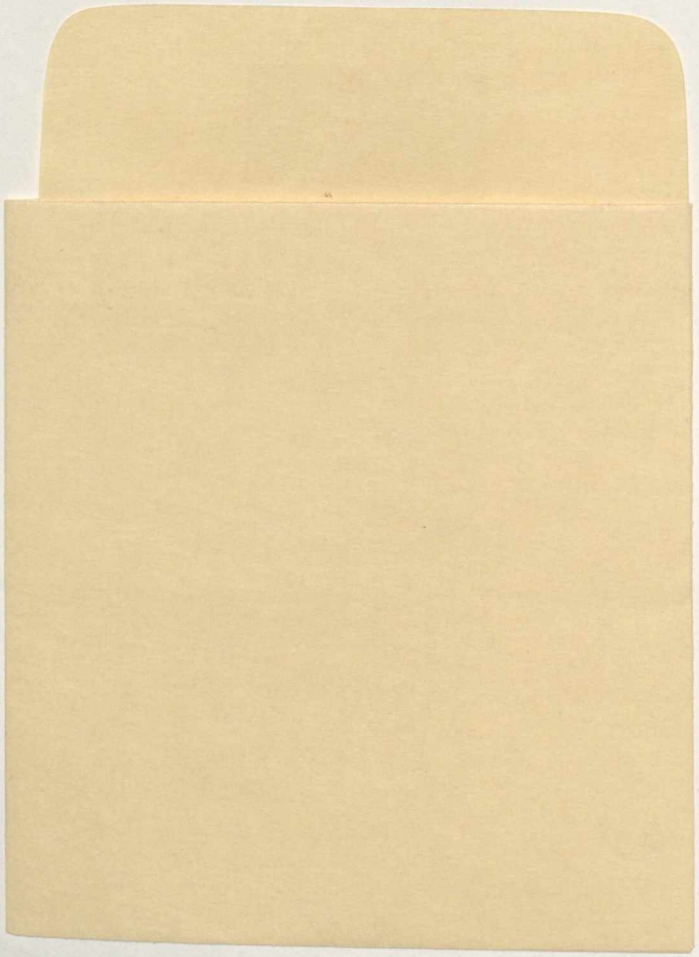
IN FLUX
BUT NOT IN CRISIS

Report of the Special Committee

ON THE REVIEW OF THE CSIS ACT
AND THE SECURITY OFFENCES ACT



IN FLUX
BUT NOT IN CRISIS

A Report of the House of Commons
Special Committee
on

The Review of the *Canadian Security Intelligence Service Act*
and the *Security Offences Act*

September 1990

Published under authority of the Speaker of the House of Commons by the Queen's Printer for Canada
Available from the Canadian Government Publishing Center, Supply and Services Canada, Ottawa, Canada K1A 0S9

The Special Committee on the Review of the *Canadian Security Intelligence Service Act* and the *Security Offences Act*

has the honour to present its

REPORT

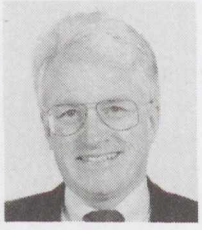
In accordance with its mandate under the Order of Reference dated Tuesday, June 27, 1989, your Committee has undertaken a comprehensive review of the *Canadian Security Intelligence Service Act* and the *Security Offences Act* and reports the following:

MEMBERS OF THE COMMITTEE

Blaine Thacker,
Chairman

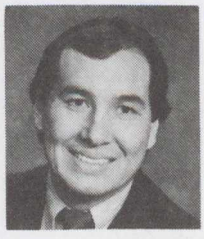
Maurice Tremblay,
Vice–Chairman

Ken Atkinson



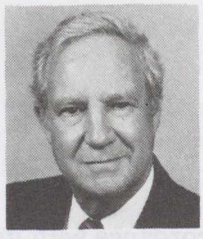
John Brewin

Derek Lee



Wilton Littlechild

George Rideout



Jacques Tétreault

* Other Members who served on the Special Committee by virtue of Standing Order 114(3) were: Robert Horner, Carole Jacques, Robert Kaplan, John Nunziata, Brian O'Kurley, Svend Robinson, Robert Skelly and Robert Wood.

COMMITTEE PERSONNEL

Director of Research

Stuart Farson

Project Co–ordinator

Philip Rosen
Research Branch
Library of Parliament

Research Associates

François Cadieux

Brian Gorlick

Research Assistant

Peter Niemczak
Research Branch
Library of Parliament

Clerks of the Committee

Donald Reid

Charles Robert

Administrative Assistant

Diane Harper

Secretaries to the Committee

Josée Deschênes

Diane Gagnon–Beaupré

Editors

Kathryn Randle

Georges Royer

Graphic Designer

Tom Littlemore

ORDERS OF REFERENCE

Tuesday, June 27, 1990

By unanimous consent, it was ordered, — That, pursuant to Section 56 of the Canadian Security Intelligence Service Act and Section 7 of the Security Offences Act, a Special Committee of the House of Commons be appointed to be the Committee to undertake a comprehensive review of the provisions and operation of the Canadian Security Intelligence Service Act and, that, the Committee be empowered to meet after July 16, 1989, and report back to the House no later than July 16, 1990;

That the Committee have all of the powers of a Standing Committee; and

That the membership of the Committee shall be composed of Mr. Thacker as Chairman, and Messrs. Brewin, Horner, Lee, Littlechild, Nunziata, Tremblay (Lotbinière) and Tétreault.

Wednesday, March 14, 1990

By unanimous consent, it was ordered, — That the Special Committee on the Review of the Canadian Security Intelligence Service Act and the Security Offences Act be authorized to travel to Washington, D.C. for the period from Tuesday, March 20, 1990 to Thursday, March 22, 1990 for the purpose of holding discussions respecting security intelligence administration and structure, and that the necessary staff do accompany the Committee; and

That the Committee be authorized to travel to Vancouver for the period from Sunday, March 25, 1990 to Wednesday, March 28, 1990 for the purpose of hearing evidence related to the Committee's Order of Reference and of visiting regional police and security facilities, and that the necessary staff do accompany the Committee.

Wednesday, June 13, 1990

By unanimous consent, it was ordered, —That, further to Order made June 27, 1989, the Special Committee on the review of the Canadian Security Intelligence Service Act and the Security Offences Act report no later than the first normal sitting day after Labour Day, 1990.

ATTEST

ROBERT MARLEAU

The Clerk of the House of Commons

ACKNOWLEDGEMENTS

Many people contributed their labour to the comprehensive review conducted by the Committee of the provisions and operation of the *Canadian Security Intelligence Service Act* and the *Security Offences Act*. Those who made written and oral submissions to the Committee played an important role in assisting it to formulate the conclusions and recommendations set out in this Report.

The successful completion of a complex, sensitive task such as the one assigned to this Committee requires the assistance of dedicated expert staff. The Committee had such assistance. Stuart Farson, the Committee's Director of Research, facilitated and inspired our work with his expertise, determination and impressive grasp of complex issues. The Committee's Project Co–ordinator, Philip Rosen, Senior Analyst with the Research Branch of the Library of Parliament, put his extensive experience and organizational skills into the conduct of this review. François Cadieux and Brian Gorlick, the Committee's Research Associates, brought enthusiasm to the many valuable research tasks they were called upon to carry out. Peter Niemczak, from the Research Branch of the Library of Parliament, provided the Committee with a summary of its evidence and performed a number of important research tasks. An analysis of some of the *Charter* issues to which the *CSIS Act* may give rise was prepared for the Committee by L.A. Vandor of the law firm McMaster, Meighen.

The Centre for Legislative Exchange set up with efficiency and dispatch an impressive program for the Committee's meetings in Washington, D.C. Anne Harris provided the Committee with valuable liaison assistance when it visited Vancouver.

This Report benefited from the considerable editing skills of Kathryn Randle and Georges Royer.

During the course of this comprehensive review, the Committee had the support of the logistical and administrative skills of two able Clerks: they were Don Reid and Charles Robert.

The Committee would like to thank the staff of the House of Commons Committees Directorate, the Translation Bureau of the Secretary of State and the other services of the House of Commons that provided administrative and technical support.

Finally, assistance was provided to the Committee by the members and staff of the Security Intelligence Review Committee, the Secretariat of the Ministry of the Solicitor General (especially the *CSIS Act* Review Division of the Police and Security Branch); the Office of the Inspector General of CSIS; the Director and members of CSIS; and the Commissioner and members of the RCMP (especially those involved with the National Security Investigations Directorate and the Special Emergency Response Team).

TABLE OF CONTENTS

FOREWORD

The Special Committee on the Review of the *Canadian Security Intelligence Service Act* (*CSIS Act*) and the *Security Offences Act* was established by an Order of the House of Commons dated June 27, 1989. This Order required the Committee to undertake a comprehensive review of the provisions and operation of both the *CSIS Act* and the *Security Offences Act* and to report its findings to the House of Commons. These findings are the subject of this Report.

The mandate under which the Committee proceeded was legislatively required by Parliament in 1984 when it adopted both the *CSIS Act* and the *Security Offences Act*. While not constituting sunset clauses in the strict sense, both statutes called for parliamentary review of their provisions and operation after five years, a point that was reached on July 16, 1989. Although a relatively recent development, legislation has from time to time required parliamentary review after an initial period of implementation and experience. This is one part of the continued development of Canadian parliamentary institutions, through which the role of parliamentarians in the consideration and review of policy and legislation has been strengthened and reinforced.

The comprehensive review undertaken by this Committee, while an integral part of the continued development of parliamentary institutions, had its own unique difficulties. The task facing this Committee was to undertake a comprehensive review in a public forum – Parliament – of legislation and agencies that believe they function most effectively when they are shielded from exposure to public scrutiny. This challenge was faced not only by the Committee itself but also by those it was mandated to review. All of those involved in this comprehensive review understood the challenge, but not all of the difficulties encountered in meeting it were resolved satisfactorily. It is hoped that this Report and the recommendations it contains will, in the long run, build confidence between Parliament and the security and intelligence community. The result will be a more effective and accountable security and intelligence community, to the benefit of all Canadians.

CHAPTER ONE

Introduction

1.1 A Unique Canadian Model

The *Canadian Security Intelligence Service Act* (*CSIS Act*)[1] and the *Security Offences Act*,[2] adopted in 1984, established a uniquely Canadian model in the security and intelligence area. The security intelligence agency is given a legislative mandate in which its powers are defined, provision is made for control and direction, and review structures are put in place. Direction of the Canadian Security Intelligence Service (CSIS) is the responsibility of the Solicitor General, while judicial control of recourse to intrusive means of investigation is exercised by the Federal Court. The Inspector General of CSIS acts as the Solicitor General's agent in relation to the Service, while the Security Intelligence Review Committee (SIRC) acts in a dual role as both a review body and a complaints tribunal. Parliament performs a limited role in this area by its consideration of Estimates and SIRC's Annual Report. In relation to security offences, the Attorney General of Canada is enabled to exercise prosecutorial authority, while the RCMP is empowered with primary investigatory authority. This uniquely Canadian model will be described in greater detail later in this Report. But first, the historical context from which the present security and intelligence model emerged will be set out.

