2005, the Commission published a Supplementary Background Paper on the RCMP and National Security Activities. This paper is available on the Commission's website.

We also expanded our information gathering to other federal national security actors, whether or not their activities were formally or substantially integrated with those of the RCMP. This was in part a consequence of some written submissions that advocated a review agency with jurisdiction over all federal national security actors. While in the end I did not opt for this model for reasons that I set out in my Recommendations Chapter, it was important that I carry out necessary information gathering in order to canvass all possible alternatives. The results of that research are set out in Chapter V of the Report.

3.3.2
International Models

My mandate specifically directed me to examine international models for the review of national security activities. Information gathering and consultation with international review bodies were an important element of my process. I

selected eight countries with liberal democratic traditions, including three with which Canada shares Westminster parliamentary institutions: Australia, New Zealand and the United Kingdom. The other countries were Belgium, Germany, Norway, Sweden and the United States. All had institutional arrangements or experience with review and oversight of law enforcement and security intelligence activities that I thought could be instructive. These countries had also variously instituted new security and counter-terrorism measures in the wake of the events of September 11, 2001; new measures to address domestic and foreign integration of national security activities; and/or new review and oversight measures.

In these eight countries, I examined the principal review and oversight bodies of both the law enforcement and security intelligence agencies. It was important to survey, at least initially, mechanisms that carried out review of either police forces or security intelligence agencies;[3] and mechanisms that carried out review functions, irrespective of the vocabulary — review, oversight or other term — commonly used to describe those agencies.[4]

Once we had identified the principal review and oversight mechanisms in these eight countries, we gathered information by consulting governing statutes; annual and other reports and publications; the agencies' websites and links; related government publications and literature such as proposed bills and formal government responses to reports; and academic, media and other publications. This process allowed me to identify and study in detail the features of these review and oversight agencies, including their respective jurisdiction, mandate, functions, powers, limitations, composition and appointment process. To better understand these institutions, and to assess the instructiveness or potential applicability of their features, I also studied to varying degrees the respective constitutional, governmental, historical, policing and security intelligence milieus, including any recent developments in counter-terrorism powers and new accountability mechanisms.

After publishing this information in the December 2004 Background Paper on International Models, I identified certain foreign review agencies that warranted more detailed examination. These were largely review agencies that appeared to be at arm's length from government, and that had jurisdiction over police forces engaged in national security activities. In some cases, this supplementary research also touched on agencies that review intelligence services, either because the agencies have jurisdiction over both intelligence and police forces, or because there were statutory features that merited further examination.

My counsel met with selected agencies and individuals, either in person or by telephone. Detailed questions were sent to the agencies in advance to

facilitate the meetings. In many cases, the agencies provided detailed responses and also answered many follow-up questions. A list of these agencies and persons can be found in Appendix C.

The information gathered from these meetings was summarized in a "Supplementary Background Paper: International Models," which was published in May 2005. This paper is available on the Commission's website.

I wish to thank the representatives of the foreign agencies who assisted us. These individuals gave generously of their time. Their contributions to the Policy Review and to the Canadian public interest were valuable, and I am grateful for their assistance.

3.3.3 Invitations for Comment from Provincial/Municipal Actors

Since the RCMP's national security activities are integrated with certain provincial and municipal police forces, recommendations for a review mechanism could impact members of these police forces, as well as the review bodies for these forces. I therefore invited comments from the chiefs of police for numerous provincial and municipal police forces, each of the review bodies for these forces, and the provincial and territorial attorneys general.

In general, these institutions declined to participate and/or preferred to await any governmental consultations that may follow my recommendations. However, the Canadian Association of Chiefs of Police, the Ontario Provincial Police and the Ottawa Police Service actively participated in the Policy Review; the Toronto Police Service provided assistance with information gathering; and numerous provincial review bodies assisted during our research for the Consultation Paper and Background Papers.

3.3.4 Review of Certain Factual Inquiry Evidence

Portions of the Factual Inquiry evidence were relevant to the Policy Review mandate, because they helped illustrate certain features of the RCMP's national security activities. I therefore discussed relevant parts of the Factual Inquiry evidence with members of the Advisory Panel. The public was invited to comment on the relevance of the public Factual Inquiry evidence to the Policy Review. In formulating my recommendations for the Policy Review, I had regard to the Factual Inquiry evidence when I considered it helpful.

3.3.5
Roundtables

I convened two separate Roundtables of Experts on Review and Oversight, one that involved Canadian experts, and the other, international experts. For balance, I included in each of these roundtables one or more individuals with operational expertise. While the questions that each roundtable addressed were similar, the Canadian roundtable focused more on Canada-specific issues. The issues for the roundtables were set out in Background Papers that were published in advance of each roundtable. Copies of these papers are available on the accompanying CD and on the Commission's website.