1.2 Some History

The review conducted by this Committee is the most recent of a series of inquiries concerning security and intelligence conducted in Canada during the Post-World War II era. The first was the 1946 Royal Commission on Espionage, presided over by Justices Kellock and Taschereau of the Supreme Court of Canada, set up as a result of the Gouzenko revelations of a Soviet spy ring in Canada. A number of prosecutions and convictions under the *Criminal Code* and the *Official Secrets Act* for conspiracy and espionage resulted from this early series of events in what later became the Cold War.

In 1966, Commissions of Inquiry concerning the Spencer and Munsinger affairs examined possible violations of the *Official Secrets Act*. They concluded there was no such violation in either instance, although each case had certain security implications. Also established in 1966, the Royal Commission on Security (Mackenzie Commission) issued its report in 1969. It made a number of recommendations in relation to the security of assets and vetting of personnel. It also recommended the creation of a civilian security agency, but its recommendation was not accepted by the government of the day, which decided instead to increase the number of civilian members of the RCMP's Special Branch (Security Service).

The events surrounding and following the October crisis of 1970 and the revelations growing out of them led in the late 1970s to the formation of the Keable Commission by the Quebec government and of the McDonald Commission by the Federal government, both of which reported in 1981. Also in 1981, the Quebec government released the Duchesne Report on the October crisis. The McDonald Commission recommended that a civilian security intelligence service be established under statute by Parliament. It was to be circumscribed by a number of mechanisms providing for direction, control and review.

The government of the day accepted the major thrust of the McDonald Commission recommendations and, in 1983, based on the work of the Security Intelligence Transition Group, tabled Bill C-157 in the House of Commons. The Bill provoked a critical public outcry and, consequently, a Special Senate Committee chaired by Senator Michael Pitfield was established to examine it. The Special Senate Committee made a number of recommendations for changes to Bill C-157, which the Government adopted when it introduced Bill C-9 in 1984. After tumultuous consideration both in committee and in the House of Commons, Parliament enacted Bill C-9 in June 1984. That Bill is now the *CSIS Act* and the *Security Offences Act*, as well as a number of related transitional and consequential legislative provisions.

During its first three years of operation, CSIS ran into a number of difficulties. It was criticized for the slow pace of transition. There were complaints about its language policies and practices. The Security Intelligence Review Committee set out a number of criticisms of CSIS in its first three annual reports. In the *Atwal* case, criminal charges had to be dropped because of irregularities in CSIS's warrant application.

In July 1987, the Solicitor General (the Honourable James Kelleher) appointed an Independent Advisory Team (IAT) headed by Gordon Osbaldeston, a former Clerk of the Privy Council, to advise him on the implementation of SIRC's recommendations concerning counter-subversion and civilianization. In September 1987, the first Director of CSIS, Ted Finn, resigned because of the alleged *Atwal* warrant irregularities and was replaced by Reid Morden, the current Director. In November 1987, the Solicitor General released the Independent Advisory Team's report and announced acceptance of its recommendations.

As CSIS was going through its internal changes, there were also developments internationally. Terrorism, for example, has emerged as a serious concern since the late 1960s. Many international and national conflicts have yielded terrorist incidents. Canada has not been immune to this development. There have been a number of instances where conflicts outside Canada have manifested themselves on Canadian soil, with serious injury and loss of life. This was one reason for the establishment of a Special Senate Committee on Terrorism and Public Safety, under the chairmanship of Senator William Kelly, which published its first report in July 1987. A second such Committee was formed in the present Parliament following an April 1989 hijacking incident on Parliament Hill; it published its report in June 1989.

1.3 A Time of Change

The change, reform and uncertainty that characterize the beginning of the 1990s, the last decade of this millennium, furnished their own challenge to the work of the Committee. This period of flux affects both the international and the Canadian political situation, as well as Canada's security and intelligence community.

Changes in ideology and political hegemony undreamed of in recent times are under way in many parts of the world, especially in Central and Eastern Europe and in the Soviet Union. Other parts of the world are also experiencing political change and upheaval, while elsewhere there is little or no reflection of this political turmoil and effervescence.

Long-held political beliefs and alliances are today in question, if not in actual mutation. Professor Jacques Levesque (University of Montreal) told the Committee during his appearance that the Warsaw Pact is coming undone militarily, in large part because of the political changes occurring within its member states. Professor Franklyn Griffiths (University of Toronto) told the Committee that Soviet-style systems are coming unravelled because they are unsustainable socially, economically and environmentally. Professor Paul Marantz (University of British Columbia) asserted that in Eastern Europe there will be a movement away from communism to new systems guided by each country's past experience. He characterized this not as the end of history, but as the rebirth of history.

It is not clear how this period of political flux will turn out. Certainly, the "end of history" is not upon us, although another historical epoch may be unfolding. It is difficult to foresee what will evolve from this period of uncertainty and unpredictability. It is certain that there will be change, although its extent is unclear. A reversion to the polarization of the Cold War is unlikely. Jeane J. Kirkpatrick said cautiously in a recent article in *Foreign Affairs*, "The Cold War is over — nearly. The post war era is finished — absolutely". The July 1990 meeting of NATO in London was more definitive on this issue. It is to be hoped that a period of rigidity and closed societies will not be replaced by ethnic, national and regional rivalry or conflict.

It is clear to the Committee that this period of unprecedented change on the international scene does not mean that some security and intelligence capacity is no longer necessary. Quite the contrary, it means that a security and intelligence capacity must be more flexible and even more capable of anticipating and understanding change than ever before.

CSIS itself is in flux and has been so particularly since 1987 when the new Director was named and the Independent Advisory Team's recommendations were accepted by the Government. Most, but not all, the recommendations made by IAT are in place. The impact of these changes has been felt throughout the Service. They will be discussed in the Report against the background of dynamic change in world affairs.

1.4 How the Committee Conducted the Comprehensive Review

Because of the unique challenges facing the Committee and the subject matter it was mandated to review, the Committee developed and applied a number of strategies and investigative techniques to supplement and complement its public hearings. While hearing from Canadians was essential to this comprehensive review, the complexity and sensitivity of the issues under consideration dictated the need for other methods of investigation and information gathering as well. The Committee's consideration of the matters dealt with in this Report brought many difficult issues to the attention of Canadians.

The Committee inaugurated its work by a first phase of *in camera* briefings given by its staff and by the various participants in the system established by the *CSIS Act* and the *Security Offences Act*. The purpose of these briefings was to give the Committee an understanding of how the various parts of the security and intelligence community fit together and the role of each in the system.

Concurrently, Committee staff conducted two dozen research interviews with people in public and private life who could give the Committee guidance and advice on how to carry out the comprehensive review and what should be examined. Using the *in camera* briefings and the research interviews, Committee staff developed a Key Issues Document, which set out a proposed structure for the comprehensive review and outlined the inter-related issues it had to address. This enabled the Committee to determine what questions it had to ask, what documents it needed to examine, what research it had to carry out, and what further briefings it had to seek. The Key Issues Document also provided, to a large degree, the model upon which the structure of this Report is based.

The Committee began the second phase of its work — public hearings — by having the main participants in the system established under the *CSIS Act* and the *Security Offences Act* appear before it. Their public presentations to the Committee were helpful, but because of time limitations and the initial reticence of some of these witnesses, not all of the Committee's questions were answered fully. Early in its deliberations, the Committee was advised by those who had experience with the security and intelligence community that it should pose its questions with precision and determination, and that it should scrutinize the answers it obtained carefully and follow them up if necessary. Faced with some of the shortcomings of public hearings involving participants in the system established under the *CSIS Act* and the *Security Offences Act* and cognizant of the sage advice it had received, the Committee submitted detailed written questions to these witnesses and requested that their answers be provided in as complete and as timely a way as possible.

Written answers to the Committee's detailed questions were received; some of them were more helpful and more forthcoming than others. The responses the Committee

received were useful in carrying out the comprehensive review; more complete answers would have been even more helpful.

As part of its review program, the Committee requested access to a number of documents it believed were essential for it to provide Parliament with an evaluation of the *CSIS Act* and the *Security Offences Act*. Among the documents to which access was requested by the Committee were ministerial directions, reports by the Director of CSIS, certificates and reports by the Inspector General, and reports by the Security Intelligence Review Committee. Access to all these documents was denied to the Committee, although a briefing on some of them was given to the members in the absence of its staff. Ultimately, the Committee was also provided with briefings in secure premises by the Privy Council Office, the Deputy Solicitor General, SIRC, CSIS and the RCMP on several other issues — largely in the absence of Committee staff.

Public hearings were, of course, an important element in the Committee's comprehensive review. The issues raised by witnesses before the Committee and the recommendations for change made by them were given serious consideration, and many are reflected in this Report. Written submissions to the Committee and oral testimony by witnesses were synthesized in a Summary of Evidence by Committee staff and structured in the same manner as both the Key Issues Document and the written questions submitted to the main participants in the security and intelligence system. The Summary of Evidence gave the Committee a snapshot of the evidence it had received on a variety of issues and facilitated the preparation of this Report.

Committee staff undertook a number of research projects whose results are reflected in this Report. Similarly, outside legal analysis of issues under the *Canadian Charter of Rights and Freedoms*[3] was commissioned.

The Committee did not want to restrict itself to Ottawa but wished to visit a region of Canada where it could gather a variety of opinions in public hearings and, at the same time, visit regional offices of both CSIS and the RCMP's National Security Investigations Directorate. It accomplished this by travelling to Vancouver. The Committee visited only this one Canadian city because of time constraints. It selected Vancouver because it met the above criteria and because the events in the *Atwal* case occurred in British Columbia.

Finally, the Committee decided it wanted to investigate the security and intelligence models with which Canada's is most often compared — those of the United States and Australia. During two days in Washington, D.C., the Committee gained a valuable sense of the U.S. model from the perspectives of both the executive and legislative branches of government, the security and intelligence agencies themselves, and outside observers. The Australian security and intelligence assessment experience was also explored during sessions in Washington. The Committee visited with the Australian Ambassador to the United States, the former head of Australia's Office of National Assessment. The Committee came away with a number of insights that are reflected in this Report.

1.5 Observations About the Committee's Comprehensive Review Process

The members of the Committee undertook this task with a commitment to effecting as thorough a review as possible. The complexity of the issues to be considered and their sensitivity made it clear early on in the process that the challenge it faced would be a daunting one, not to be easily completed in the time available.

This challenge was made even more difficult by the reluctance of some elements of the security and intelligence community to provide the Committee with the type of assistance it required to complete its task. This reluctance was manifested in an unwillingness to give the Committee full access to documents, to allow staff to accompany the Committee to all briefings, and to permit staff to visit all premises toured by the Committee. In fairness, however, it must be admitted that this review of security and intelligence in a public forum is a rarity for Canada, and a certain degree of reticence was to be expected. It must also be admitted that a fair degree of information was provided to the Committee and that it aided the review process. The Committee sensed the development of some degree of mutual understanding and trust between it and the security and intelligence community as it proceeded through its review.

The Committee has compared its experience of reticence and reluctance among the security and intelligence community in Canada with what it learned about the U.S. experience. Almost without exception, all those with whom the Committee came into contact in Washington, in both the Executive Branch and the intelligence agencies, were comfortable with Congressional review and oversight. It took time, however, for reticence to be overcome and for mutual trust to develop. As a result of progress in these matters, the U.S. Congressional oversight system appears to work better now than it did in the past. The Committee hopes that similar developments will occur in this country. Several of the Committee's recommendations will advance this goal.

The Committee's review was conducted at a time of change and flux in the Canadian security and intelligence community and in the international political realm. Unlike earlier reviews in Canada, this Committee's work was not animated by scandal or extraordinary events. The time was propitious for calm reflection in a period of flux but not of crisis. The recommendations in this Report are intended to take Canada's security intelligence community into the 1990s and beyond.

1.6 What the Committee Learned from the Review Process

The Committee sees its review as part of a two-directional continuum where the participants start out at opposite ends. The first part is the development by parliamentarians of their experience and expertise in the consideration of security and intelligence matters. The other part of the continuum is the acceptance by the security and intelligence community of the necessity and utility of parliamentary review. At the

beginning of the Committee's work there was much reticence within the security and intelligence community about parliamentary review. Through test and trial, both parliamentarians and the security and intelligence community appear to have come a long way. There is still a long way to go, however, to reach the point of convergence on the continuum.

Both sides will have to undertake confidence-building measures for any future parliamentary review. Parliament will have to establish clearly how it intends to ensure that the security and intelligence community is accountable to it and to Canadians. Parliament will have to engage permanent staff who are knowledgeable about security and intelligence issues and experienced in working with parliamentary institutions, ensure that this staff is security-cleared, and make provisions for it to operate in secure premises. On the security and intelligence community's side, it will have to learn to be more forthcoming in providing Parliament with access to documents and personnel. The Committee believes strongly, after a year of living with the uncertainties and suspicions felt on both sides of the review process, that such undertakings on both sides will lead to better accountability to Parliament and to a more effective security and intelligence community.

1.7 Are CSIS and Security Intelligence Still Needed?

Since the end of the World War II, the main preoccupation of Canadian security intelligence has been the threat and fact of espionage in Canada by the Soviet Union and other Warsaw Pact governments. The tumultuous changes in Eastern Europe in recent years are already having an impact on defence and arms control policies.

The threshold question for the Committee was whether the end of the Cold War means the end of a need for security intelligence in Canada and, in particular, whether there is any continuing need for CSIS.

The Committee has concluded that there still is a need for security intelligence and, subject to some modifications, for the special intrusive powers the *CSIS Act* gives CSIS. However, the dramatic events of the past few years in Eastern Europe suggest that a new creativity in security intelligence policy is required.

The Committee received a briefing on the current nature of threats to the security of Canada and some of the measures undertaken by the Service. In preparation for this briefing by the Service, the Committee held an information session with its staff.

The Committee has concluded that terrorism and espionage continue to threaten Canada and the interests of Canadians. Foreign governments still engage in covert intelligence activities against Canada and maintain a capacity in the area and an interest in doing so. There are current cases of foreign governments covertly intervening in Canadian public affairs. International terrorism remains a threat to world order; from time to time Canada is a base for activities in support of terrorism in other countries.

Terrorist acts can have direct impacts on the lives of Canadians. The guests of Canada can also be the subject of terrorist threats.

CSIS reported that the nature of Eastern European espionage was changing to a greater focus on acquiring technological and scientific information.

The Committee notes that no witness came forward to argue that security intelligence was no longer necessary or that CSIS should be rolled back into the RCMP. No one argued for a complete end to the intrusive powers afforded CSIS under its Act. In general terms, the Committee was satisfied that the basic scheme of the Act is working well, that a separate civilian service is in the best interests of Canadians, and that CSIS is still performing a necessary service.

The Canadian security intelligence model, with a statutory mandate and built-in direction, control and review capabilities, is unique. It enables the Service to perform its functions effectively, but ensures control and accountability. The Committee believes that the Canadian experience in this area has been largely successful. The recommendations made in this Report build and improve upon the institutions already in place, while augmenting the role of Parliament.

RECOMMENDATION 1

The Committee recommends that the Canadian Security Intelligence Service, the Inspector General and the Security Intelligence Review Committee be continued, and that the provisions of the *Canadian Security Intelligence Service Act* and the *Security Offences Act* be retained and amended by adoption of the recommendations contained in this Report.

NOTES

1. RSC, 1985, c. C-23, as amended.

2. RSC, 1985, c. S-7.

3. *Constitution Act, 1982*, Part I, Schedule B of the *Canada Act, 1982*, c. 11 (U.K.).

CHAPTER TWO

Mandates of the Service

2.1 In General

The Canadian Security Intelligence Service (CSIS) is a civilian agency controlled and managed by its Director under the direction of the Solicitor General. The Service does not have law enforcement powers and, as an intelligence agency, is not authorized to engage in offensive or "countering" activities. This means that its employees do not have the powers of peace officers to collect criminal evidence or effect arrests and that its activities are largely defensive in nature. CSIS has both a primary mandate and several secondary mandates.

2.2 Primary Mandate

The Service's primary mandate is established by section 12 of the *CSIS Act*. It is required to collect, by investigation or otherwise, to the extent that is strictly necessary, and to analyze and retain, information and intelligence about activities that are on reasonable grounds suspected of constituting a threat to the security of Canada. The Service reports to and advises the Government of Canada on these activities.

Section 12 of the *CSIS Act* must be read in conjunction with the section 2 definition of "threats to the security of Canada". Threats to the security of Canada are defined as espionage or sabotage, foreign-influenced activities, terrorism and subversion. Under this definition, lawful advocacy, protest and dissent are not in and of themselves to be considered threats to the security of Canada unless carried on in conjunction with one of the elements of the definition. The combination of section 12 and the definition of threats to the security of Canada sets out the Service's security intelligence mandate.

2.3 Secondary Mandates

The Service has three secondary mandates. They are set out in sections 13, 14 and 16 of the Act.

Under section 13 of the *CSIS Act*, CSIS provides security assessments to departments and agencies of the government of Canada, which in turn make their own security clearance decisions in relation to employees and contractors under the Government Security Policy. With the Solicitor General's approval, CSIS may enter into arrangements with provincial governments, provincial government departments or police

forces under provincial jurisdiction to provide them with security assessments. The Service may also, with the approval of the Solicitor General after consultation with the Secretary of State for External Affairs, enter into arrangements with foreign states (or institutions thereof) or international organizations (or institutions thereof) to provide them with security assessments. Under section 38 of the *CSIS Act*, the security assessment arrangements entered into by the Service are reviewed by the Security Intelligence Review Committee (SIRC), and the information or intelligence provided pursuant to them is monitored by SIRC.

Section 14 of the *CSIS Act* allows the Service to advise ministers of the Crown on matters relating to the security of Canada or to provide them with information relating to criminal or security matters, subject to the proviso that such advice or information must relate to the performance of ministerial duties or functions under either the *Citizenship Act* or the *Immigration Act*.

The third of CSIS's secondary mandates is set out in section 16 of the *CSIS Act* dealing with the collection of information or intelligence concerning foreign states or persons. On the request of the Minister of National Defence or the Secretary of State for External Affairs, and with the consent of the Solicitor General, the Service may, in relation to the defence of Canada or the conduct of its international affairs, collect *within Canada* information or intelligence relating to the capabilities, intentions or activities of foreign states or persons other than Canadian citizens, permanent residents or corporations incorporated in Canada. Unlike the Service's primary mandate described in section 12, its section 16 mandate does not require that the information or intelligence collected under this provision relate to threats to the security of Canada. SIRC monitors any requests made to the Service under this part of its mandate. Section 16, therefore, sets out the Service's mandate in relation to foreign intelligence.

2.4 Co-Operative Arrangements

Under section 17 of the *CSIS Act*, the Service may, with the approval of the Solicitor General, enter into arrangements with departments of the government of Canada, the provinces, or with local police. After consultation with the Secretary of State for External Affairs, the Solicitor General also may approve the entry by the Service into co-operative arrangements with foreign states or international organizations. The arrangements entered into by CSIS under this section must be for the performance by the Service of its duties and functions. Copies of these written arrangements are provided to SIRC, which reviews them and monitors the provision of information and intelligence pursuant to them.

2.5 Judicial Control

Under Part II of the *CSIS Act* (sections 21–28) the Service may seek judicial warrants when intrusive techniques are required to investigate a threat to the security of Canada or to perform its functions under section 16. Such intrusive investigative techniques, dealing

with the interception of communications or the obtaining of information, records, documents or things, are not available to carry out the other elements of CSIS's mandate. Judicial control of the Service's activities by the Federal Court will be considered at greater length later in the Report.

2.6 Limits on the Service's Mandates

As indicated earlier in this chapter, a proviso at the end of the definition of threats to the security of Canada says that this definition does not include lawful advocacy, protest or dissent, unless it is carried on in conjunction with any of the activities set out in paragraphs (*a*) to (*d*). Both the Canadian Jewish Congress and the British Columbia Law Union expressed concern that this proviso inadequately limited the exercise by the Service of its primary mandate. The Committee agrees.

Both organizations recommended that section 12 be amended to restrict CSIS activities. The Canadian Jewish Congress recommended the following amendment as new subsection 12(2):

> The Service is prohibited from investigating the affairs or activities of or engaging in surveillance of any person or group of persons solely on the basis of the participation by that person or group of persons in lawful advocacy, protest or dissent.

The British Columbia Law Union proposed the following amendment to the *CSIS Act* as new section 12.1:

> Nothing in this Act is intended in any way to limit, abridge or infringe fundamental human rights and freedoms and, in particular, advocacy, protest and dissent are hereby recognized as inviolate elements of an open, free and democratic society in Canada.