These roundtables were open to the public, and were simulcast and recorded by the Cable Public Affairs Channel (CPAC). Each roundtable lasted one day. The public had an opportunity to pose questions to the roundtable participants during each of the morning and afternoon sessions. The transcripts from the roundtables are included on the accompanying CD and on the Commission's website.

I wish to express my thanks to the individuals who participated in these roundtables. I have set out a list of these individuals in Appendix D.

3.4
PUBLIC HEARINGS AND FINAL PUBLIC CONSULTATIONS

In November 2005, I convened four days of public hearings for the Policy Review. The persons who appeared at these hearings were individuals and organizations who had made written submissions. The public hearings provided an opportunity to these individuals and organizations to discuss their submissions with me directly, and to canvass, where applicable, the relative merits of their proposals for review mechanisms. Some of these participants did not advocate models, but appeared either to ensure that relevant information was presented or to answer any questions that I had.

These hearings were held in public and were simulcast and recorded by CPAC. The transcripts are available on the accompanying CD and on the Commission's website. I am grateful to those who participated in these hearings, which have added considerably to my consideration of the various review models.

I am also grateful to all those who provided written comments and replies in December 2005, in response to two final publications by the Policy Review: "Further Questions for Public Consultation," published in October 2005; and "Integrated National Security Review Committee: Further Option for Public

Comment," published in November 2005. These individuals and groups are listed in Appendix B.

4.
BUDGET

The final figure for the expenditure of the Inquiry is not yet available. However, I expect that the total amount spent for the Factual Inquiry and the Policy Review will be approximately 16 million dollars, which figure includes the amount provided to intervenors, including Mr. Arar, of approximately 1 million dollars. It is not practical to allocate between the Factual Inquiry and the Policy Review.

5.
EXPERT ADVICE

Throughout the Policy Review, I sometimes required expert advice on specific issues. In general I tried to rely on the Advisory Panel members for this advice, but from time to time it was necessary to seek outside advice and other contributions from other experts. For example, I was assisted in research and drafting of the Background Papers by Professor Martin Friedland of the Faculty of Law, University of Toronto. I also spoke to Reid Morden, the former Director of CSIS, about certain national security confidentiality issues and to Harry Swain, a former deputy minister in the federal government, about certain specific "machinery of government" issues.

6.
APPRECIATION

The Policy Review process was a very collaborative process and it benefited from the contributions of many organizations and individuals who gave their time willingly and generously. First, I would like to thank the members of my Advisory Panel: the honourable Monique Bégin, Alphonse Breau, Kent Roach, Martin Rudner and Reg Whitaker. I am deeply appreciative of their many contributions to the Policy Review process.

I was also greatly assisted by my counsel, Ronald Foerster, Freya Kristjanson and Andrea Wright, whom I commend for their first-rate work. Their contributions to the Commission's information gathering and publications, as well as to my deliberations, were outstanding.

I was also ably assisted at various stages by junior counsel, Sanjay Patil and Erin Shaw, by counsel Adela Mall and by a graduate student, Shawna Godbold. I wish to thank them for the important role that they played in the process.

Paul Cavalluzzo, lead counsel in the Factual Inquiry, provided helpful insights and suggestions throughout the Policy Review.

I would also like to express my appreciation to those involved with the administration of the Inquiry: Nicole Viau, Director, Finance and Administration, Céline Lalonde, Deputy Director, and Francine Bastien, Media Relations. The Policy Review also benefited from the administrative assistance of Gisèle Malette, Isabelle Dumas, Françoise Roy-Lalonde, Mary O'Farrell and Lise Scharf.

As he did for the Factual Inquiry, Gilles Desjardins performed his duties as Records Manager with care and efficiency.

Finally, I would like to recognize the skills and dedication of the following people: Guylaine Beauchamp (translator); Miriam Bloom of Expression Communications (publication designer); Brian Cameron of gordongroup marketing + communications (lead English editor); Carole Chamberlin of PWGSC (English editor); Jane Chapman (English editor); Pierre Cremer (translator); Tyler Gibbs of eSCAPE Marketing Solutions (Webmaster); Mélanie Lefebvre of PWGSC (fact checker); Alphonse Morissette (lead French editor); Judith Richer of gordongroup marketing + communications (English editor); Marie Rodrigue (translator and French editor); and Jean-Pierre Thouin of the University of Ottawa's Centre for Translation and Legal Documentation (translator). All of these people worked on difficult material under tight time constraints, and I thank them.

Notes

1 Electronic or hardcopy, letter or bound format

2 *Canadian Foreign Policy*, Vol. 11, No. 2 (Winter, 2004).