Both the proviso at the end of the section 2 definition of threats to the security of Canada and the amendments proposed by the Canadian Jewish Congress and the British Columbia Law Union deal only with the Service's primary mandate. They do not set out the limits that would also apply to the Service's secondary mandates. The Committee realizes that the Service and the *CSIS Act* are conscious of and subject to the *Canadian Charter of Rights and Freedoms* in their daily operations. No obvious violations of rights and freedoms have come to the attention of the Committee in the conduct of this review.

Nevertheless, the Committee finds it somewhat unusual that there is a direct statutory limitation on CSIS's primary mandate, but no equivalent restraint on its secondary mandates. This gap in the *CSIS Act* must be filled.

Section 17A of the *Australian Security Intelligence Organization Act* reads as follows:

> This Act shall not limit the right of persons to engage in lawful advocacy, protest or dissent and the exercise of that right shall not, by itself, be regarded as

prejudicial to security, and the functions of the Organization shall be construed accordingly.

Section 3 of the *CSIS Act* provides for the establishment of the Service and for the location of its principal and other offices. The Committee believes that the objectives of the Service and the limitation on its primary and secondary mandates must be set out clearly in the provision of the Act establishing the Service. The objectives of the Service are to provide effective security intelligence, security assessment, advice to government and foreign intelligence. These objectives should be interpreted and implemented in such a way as not to infringe upon rights and freedoms.

RECOMMENDATION 2

The Committee recommends that section 3 of the *CSIS Act* be amended to set out the objectives to be pursued by the Service, and to ensure that these objectives and the primary and secondary mandates of CSIS are not pursued to the detriment of lawful advocacy, protest or dissent.

CHAPTER THREE

Primary Mandate — Warning the Government

3.1 Introduction

This chapter deals with the primary mandate of CSIS — the collection, analysis and retention of information and intelligence relating to threats to the security of Canada. Prior to dealing with the primary mandate set out in section 12 of the *CSIS Act*, the definition of threats to the security of Canada will be discussed and recommendations made. This definition provides the entry to the Service's primary mandate — if an activity does not fall within its ambit, it cannot become, at least under section 12, the object of CSIS attention. The issues dealt with in discussing this definition are difficult and controversial.

3.2 Threats to the Security of Canada

3.2.1 *In General*

In 1983 and 1984, the definition of threats to the security of Canada was one of the most controversial objects of debate in relation to Bills C–157 and C–9. The issues raised by this controversy are as important today as they were then but, surprisingly, the debate before this Committee on the issues, as on some others, was neither as vigorous nor as polarized as it was during that earlier period.

The definition required the adoption of what the 1983 Special Senate Committee called a "delicate balance" to address the controversy contained in discussions of threats to the security of Canada. The opposing views in this controversy found their way into testimony before the Committee. Some witnesses expressed the view that Canada should recognize that threats to the country's security have not diminished and that the Service's powers to deal with them should not be lessened. Others told the Committee that the looseness of wording in the definition of threats to the security of Canada may lead to the infringement of rights and freedoms of Canadians who do not represent threats to the country's security.

The Director of CSIS told the Committee in public session that despite political changes in many countries, there has been little reduction in the intelligence activities of other countries in Canada. He informed the Committee, for example, that because of the poor state of the economies of certain countries, they still actively seek technological and scientific information to build their own infrastructure. The Committee was told that the

unpredictable and devastating nature of terrorism is still a serious concern and that espionage and foreign-influenced activities are still present in Canada. Finally, certain commentators urged a broader approach to threats to security that would embrace global environmental, climatic, economic and health problems.

The Committee can assert not only that there are threats to the security of Canada, but also that they are in a dynamic period of change. While the Committee is convinced there are threats to the security of Canada, it believes there have to be changes both to the *CSIS Act* and to the Service itself to better reflect a changing reality.

The Committee examined the definition of threats to the security of Canada with witnesses' differing views in mind. It also took into consideration the requirement for an effective security intelligence agency that needs to be properly equipped to address real threats to the security of Canada. It considered this need in the context of the requirement to respect the rights and freedoms guaranteed by the *Charter*. The courts have elaborated a number of tests under the *Charter* to protect such rights as freedom of expression, freedom of assembly and the reasonable expectation of privacy. They have struck down a number of legislative and regulatory initiatives that have had a disproportionately negative impact on guaranteed rights and freedoms or have been excessively vague. Consequently, the Committee considered the different elements making up the definition of threats to the security of Canada and the elaboration of the Service's primary mandate in light of the requirement for an effective security intelligence agency and the guarantees set out in the *Charter*.

The definition of threats to the security of Canada is a comprehensive one — Parliament has indicated the nature of the conduct it considers to constitute threats. Similar definitions of threats are contained in the *Australian Security Intelligence Organization Act*, the *New Zealand Security Intelligence Service Act* and the recently adopted British *Security Service Act, 1989*. The Committee recognizes the difficulty of finding the right definition of threats to security that will both provide the Service with a workable primary mandate and not interfere with rights and freedoms.

3.2.2 *Espionage or Sabotage*

Section 2 of the *CSIS Act* says that "threats to the security of Canada" means:

> (*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.

There appear to be at least four elements to this portion of the definition of threats to the security of Canada. These four elements are:

1) espionage against Canada or detrimental to its interests;

2) sabotage against Canada or detrimental to its interests;

3) activities directed toward or in support of such espionage; or

4) activities directed toward or in support of such sabotage.

Both espionage and sabotage are included in the mandates set out in the *Australian Security Intelligence Organization Act* and the British *Security Service Act, 1989*. They were also included in the definition of threats recommended by the McDonald Commission in its 1981 Report.

A number of terms and phrases used in this portion of the definition are not themselves defined in the *CSIS Act*. Among them are "espionage", "sabotage", "detrimental to the interests of Canada", and "activities directed towards or in support of". Some of them are defined in other legislation — the *Criminal Code* and the *Official Secrets Act*, among others.

There is some reason for concern about the breadth of CSIS's mandate in this area. In this field of activity as in others, the Service gives the Government of Canada early warning of espionage and sabotage. Its mandate in this area, however, should not be so broad as to violate rights and freedoms guaranteed under the *Charter*. Hence this part of the definition must be redrawn so that it can stand up to scrutiny by the courts under the *Charter*, not be in violation of rights and freedoms, and provide adequate protection to national security.

First, the terms "espionage" and "sabotage" are not defined in the *CSIS Act*, although both are defined in the *Criminal Code* and the *Official Secrets Act*. The definitions of these terms in other legislation are not of recent vintage and may themselves require reconsideration in light of modern-day reality. A statutory definition of these terms would give CSIS and Canadians a clearer indication of the types of activities to which the Service's security intelligence mandate would extend. It may also be necessary to redefine these terms to indicate clearly whether industrial and technological espionage also fall within the Service's security intelligence mandate. Such redefinition would also clarify the issue of whether such activities need to be either domestic or foreign-inspired and whether they need be directed against the government of Canada alone or against any government in Canada to fit within this portion of the definition. Not only should these terms be defined in the *CSIS Act*, they should also be redrafted in the *Criminal Code*, the *Official Secrets Act* and related legislation to reflect modern conditions.

RECOMMENDATION 3

The Committee recommends that the terms "espionage" and "sabotage" be defined in the *CSIS Act* and that modern definitions of these terms be

inserted into the *Criminal Code*, the *Official Secrets Act*, and related legislation.

The phrase "detrimental to the interests of Canada" is undefined in the *CSIS Act* and lacking in precise meaning. What is meant by "detrimental" — is it meant to be interpreted in an economic, political, geographical or defence context? The present version of paragraph (*a*) does not provide an answer. Similarly, what is meant by the "interests of Canada"? Such vague terminology contributes to an overly broad mandate in this area and may lead to activities by the Service potentially in violation of rights and freedoms guaranteed by the *Charter*.

SIRC offered the following definition in its brief to the Committee:

> "detrimental to the interests of Canada" means activities which are foreign directed, are surreptitious or deceptive, and are directed toward:
>
> a) diminishing the sovereignty or territorial integrity of Canada;
>
> b) weakening Canada's military defences;
>
> c) harming Canada's international relations with any nation or organization;
>
> d) seriously endangering the lives, health or safety of Canadians;
>
> e) obtaining, illegally, or without proper authorization, any information or thing classified in the national interest by the Government of Canada; and,
>
> f) the bribery, coercion, or corruption of Canadians in respect of activities falling within paragraphs *a*), *b*), *c*), *d*) or *e*).

Further elements of a definition may be found in the September 1989 Ministerial Direction on national requirements for security intelligence. The following "national interest areas" are set out:

a) **Public Safety:** the ability of people to engage in ordinary social activity without fear of harm;

b) **Integrity of the Democratic Process:** the functioning of those institutions, rights and freedoms fundamental to the political well–being of a democratic society;

c) **Security of Government Assets:** the responsibility of the Government to protect those human, intellectual and physical assets which it manages in trust for the people of Canada;

d) **Economic Security:** the conditions necessary to sustain a competitive international position, provide productive employment, and contain inflation;

e) **International Peace and Security:** the ability of the international system to evolve, while avoiding war, containing regional conflicts and minimizing violence.

The Committee believes that the *CSIS Act* should be amended to indicate clearly what is meant by "detrimental to the interests of Canada".

RECOMMENDATION 4

The Committee recommends that the phrase "detrimental to the interests of Canada", used in paragraphs (*a*) and (*b*) of the definition of threats to the security of Canada, contained in section 2 of the *CSIS Act*, be itself defined.

The phrase "activities directed towards or in support of" espionage or sabotage is somewhat vague and unclear. If activities are "in support of" some other activity, a concrete link between one and the other will have to be shown — the same does not apply to "activities directed toward" which would appear to be one or more steps removed from the ultimate activity. The use of such vague terminology in this part of the definition appears to give CSIS too wide a mandate in relation to espionage and sabotage. This vague wording may also make paragraph (*a*) susceptible to a successful *Charter* challenge in the courts. Therefore, this part of the definition is also in need of amendment to reduce any overbreadth in the Service's mandate.

RECOMMENDATION 5

The Committee recommends that paragraph (*a*) of the definition of threats to the security of Canada contained in section 2 of the *CSIS Act* be amended by removing the words "directed toward or".

3.2.3 *Foreign–Influenced Activities*

Paragraph (*b*) of the definition of threats to the security of Canada is as follows:

(*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.

There are four elements to this portion of the definition of threats to the security of Canada:

1) foreign-influenced activities;

2) within or relating to Canada;

3) detrimental to the interests of Canada, and are;

4) clandestine, deceptive or involve a threat to any person.