3 As I mentioned in the Guiding Principles section above, it was important that I consider a review mechanism for both law enforcement and security intelligence agencies, given the fact that the RCMP's national security activities have characteristics in common with both. To do otherwise would have unduly limited the scope of my examination and its potential findings.

4 The words "review" and "oversight" are used disparately, both domestically and abroad, including in translation, to describe the mandate of bodies with an accountability role over law enforcement and intelligence agencies. We did not wish to limit the scope of the examination of international models by virtue of the vocabulary used to describe particular accountability functions. We chose models for examination based on an initial identification of features, such as jurisdiction, audit power, etc. For convenience, I generally refer to these mechanisms throughout this Report as "review" agencies or models.

APPENDIX A

Canadian Departments, Agencies and Groups With Which the Arar Commission Policy Review Conducted Direct Information Gathering

British Columbia Office of the Complaint Commissioner
Canada Border Services Agency
Canada Revenue Agency
Canadian Air Transport Security Authority
Canadian Human Rights Commission
Canadian Security Intelligence Service
Citizenship and Immigration Canada
Commission for Public Complaints Against the RCMP
Communications Security Establishment
Foreign Affairs Canada and International Trade Canada (DFAIT)
Department of National Defence, Intelligence
Financial Transactions and Reports Analysis Centre
Information Commissioner of Canada
Inspector General, Canadian Security Intelligence Service
Integrated Threat Assessment Centre
Department of Justice Canada
Military Police
Military Police Complaints Commission of Canada
Office of the Communications Security Establishment Commissioner
Ontario Civilian Commission on Police Services
Ontario Provincial Police
Privacy Commissioner of Canada
Privy Council Office
Public Safety and Emergency Preparedness Canada
Quebec Police Ethics Commissioner (Commissaire à la déontologie policière)
Roberta Jamieson, former Ombudsman of Ontario
Royal Canadian Mounted Police, including:

- Criminal Intelligence Directorate
- Integrated Immigration Enforcement Team, "O" (Toronto) Division
- Integrated Border Enforcement Team, Windsor Division
- Integrated National Security Enforcement Team, "O" (Toronto) Division
- National Operations Centre
- National Security Intelligence Branch
- National Security Operations Branch

Security Intelligence Review Committee
Toronto Police Service
Transport Canada

APPENDIX B

Individuals and Organizations Who Made Submissions to the Policy Review:

Amnesty International Canada
Andrew Koczerzuk
British Columbia Civil Liberties Association
C.C. Kitteringham
Canadian Arab Federation and Canadian Council on American-Islamic Relations
Canadian Association of Chiefs of Police
Canadian Association of University Teachers
Canadian Bar Association
Canadian Civil Liberties Association
Canadian Security Intelligence Service
Clayton Ruby
Commission for Public Complaints Against the RCMP
Communications Security Establishment Commissioner
International Civil Liberties Monitoring Group
Jiarong Tsang
L.D. Cross
Maher Arar
Ontario Provincial Police
Ottawa Police Service
Privacy Commissioner of Canada
RCMP External Review Committee
Rémi Hyppia
Royal Canadian Mounted Police
Scott Burbidge
Security Intelligence Review Committee
The Redress Trust, the Association for the Prevention of Torture, and the World Organization Against Torture

Signatories to Joint Intervenors' Submmission:
Amnesty International Canada, the British Columbia Civil Liberties Association, Canadian Arab Federation, Canadian Islamic Congress, Canadian Labour Congress, Council of Canadians, Council on American-Islamic Relations (Canada), International Coalition Against Torture, International Civil Liberties Monitoring Group, Law Union of Ontario, Minority Advocacy Rights Council, Muslim Canadian Congress, Muslim Community Council of Ottawa-Gatineau, National Council on Canada-Arab Relations, Polaris Institute, The Redress Trust, Association for the Prevention of Torture, World Organisation against Torture (OMCT).

APPENDIX C

Foreign Review/Oversight Bodies, As Well As Other Persons With Whom the Commission Conducted Direct Information Gathering

Country	Institution
Australia	Commonwealth Ombudsman
Australia	Inspector-General of Intelligence and Security
Belgium	Permanent Committee for the Control of Intelligence Services (Committee I)
Belgium	Standing Police Monitoring Committee (Committee P)
Germany	G-10 Commission
Germany	Parliamentary Control Panel
New Zealand	Inspector-General of Intelligence and Security
New Zealand	Police Complaints Authority
Norway	Parliamentary Intelligence Oversight Committee (EOS Committee)
Sweden	Parliamentary Ombudsmen's Office
Sweden	Records Board
United Kingdom	Independent Police Complaints Commission
United Kingdom	Interception of Communications Commissioner
United Kingdom	Investigatory Powers Tribunal
United Kingdom	Her Majesty's Inspectorate of Constabulary
United Kingdom	Office of the Surveillance Commissioners
United Kingdom (Northern Ireland)	Police Ombudsman for Northern Ireland
United States	Office of the Inspector General, Department of Justice
United States	Office of the Inspector General, Central Intelligence Agency
United States	Office of the Inspector General, Department of Homeland Security

Others:

Iain Cameron, Professor in Public International Law, University of Uppsala, Sweden

Laurence Lustgarten, Professor of Law, Southampton University, and Commissioner, Independent Police Complaints Commission, England and Wales

Fredrik Sejersted, Attorney at Law, Office of the Attorney General (Civil Affairs), Norway

APPENDIX D

Roundtable of International Experts on Review and Oversight, May 20, 2005

Hans Born, Senior Fellow, Geneva Centre for the Democratic Control of Armed Forces, Switzerland

Iain Cameron, Professor in Public International Law, University of Uppsala, Sweden

Marina Caparini, Senior Fellow, Geneva Centre for the Democratic Control of Armed Forces, Switzerland

Peter Gill, Professor in Politics and Security, Liverpool John Moores University, U.K.

Ian Leigh, Professor of Law, Durham University, U.K.

Nuala O'Loan, Police Ombudsman for Northern Ireland, U.K.

Roundtable of Canadian Experts on Review and Oversight, June 10, 2005

Warren Allmand, consultant in international human rights

Reem Bahdi, Assistant Professor, University of Windsor Faculty of Law

Gwen Boniface, Commissioner, Ontario Provincial Police

Alan Borovoy, General Counsel, Canadian Civil Liberties Association

Stuart Farson, Professor of Political Science, Simon Fraser University

Norman Inkster, Partner, Gowlings Consulting Inc.

Dirk Ryneveld, British Columbia Police Complaints Commissioner

Wesley Wark, Professor, University of Toronto's Munk Centre for International Studies

APPENDIX E
Policy Review Publications*

List of Issues for Public Consultation (June 17, 2004)
Outline of Consultation Paper (June 17, 2004)
Consultation Paper (October 5, 2004; amended December 14, 2004)
Background Papers to the Consultation Paper (December 10, 2004):

- The RCMP and National Security
- Statutory Framework for the Activities of the RCMP with Respect to National Security
- National Security and Rights and Freedoms
- Accountability and Transparency
- Police Independence
- Domestic Models of Review of Police Forces
- Accountability of Security Intelligence in Canada
- International Models of Review and Oversight of Police Forces and Security Intelligence Agencies

Supplementary Background Papers:

- International Models of Review of National Security Activities: A Supplementary Paper to the Commission's Background Paper on International Models (May 2005)

Roundtable Background Papers:

- Questions for Panel Members: A Background Paper to the Commission's Roundtable of International Experts on Review and Oversight (May 19, 2005)
- Questions for Panel Members: A Background Paper to the Commission's Roundtable of Canadian Experts on Review and Oversight (June 2005)

Further Questions for Public Consultation (October 17, 2005)
Integrated National Security Review Committee: Further Option for Public Comment (November 25, 2005)

---

* Some of these publications are available on the accompanying CD (see Appendix F for list), and all are available on the Commission's website, www.ararcommission.ca.

APPENDIX F
Policy Review Documents on Accompanying CD

Notices and Information

December 19, 2005 – List of Submissions received as of December 19, 2005

August 19, 2005 – Notice re Funding for October 11-14 Policy Review Public Hearings

May 30, 2005 – Notice re Roundtable of International Experts on Review and Oversight and Roundtable of Canadian Experts on Review and Oversight

May 5, 2005 – Notice re Commissioner O'Connor's Examination of International Review Models

December 14, 2004 – Call for Submissions

October 5, 2004 – Publication of Consultation Paper.

Roundtables

Roundtable of International Experts on Review and Oversight, May 20, 2005:

- Notice re Roundtable
- Programme
- Biographical Information of Experts
- Background Paper to the International Roundtable
- Original Transcript

Roundtable of Canadian Experts on Review and Oversight, June 10, 2005:

- Notice re Roundtables
- Programme
- Biographical Information of Experts
- Background Paper to the Canadian Roundtable
- Original Transcript

Public Hearings

Schedule of Appearances, November 15-18, 2005

Transcripts of the Public Hearings

Process

Process description

Documents

November 25, 2005 – Integrated National Security Review Committee: Further Option for Public Comment

October 17, 2005 – Further Questions for Public Consultation

December 14, 2004 – Amendments to the Consultation Paper

October 5, 2004 – Consultation Paper

June 17, 2004 – Outline of Consultation Paper

June 17, 2004 – List of Issues for Public Consultation