The British *Security Service Act, 1989* gives its Service a mandate to provide protection against activities of agents of foreign powers. The *Australian Security Intelligence Organization Act* provides for a mandate in relation to acts of foreign interference. Such acts must be carried out on behalf of, directed or subsidized by, or undertaken in collaboration with a foreign power. The McDonald Commission proposed a definition of foreign-influenced activities similar to paragraph (*b*) of the present definition.

The Committee believes that paragraph (*b*) of the definition of threats to the security of Canada should be retained but with amendments to clarify the meaning of CSIS's mandate in this area. Despite recent worldwide political changes, there are still foreign-inspired activities that, while not amounting to espionage, sabotage or terrorism, merit the Service's attention.

The first problem with paragraph (*b*) is the use of the expression "foreign-influenced". There is no indication in the definition as to what is meant by these words. Foreign influence may be distant, indirect and unconscious and yet still fall within the ambit of activities subject to CSIS's attention. Both SIRC and the Canadian Bar Association recommend that the words "foreign-influenced" be replaced by "foreign-directed". The Committee agrees with this recommendation. This change in wording would require that there be some degree of conscious foreign control of the activities to be covered by this portion of the definition. The mere support of, or conscious or unconscious paralleling of, foreign ideas or activities will not suffice to fall within this portion of the definition if the Committee's recommendation is implemented.

RECOMMENDATION 6

The Committee recommends that paragraph (*b*) of the definition of threats to the security of Canada contained in section 2 of the *CSIS Act* be amended so that the words "foreign-influenced" are replaced by "foreign-directed".

The foreign-influenced activities covered by paragraph (b) must be within or relate to Canada. There is no problem in the requirement that such activities be within

Canada — this apparently means that they should occur in the country's geographical confines. There is no way to determine within the *CSIS Act* what is meant by "relating to Canada". It would appear that this phrase could capture any foreign-influenced activity, no matter how tenuous its connection with Canada. The connection becomes even more tenuous if the activity does not have to be within the geographical confines of the country. To narrow this part of the definition, and hence CSIS's mandate in this area, it is necessary to add criteria or some qualification to the phrase "relating to Canada". SIRC recommended in its submission to the Committee that the word "directly" be added to modify the phrase "relating to Canada". The Committee agrees. Such an amendment would have the effect of narrowing this part of the definition and putting in place a criterion for measuring the relation to Canada of the activities under consideration.

RECOMMENDATION 7

The Committee recommends that paragraph (*b*) of the definition of threats to the security of Canada contained in section 2 of the *CSIS Act* be amended by inserting the word "directly" before the phrase "relating to Canada".

The third element of this part of the definition requires that the foreign-influenced activities in question be "detrimental to the interests of Canada". This issue was addressed by the Committee in its discussion of paragraph (a) of the definition of threats to the security of Canada.

The fourth element of this part of the definition requires that the activity be clandestine, deceptive or involve a threat to any person. The Committee is unable to improve upon the wording of the first two alternatives, despite recommendations by the Canadian Bar Association and SIRC. It does, however, believe that the third alternative, "involve a threat to any person", needs amendment. There are no limiting criteria in the *CSIS Act* by which it is possible to judge the nature or the intensity of the threat in question. The Committee believes that this overly broad element requires some qualification. Both the Canadian Bar Association and SIRC recommend that "threat to any person" be qualified by the word "serious". The Committee agrees with this recommendation. It would require a demonstration that a threat be more than minimal or incidental before a foreign- influenced activity fell within this part of the definition of threats to the security of Canada.

RECOMMENDATION 8

The Committee recommends that paragraph (*b*) of the definition of threats to the security of Canada contained in section 2 of the *CSIS Act* be amended by inserting the word "serious" before the phrase "threat to any person".

3.2.4 *Political Violence and Terrorism*

Paragraph (*c*) of the definition of threats to the security of Canada contained in section 2 of the *CSIS Act* is as follows:

> (*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 objective within Canada or a foreign state.

There are four possible types of activities covered by paragraph (*c*) of the definition of threats to the security of Canada. These are activities:

1) within Canada directed toward the threat or use of acts of serious violence;

2) within Canada in support of the threat or use of acts of serious violence;

3) relating to Canada directed toward the threat or use of acts of serious violence; or

4) relating to Canada in support of the threat or use of acts of serious violence.

A further qualification contained in paragraph (*c*) is that the acts of serious violence threatened or used must be:

1) against persons or property and must be

2) for the purpose of achieving a political objective within Canada or a foreign state.

The *Australian Security Intelligence Organization Act* includes politically motivated violence within its definition of security, while the British *Security Service Act, 1989* includes political violence and terrorism within its Service's mandate. The McDonald Commission proposed a definition similar to paragraph (*c*) in its 1981 report.

The Committee believes that paragraph (*c*) of the definition of threats to the security of Canada should be retained but amended to clarify the Service's mandate and to make it consistent with the requirements of the *Charter*. There is no doubt in the Committee's mind that there are activities involving political violence and terrorism that should continue to be the object of the Service's attention. In recent years Canada has been both the site and the staging area for such activities. There is, however, the danger that security intelligence work in this area will have a chilling effect on legitimate fund-raising and other forms of non-violent political activity. The aim of the amendments proposed in this area is to ensure that security intelligence activity in relation to political violence is kept within reasonable limits.

The activities in paragraph (*c*) need only relate to Canada – there are no limiting criteria in the Act whereby it may be readily determined whether the activities are important enough in their impact on Canada to merit the Service's attention. As set out in relation to the same issue discussed under paragraph (*b*), the Committee believes that "directly" should also precede the word "relating" in paragraph (*c*). Similarly, the Committee believes that the words "directed toward" should be removed from paragraph (*c*). The same recommendation was made by the Committee in relation to paragraph (*a*) of the definition of threats to the security of Canada and is made here for the same reasons.

RECOMMENDATION 9

The Committee recommends that paragraph (*c*) of the definition of threats to the security of Canada contained in section 2 of the *CSIS Act* be amended by inserting the word "directly" before the phrase "relating to Canada" and by deleting the words "directed toward".

3.2.5 *Subversion*

Paragraph (*d*) of the definition of threats to the security of Canada contained in section 2 of the *CSIS Act* is as follows:

> (*d*) activities directed toward undermining by covert unlawful acts, or directed toward or ultimately intended to lead to the destruction or overthrow be violence of, the constitutionally established system of government in Canada.

Two types of activities are included in paragraph (*d*) of the definition of threats to the security of Canada. It covers activities that are either:

1) directed toward undermining by covert unlawful acts the constitutionally established system of government in Canada; or

2) directed toward or intended ultimately to lead to the destruction or overthrow by violence of the constitutionally established system of government in Canada.

Although it does not include subversion *per se* in its definition of security, the *Australian Security Intelligence Organization Act* does include politically motivated violence, promotion of communal violence and acts of foreign interference within its ambit. The British *Security Service Act, 1989* gives its Service a mandate to provide protection from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means. The recommendation made by the McDonald Commission in its 1981 Report was similar to paragraph (*d*), but dealt with "revolutionary

subversion" and would not have allowed for intrusive investigative techniques under this heading.

In accepting the recommendations of the Independent Advisory Team (IAT), the Solicitor General ordered CSIS's Counter-Subversion Branch dismantled in 1987. Most of the Counter-Subversion Branch targets were discontinued. Its remaining targets were divided among the Counter Intelligence, Counter Terrorism, and Analysis and Production Branches. Since 1988, any investigation by the Service under paragraph (*d*) involving more than the collection of open source information requires, under a ministerial direction to that effect, the approval of the Solicitor General. No such ministerially-approved intrusive investigations have been authorized since the direction was issued in February 1988.

Paragraph (*d*) is by far the most controversial provision addressed by the Committee in this Report. Those who call for the repeal of paragraph (*d*) see it as having a chilling effect on rights and freedoms. They argue that the vagueness of this provision leads to excessive speculation on the ultimate effect of the exercise of guaranteed rights and freedoms and, consequently, to uncalled-for targeting of legitimate activity. They also say that since the Counter-Subversion Branch of CSIS was disbanded in 1987, it is now time to repeal paragraph (*d*) of the definition of threats to the security of Canada as a spent provision.

Those who argue in favour of retaining paragraph (*d*) admit that the activities it covers do not constitute a major threat to the security of Canada at present and that many of the activities it encompasses may be captured by paragraphs (*b*) and (*c*) of the definition. But they go on to argue that Canadians expect CSIS to be in a position to forewarn the Government of Canada about potential threats to the security of Canada, especially if the activities dealt with by paragraph (*d*) again become a significant threat at some future time.

This was one of the most controversial and difficult issues addressed by the Committee in conducting this comprehensive review. The divergent points of view are strongly held and vigorously expressed. After a thorough discussion of the implications of a number of options to deal with this part of the definition, the Committee, although not unanimously, came to the conclusion that paragraph (*d*) should be repealed. Many of the activities, it was felt, now caught by paragraph (*d*) could be dealt with under paragraphs (*a*), (*b*) and (*c*) of the definition, even if the Committee's recommendations in relation to them are implemented. If paragraph (*d*) is repealed, a consequential amendment to section 21(5)(*a*) of the Act limiting judicial warrants to sixty days would also have to be adopted.

RECOMMENDATION 10

The Committee recommends that paragraph (*d*) of the definition of threats to the security of Canada contained in section 2 of the *CSIS Act* be repealed.

RECOMMENDATION 11

The Committee recommends that section 21(5)(*a*) of the *CSIS Act* be repealed.

3.3 CSIS's Primary Mandate

Section 12 of the *CSIS Act*, which establishes CSIS's primary mandate, reads as follows:

> 12. The Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyze and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada.

A number of terms and phrases in this provision are ambiguous or unclear. Some of these phrases are: "by investigation or *otherwise*", "to the extent that it is strictly necessary", "reasonable grounds be suspected" and "constituting threats to the security of Canada". It is difficult to come up with amendments that would give the Service a more precise definition of its primary mandate than section 12 already establishes. Nevertheless, there is no doubt that the Service needs guidance on how to interpret its primary mandate as set out in the definition of threats to the security of Canada and section 12 of the *CSIS Act*.

To this end, in March 1985 the Inspector General circulated to various elements of the Canadian security and intelligence community an exhaustive 300-page legal memorandum prepared by a consultant dealing with CSIS's primary mandate. It dealt with many of the issues addressed in this chapter. This initiative by the Inspector General appears to have met with little or no interest from the security and intelligence community. In April 1987, the Inspector General circulated a legal memorandum prepared by another consultant dealing with the "strictly necessary" limitation on the Service's primary mandate. It included principles or guidelines for the interpretation of this phrase. In October 1987, the IAT urged that the Solicitor General's Ministry Secretariat develop, in collaboration with the Service, legal/policy frameworks for the section 12 primary mandate and the section 2 definition of threats to the security of Canada.

In an implementation report on the status of the recommendations made by the IAT in 1987, the Service informed the Committee that "directives" dealing with section 12 and the definition of threats to the security of Canada were in preparation and a draft would be ready for consideration by the Deputy Solicitor General and the Director of the Service in the spring of 1990. Despite the work of the Inspector General and the urging of the IAT, there is still, six years after CSIS was established, no comprehensive ministerial direction

dealing with the Service's primary mandate. It is not clear to the Committee why such a comprehensive ministerial direction is not yet in place — it may be because of inadequate resources or more pressing priorities. Nevertheless, the Committee urges strongly that such a comprehensive ministerial direction be put in place.

RECOMMENDATION 12

The Committee recommends that the Solicitor General issue to the Director of the Canadian Security Intelligence Service a comprehensive direction dealing with CSIS's primary mandate.

CHAPTER FOUR

Secondary Mandate — Security Assessments

4.1 Introduction

The Government Security Policy deals essentially with two matters: it establishes criteria for vetting persons for employment with the federal public service or under contract to it; and it provides procedures to be followed in the classification and protection of government assets.

4.1.1 *Vetting Employees and Persons Under Contract*

CSIS has been given the primary responsibility for conducting security assessments. Such assessments are required in occupations where the individual concerned will regularly come in contact with information or materials that are sensitive in the national interest.

Sections 13 through 15 of the *CSIS Act* give the Service authority to conduct security assessments.

Section 13 allows the Service to provide security assessments to federal government departments and to provincial governments. It also authorizes the Service to enter into arrangements with provincial police forces, foreign governments and institutions of such governments with a view to providing them with security assessments.

Section 14 allows the Service to provide certain help to ministers of the Crown regarding their duties or functions under the *Citizenship Act* or the *Immigration Act*. In particular, the Service may, under this section, advise ministers on matters relating to the security of Canada or provide such ministers with pertinent information concerning security issues or criminal activities.

Section 15 empowers the Service to conduct such investigations as are considered necessary to provide either the security assessments identified in section 13 or the advice detailed in section 14.

The Government Security Policy also permits the Department of National Defence and the RCMP to provide security assessments of their own employees.

The Committee understands that the Director of the Service must now personally approve any adverse recommendations with respect to security assessments made by

CSIS. In citizenship and immigration cases, the Director must also forward reports to the Solicitor General. The Committee has been advised that approximately 15 recommendations for denial of a security clearance have been made since the Government Security Policy was introduced in 1986.

4.1.2 *Protection and Classification of Government Assets*

The Government Security Policy establishes a system for protecting and classifying government documents, information and other assets. The essential features of the classification scheme are as follows:

1) assign accountability to Deputy Heads for the safeguarding of information and other assets under their control;

2) classify information when its unauthorized disclosure or other compromise could reasonably be expected to result in injury to the national interest, with reference to specific provisions of the *Access to Information Act* and the *Privacy Act*;

3) limit access to classified information and assets to those whose duties require such access and who have a security clearance at the appropriate level;

4) designate information when its unauthorized disclosure or other compromise could reasonably be expected to cause injury to interests other than the national interest, with reference to specific provisions of the *Access to Information Act* and the *Privacy Act*;

5) limit access to designated information and assets to those whose duties require such access and who have enhanced reliability status;

6) ensure that all persons subject to personnel screening are treated in a fair and unbiased manner; and

7) safeguard classified or designated information and assets in accordance with security standards and threat and risk assessments.[1]

Material considered sensitive for reasons of national security are classified at one of three levels. Persons requiring access to particular levels of classified documents must have the appropriate level of security clearance.

4.2 Security Assessments

4.2.1 *Security Assessments for Government Employment*

Under section 2 of the *CSIS Act*, "security assessment" means an appraisal of the *loyalty* to Canada and, so far as it relates thereto, the reliability of an individual.

Under the current Government Security Policy, individuals are denied a security clearance if there are reasonable grounds to believe that:

a) they are engaged in, or may engage, in activities that constitute a threat to the security of Canada within the meaning of the *CSIS Act*; or

b) because of personal beliefs, features of character, association with persons or groups considered a security threat, or family or other close ties to persons living in certain countries;

— they may act or may be induced to act in a way that constitutes a "threat to the security of Canada"; or

— they may disclose, may be induced to disclose or may cause to be disclosed in an unauthorized way, classified information.[2]

The Committee believes that the above provisions, especially paragraph (*b*), are overly vague and may lead to abusive activity by CSIS. "Personal beliefs" and "features of character", for example, are not defined in the Government Security Policy or the CSIS Act. This policy mandate may give the Service free reign to delve into all aspects of an individual's personal life, irrespective of whether such matters are strictly related to national security concerns.

For example, the Committee learned of at least one case involving a person who, while undergoing a security assessment for government employment, was suspected of being homosexual. During lengthy interviews conducted by CSIS officers, questions were repeatedly asked about the individual's sexual orientation. Because the individual refused to answer these questions, the CSIS officers appear to have concluded that the person was dishonest and unco–operative.

Such inquiries by CSIS may indeed be contrary to the *Canadian Charter of Rights and Freedoms*. In addition, the Committee believes that they have little, if anything, to do with national security concerns as contemplated by the Government Security Policy.[3]

The Committee also learned of cases where persons have been denied security clearances because they occasionally used soft drugs. SIRC has concluded, in a number

of cases involving DND security assessments, that such activity, although it may be a concern regarding a person's lifestyle, has nothing to do with national security.

RECOMMENDATION 13

The Committee recommends that the *CSIS Act* be amended to define "security assessment" under section 2 of the Act to coincide with the "threats to the security of Canada" provisions under the Act.

Professor Peter Russell, during testimony before the Committee, stated that non-CSIS security staffing officers should be responsible for dealing with "character concerns" of an individual, while CSIS should restrict itself to those relating to "security intelligence" matters.

The McDonald Commission had earlier noted, especially in the area of field investigations undertaken during a security assessment, that such investigations "are primarily a personnel function in a security context, not a security intelligence function".[4]

The Committee believes that the Government should consider restricting CSIS's mandate regarding security assessments for government employment. Moreover, the Committee believes that the Government should also consider establishing a group of security staffing officers to undertake the activities suggested by the McDonald Commission.

4.2.2 *Delays*

SIRC has noted repeatedly in its annual reports that there has been a persistent problem with delays in processing security assessments. As noted elsewhere in this Report, the Committee recommends that persons who are undergoing security assessments may make a complaint to SIRC when there is undue delay. Although delays have been a more significant problem in the past, CSIS has made significant efforts to reduce the time required to process security assessments under the Government Security Policy. As noted in the 1988-89 SIRC *Annual Report*:

> It is still, as CSIS acknowledges, taking too long to process requests for security assessments. In some cases, notably in immigration, which depend on information from foreign governments, timing is beyond the Service's control. With respect to clearances under the Government Security Policy, the goal is a 30-day turnaround time for levels I and II (Confidential and Secret) and 120 days for Level III (Top Secret). It now takes twice that long — 60 days for Levels I and II and 240 days for Level III. These are, of course, averages. Some are quicker, some slower.[5]

The Committee believes that allowing SIRC to entertain complaints concerning security assessments that are taking an inordinate length of time to complete provides

protection to persons who are the subjects of assessment. The Committee also wishes to encourage CSIS to continue its efforts to reduce the length of time required to complete security assessments. The Committee recognizes fully that many delays may be outside the control of the Service.

4.2.3 *Security Assessment Interviews*

The Committee has learned of a number of instances where security assessment subjects were interviewed in a questionable manner by CSIS officers. Inappropriate questions were asked, intimidating comments were made, and individuals were asked to name other persons with whom they associated.

A related problem is that the answers provided during these interviews are commonly used in the preparation of CSIS reports or during hearings before SIRC. Moreover, the person concerned is unable to obtain, as of right, copies of the notes or a transcript (if a recording was made) from the interview.

The Committee believes that a person who is the subject of a security assessment should be able, if she or he wishes, to attend the interview accompanied by legal counsel or an agent and to record the interview after advising the attending officers of an intention to do so. Conversely, the investigating security officers should be allowed to record an interview with the consent of the person concerned.

This recommendation would protect both the person subject to the security assessment and the investigating officers (in the event that allegations of impropriety were to arise at a later date). Both parties would be able to rely on the recording of the interview to substantiate their version of the facts. The Committee believes that this practice should be allowed for all categories of security assessment cases, whether for government employment, or immigration and citizenship cases.

RECOMMENDATION 14

The Committee recommends that the *CSIS Act* and the Government Security Policy be amended to provide that a person who is subject to a security assessment interview be allowed to be accompanied by legal counsel or an agent and to have the interview tape-recorded after advising the Service of his or her intention to do so.

4.2.4 *Security Assessments Under the Immigration Act*

The "threats" provisions in section 2 of the *CSIS Act* differ from those in the *Immigration Act*. The latter use wording that does not conform with or exist in the *CSIS Act*. The McDonald Commission argued that the criteria for denying admission to Canada in the *Immigration Act* should be consistent with the definition of threats to the

security of Canada as defined in the statutory mandate of the security intelligence agency.[6] SIRC also recommended that the *Immigration Act* be amended to define classes inadmissible on security grounds in a manner consistent with the definition of "threats to the security of Canada" in the *CSIS Act*.[7] The Committee agrees with these proposals and accordingly makes the following recommendation.

RECOMMENDATION 15

The Committee recommends that the "Security Exclusion" provisions of the *Immigration Act* be amended to correspond with the "threats to the security of Canada" definition contained in section 2 of the *CSIS Act*.

4.2.5 *Quality of CSIS Information*

SIRC indicated in its 1986–87 *Annual Report*, that the "quality of CSIS reports and [the] evidence it presented to [the Review Committee] in citizenship and immigration cases... was especially disappointing."[8] By contrast, in a report prepared by the Inspector General for SIRC, interviews with CSIS officers indicated that "foreign agency information reliability is not of concern to CSIS".[9]

Without question, CSIS has to rely on information from other foreign security or police agencies when conducting security screening checks in the immigration and citizenship fields. It is of concern to the Committee that the Service may be receiving information from these foreign agencies that has been "massaged" or is provided with an underlying political motive. The McDonald Commission recognized that:

> There is a danger in the immigration screening process of placing too great and uncritical reliance on foreign agency information. The information received must always be carefully analyzed in the context of the political circumstances of the country providing it. No foreign agency should be considered a 'reliable source' in the sense that its reports can be accepted uncritically.[10]

Because it agrees with the views expressed by the McDonald Commission, the Committee believes that CSIS should be cautious in using information provided by foreign agencies, especially from countries that may have poor human rights records or foreign policy objectives inimical to those of Canada. The Committee believes that CSIS Security Liaison Officers posted abroad and analysts at Headquarters should guard against accepting information from foreign intelligence or police agencies without testing its accuracy and reliability.

4.3 Classification of Government Information

The current classification of government information is overly complex. It is the Committee's understanding that the United States has simplified its scheme to include two categories of classification, while the Canadian scheme currently has three:

Confidential, Secret and Top Secret. In the United States, the Senate Select Committee on Intelligence recommended that the 'Confidential' classification be dropped, with such information either being kept unclassified or protected at a higher (Secret) level. It was felt that the classification threshold in the United States should reflect a policy that classifies information only where it is truly necessary.[11]

The Committee did not find the distinguishing definitions for different levels of classification particularly helpful. The distinctions regarding the gravity of injury contemplated by the 'Confidential', 'Secret' and 'Top Secret' classifications are simply not clear. There is concern that the classification scheme, as now constituted, may indeed lead to overclassification or misclassification of information.

The Committee believes that the current classification of government information under the Government Security Policy should be revised. Such revision should be undertaken with a view to simplifying the categorization process, reducing the number of categories of information, and providing better distinguishing definitions.

RECOMMENDATION 16

The Committee recommends that Treasury Board study the possibility of revising the Government Security Policy so as to reduce the number of categories for the classification of government information.

4.4 Putting Government Security Policy Into Regulatory Form

The current Government Security Policy is not a statute or a regulation. It does not, therefore, offer the type of certainty and protection inherent in statutory or regulatory instruments. Policy guidelines are more flexible and more readily adaptable to 'interpretation' and the exercise of 'discretion'. On one hand, such flexibility may be desirable. On the other hand, it may lead to uncertainty as to its application.

The Committee believes that the Government Security Policy should be placed into regulatory form by the Governor in Council. This would give the Government Security Policy a statutory base which, it is suggested, would not only enhance the visibility of the policy but would also augment the legal status of decisions based upon it.

RECOMMENDATION 17

The Committee recommends that the Government Security Policy be adopted as regulations by the Governor in Council.

4.5 Dissemination of CSIS Reports

The Committee learned of a situation where a CSIS security assessment report on a person seeking a security clearance, which contained substantial personal information, was communicated to unauthorized persons in the government department where the person was employed. This case resulted in a complaint being made to SIRC, which concluded that CSIS should develop internal guidelines on the provision of sensitive information in its reports to deputy ministers.

The Committee believes that CSIS should ensure that when it provides personal information to a government department, such information is treated with the utmost care to protect the privacy of the individual concerned. The Committee supports the conclusion of SIRC that internal guidelines should be developed, if they do not already exist, to provide direction to the Service on this issue.

As well, the Committee believes that government departments should develop similar guidelines to ensure that CSIS security assessment reports are treated and disseminated in an authorized manner.

RECOMMENDATION 18

The Committee recommends that the Government ensure that guidelines are in place both within CSIS and in government departments to ensure that security assessment reports are treated as confidential and are communicated only to persons who have authority to have access to them.

NOTES

1. Treasury Board of Canada, Secretariat, *Security Policy and Standards*, Ottawa, December 1989, p. 1.

2. *Security Policy and Standards*, Appendix 'F' pp. 10–11.

3. Regarding the issue of sexual orientation as a ground covered by section 15 of the *Charter*, see *Correctional Service of Canada* v. *Veysey*, an unreported decision of the Federal Court of Appeal rendered May 31, 1990, court file # A–557–89.

4. Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (McDonald Commission, 1981), Second Report, Volume 2, p. 798.

5. Security Intelligence Review Committee, *Annual Report 1988–89*, p. 17.

6. McDonald Commission, Second Report, Volume 2, p. 823.

7. Security Intelligence Review Committee, "Immigration Screening Activities of the Canadian Security Intelligence Service", Report prepared under section 54 of the *CSIS Act*, January 18, 1988, expurgated version released under the *Access to Information Act*, p. 23.

8. Security Intelligence Review Committee, *Annual Report 1986–87*, p. 58.

9. Security Intelligence Review Committee, "Immigration Screening Activities...", p. 10.

10. McDonald Commission, Second Report, Volume 2, p. 824.

11. United States Senate, "Meeting the Espionage Challenge: A Review of United States Counter Intelligence and Security Programs", Report of the Select Committee on Intelligence, Washington, 1986, p. 75.

CHAPTER FIVE

Secondary Mandate — Foreign Intelligence

5.1 Foreign Intelligence

A foreign intelligence capacity for Canada has been a recurrent but muted theme of the intelligence debate in this country for more than forty years. Generally, the consensus has been that Canada does not need a foreign intelligence service that collects intelligence abroad by covert means. Recently the Security Intelligence Review Committee (SIRC) recommended that the foreign intelligence mandate of the Canadian Security Intelligence Service be expanded. Under section 16 of the *CSIS Act*, the Service can collect foreign intelligence only within Canada. SIRC would like to see the *CSIS Act* amended to give the Service the authority to send intelligence officers abroad on foreign intelligence missions.

5.1.1 *Definitional Framework*

The terms "security intelligence" and "foreign intelligence" are often confused with one another. One reason is that they have a common denominator: the national interest. They differ significantly, however, in their approach to the national interest.

Security intelligence seeks to preserve the national interest by collecting intelligence on threats to national security — that is, threats to a nation's territory, inhabitants, institutions or material possessions. The *leitmotif* of security intelligence is embodied in the section 2 definition of threats to the security of Canada in the *CSIS Act*. In this section, threats to national security are defined as activities directed against Canada that fall under such general headings as espionage, sabotage, foreign-influenced activities, political violence or terrorism, and subversion.

By contrast, foreign intelligence attempts to promote the national interest. Its aim is to obtain information that would otherwise not be available on the activities of foreign states, institutions or agents, independent of whether those activities are specifically or purposefully directed against the national interest. Foreign intelligence may constitute a security threat for those against whom it is directed. Paradoxically, one of the defence mechanisms to counter foreign intelligence is security intelligence.

Security intelligence and foreign intelligence can be collected both inside and outside the territorial boundaries of the country gathering such intelligence. CSIS is more than a security intelligence agency. Under section 16 of the *CSIS Act*, the Service can collect foreign intelligence. It can do so, however, only within the territorial boundaries of Canada.

Canadian public officials have consistently denied that Canada engages in covert foreign intelligence abroad. Military attachés of the Department of National Defence and foreign service officers of the Department of External Affairs collect foreign intelligence. But they do this by way of open sources, not by covert means. The Communications Security Establishment (CSE) also collects foreign intelligence within Canada. It gathers signals intelligence in support of Canada's foreign and defence policies, based on the collection of foreign radio, radar and other electro-magnetic transmissions, and distributes reports on what such intelligence reveals. The CSE also provides for the security of data processing in and communications between federal agencies.

5.1.2 *Legislative Framework Governing the Foreign Intelligence Activities of the Service*

When the Senate Special Committee reviewed Bill C-157, the precursor to the current *CSIS Act*, it recommended that the Service should have a monopoly on all operational work relating to the conduct of foreign intelligence within Canada. The rationale was that all intelligence gathering activities conducted inside Canada should be brought within the same oversight net. This proposal was not incorporated into the *CSIS Act*. The government of the day considered that granting such a monopoly to CSIS would give the new agency an inappropriate degree of responsibility for the management of part of the foreign intelligence program of Canada.

As a result the *CSIS Act* enabled the Service to collect foreign intelligence only within the territorial boundaries of Canada, on request of the Minister of National Defence or the Secretary of State for External Affairs, and following the approval of the Solicitor General. Section 16 states that:

> 16. (1) Subject to this section, the Service may, in relation to the defence of Canada or the conduct of the international affairs of Canada, assist the Minister of National Defence or the Secretary of State for External Affairs, within Canada, in the collection of information or intelligence relating to the capabilities, intentions or activities of
>
> (*a*) any foreign state or group of foreign states; or
>
> (*b*) any person other than
>
> (i) a Canadian citizen,
>
> (ii) a permanent resident within the meaning of the Immigration Act, or
>
> (iii) a corporation incorporated by or under an Act of Parliament or of the legislature of a province.

(2) The assistance provided pursuant to subsection (1) shall not be directed at any person referred to in subparagraph (1)(*b*)(i), (ii) or (iii).

(3) The Service shall not perform its duties and functions under subsection (1) unless it does so

(*a*) on the personal request in writing of the Minister of National Defence or the Secretary of State for External Affairs; and

(*b*) with the personal consent in writing of the Minister.

The section thus allows the Service to provide assistance to the foreign intelligence program of the Government of Canada, in particular the Communications Security Establishment, the Department of External Affairs and the Department of National Defence. The section expressly prohibits the targeting of Canadians.

5.1.3 *Current Practices*

In its Annual Report for 1985–86 SIRC reported that the Service had not exercised its authority under section 16. However, the former Solicitor General, the Honourable Pierre Blais, confirmed in his written responses to the Committee's questions that section 16 has since been used. He declined to give the Committee details regarding its use, on the grounds that such disclosure would be injurious to national security and to the conduct of Canada's international relations.

The former Solicitor General also confirmed when he appeared before the Committee that the Service occasionally sends intelligence officers abroad to conduct investigations. The Government considers that under section 12 of the *CSIS Act*, the Service may receive or collect information outside Canada that relates to the investigation of a threat to the security of the country. In response to a question by a member of the Committee as to whether the Service has legal authority to send officers outside Canada to gather intelligence, the former Solicitor General stated:

> The answer to the question is clear and is based upon the nature of CSIS as a defensive security intelligence service. It does not seek to conduct offensive intelligence operations abroad. However, CSIS does have the power to investigate threats to the security of Canada. Under the Act we have not only the power but the duty to send informants or Service employees abroad. It is a known fact, there is no secret about it. Our foreign operations always relate to investigations of a threat to Canadian security. That is something we must remember.

The Honourable Pierre Blais went on to explain that as a matter of policy, his personal authorization is required before CSIS intelligence officers are sent abroad. The

Solicitor General has given direction to CSIS with respect to foreign liaison and security intelligence investigations abroad.

The Service also has security liaison officers stationed in a number of countries. The responsibilities of such officers include:

1) selective development of channels of communication for exchanges of information with police, security and intelligence agencies, relating to threats to the security of Canada;

2) assessment of the reliability of co-operating agencies and their intelligence product;

3) provision of an immigrant / visa vetting service on prospective immigrants for the Canada Employment and Immigration Commission; and

4) collection and analysis of security-related open source information.

5.1.4 *The Need for Change*

SIRC is currently opposed to the establishment of a separate, offensive foreign intelligence agency for Canada; it believes the case has not been made for such an agency. In its proposals to the Committee, SIRC wrote that:

> Since we have no capacity to collect foreign intelligence by covert human means, we are dependent upon other countries for some types of information about foreign countries, which may pose a threat to Canadian independence in some circumstances. To the extent that covert sources of intelligence are an asset in gaining access to markets and technologies and in international bargaining, Canada will be at a disadvantage with its major trading partners. However, it is by no means clear that Canada needs a secret foreign service.

In its proposals to the Committee on amendments to the *CSIS Act*, SIRC recommends that the foreign intelligence mandate of the Service be expanded. In particular, it recommends that section 16 of the *CSIS Act* be amended by removing the words "within Canada". According to Professor Peter Russell, on whose work this recommendation was based:

> This amendment of the Act would simply mean that there would no longer be a legal constraint on the Minister of Defence or Secretary of State for External Affairs should they wish to have the assistance of CSIS personnel in collecting information relating to the capabilities, intentions or activities of foreign states or persons. Already, under section 16, these Ministers can request such assistance from CSIS within Canada. With the proposed change in place, they could request this assistance outside of Canada.[1]

5.1.5 *Research Undertaken by the Committee*

In considering the SIRC recommendation that the words "within Canada" be deleted from section 16 of the *CSIS Act*, the Committee heard evidence from a wide range of witnesses, both for and against an expanded foreign intelligence mandate for CSIS.

Those in favour included the Strategic Studies Program of the University of Manitoba, Geoffrey Weller (Lakehead University), and Peter Russell (University of Toronto) and the Czechoslovak Association of Canada. They argued that the mandate of the Service should be expanded to permit independent operations overseas. Failure to do this would undermine the ability of CSIS to deal effectively with threats to the security of Canada. Close political control should be a *sine qua non* of foreign intelligence operations abroad.

Those against a foreign intelligence mandate for CSIS included Archie Barr, former Deputy Director of National Requirements, CSIS; Dr. Maurice Tugwell (Mackenzie Institute); the British Columbia Law Union; and Senator Michael Pitfield. Senator Pitfield put it clearly when he appeared before the Committee:

> . . .there are in the SIRC recommendations some issues of grand policy, and this has to do with foreign activities. Perhaps it has also to do with the Office of National Assessments. On those issues I would really argue, and try to argue as strongly as I could, that the case is not proven. I would come back to the healthy scepticism argument I tried to put earlier and say that until it is proven I would be loath to see us adding a dimension to our security and intelligence establishment that will have our agents running abroad under God knows what circumstances for God knows what purpose.

A third group of witnesses included those who argued that any proposal allowing CSIS to undertake extra-territorial operations should be implemented only after the fullest possible analysis and public discussion. This group of witnesses included Professor Jean-Paul Brodeur (University of Montreal) and the Canadian Bar Association. Professor Brodeur in particular recommended that a limited group of federal government officials and academic experts be created to examine every aspect of this question and report its findings to the Government:

> Events we are witnessing today in Eastern Europe presage profound changes in the global political situation. It would be important to know more about the direction these changes will take before becoming involved in the creation of a foreign intelligence service.

5.1.6 *Conclusion*

The Committee believes that it is inappropriate for the Service, or any other department or agency of the Government of Canada, to engage in covert unlawful acts abroad — that is, action that is above and beyond the collection of foreign intelligence —

that is clearly in breach of international law or foreign domestic law. This view was supported by Ron Atkey, the former Chairman of SIRC, when he appeared before the Committee. The Committee is nevertheless of the view that the question of whether Canada should have an agency engaged in the collection of foreign intelligence and information abroad through means that are not unlawful, and whether CSIS should be that agency, requires further examination.

If implemented, the SIRC proposal might have significant consequences for Canada, particularly with respect to the conduct of its foreign affairs and defence policies. It also remains to be proven whether CSIS has sufficient resources or the proper skills mix to meet this new challenge. The Committee believes that this matter should be examined in greater depth by an Independent Advisory Team along the lines of that created under Gordon Osbaldeston to report on CSIS.

RECOMMENDATION 19

The Committee recommends that an Independent Advisory Team be created with a mandate to examine Canada's foreign intelligence capacity.

RECOMMENDATION 20

The Committee recommends that the Independent Advisory Team study the implications of enlarging the foreign intelligence mandate of CSIS by repealing the words "within Canada" from section 16 of the *CSIS Act*.

RECOMMENDATION 21

The Committee recommends that the Independent Advisory Team ascertain, among other things, 1) whether the Service has the necessary resources and appropriate skills mix to enable it to conduct foreign intelligence operations outside Canada, and 2) whether it is appropriate for a single agency to conduct both security intelligence and foreign intelligence operations, either in Canada or abroad.

RECOMMENDATION 22

The Committee recommends that the Independent Advisory Team prepare a public version of its findings to be tabled in Parliament.

Section 16 of the *CSIS Act* does not state that the activities provided for under that section fall under the rubric "foreign intelligence". Most people envisage the Service strictly as a security intelligence agency. They do not realize that the Service does indeed have a foreign intelligence mandate, territorially limited to the collection of such

intelligence within Canada. The Committee believes that section 16 of the *CSIS Act* should be amended to include the term "foreign intelligence" in such a way as to show clearly that the activities mandated under this section constitute the collection of such intelligence. This modification would require a consequential amendment to the interpretation section of the *CSIS Act* defining "foreign intelligence".

RECOMMENDATION 23

The Committee recommends that section 16 of the *CSIS Act* be amended by adding the term "foreign intelligence" in such a way as to show that the collection and investigation activities mandated under that section constitute foreign intelligence.

RECOMMENDATION 24

The Committee recommends that the term "foreign intelligence" be added to the interpretation section of the *CSIS Act*.

5.2 The Co-Ordination, Assessment and Dissemination of Intelligence

Intelligence is useful only if the government can make good use of it. This means that the collection of both security and foreign intelligence by the different government departments and agencies — CSIS, National Defence, and External Affairs, for instance — must be centrally co-ordinated. It also implies that intelligence be properly assessed, in a uniform and cogent fashion. Finally, it presupposes that intelligence is relevant and can be disseminated to all the appropriate arms of government in a timely enough fashion for them to act on it.

5.2.1 *The Role of the Privy Council Office*

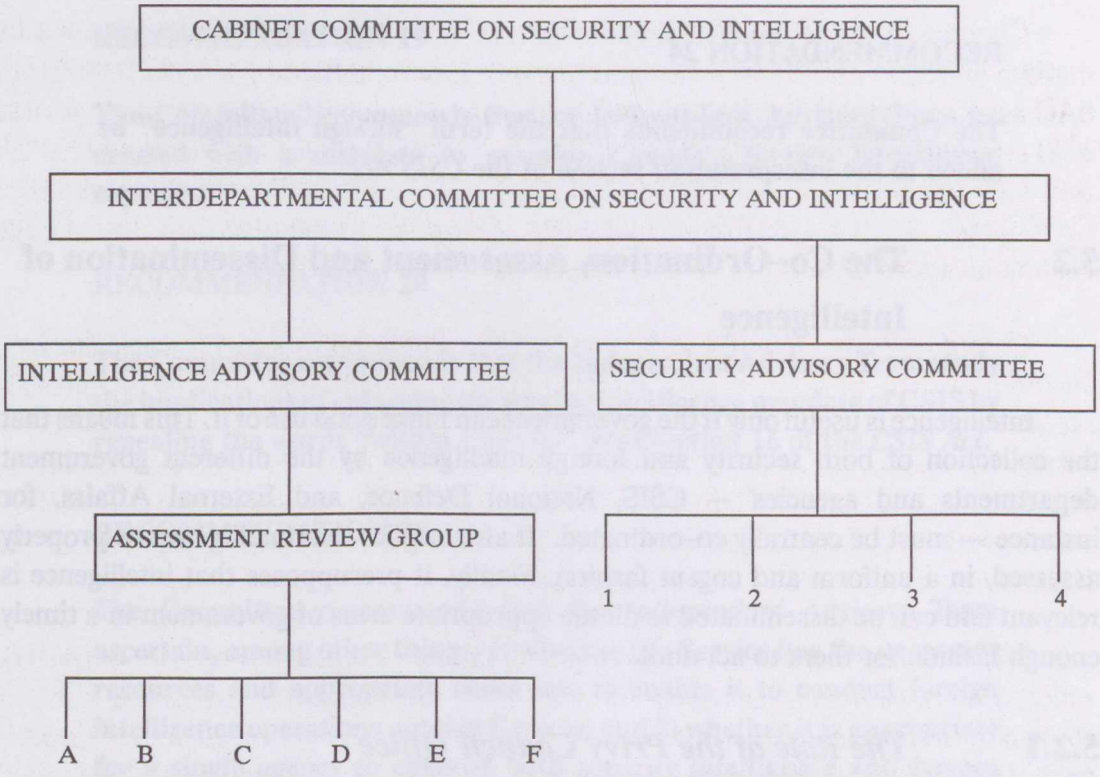
The primary function of the Privy Council Office (PCO) is to support the Prime Minister and Cabinet in the operation of the central policy decision-making process and to provide information and advice to the Prime Minister in the discharge of his or her responsibilities as head of the Government of Canada and Chairman of the Cabinet. The PCO furthermore has a central role in the co-ordination of government activities. It communicates the will of the Prime Minister to the rest of the federal bureaucracy.

On this basis, one might assume that the PCO should play an important role in security and intelligence matters. It is not altogether clear, however, that the PCO's role in security and intelligence matters is exercised to its fullest capacity.

5.2.2 *Overview of the Present Structure*

The Prime Minister and Cabinet have ultimate authority for the security and intelligence component of the Government of Canada. As Figure 5.1 indicates, however, several committees, centred around the PCO, play a role in controlling Canada's security and intelligence community, assessing its intelligence product, and co–ordinating its activities. These committees serve the Prime Minister and Cabinet by relaying the activities of the various members in the security and intelligence community to them.

FIGURE 5.1
SECURITY AND INTELLIGENCE COMMITTEE STRUCTURE



KEY

A–F = SPECIAL ASSESSMENT REVIEW GROUPS (NUMBER UNKNOWN, SUBJECTS UNKNOWN)

1 = COUNTER–TERRORISM COMMITTEE
2 = SECURITY EQUIPMENT ADVISORY COMMITTEE
3 = PUBLIC COMMUNICATIONS COMMITTEE
4 = SPECIAL THREAT ASSESSMENT GROUP

The Cabinet Committee on Security and Intelligence (CCSI) has existed since 1963. Apparently, it does not meet on a regular basis. Rather it convenes to deal with particular issues when they are referred to it.

The Interdepartmental Committee on Security and Intelligence (ICSI) is the senior committee of public servants. Chaired by the Secretary to the Cabinet, it is composed of the deputy heads of the principal departments and agencies involved in security and intelligence matters and is responsible for reviewing security and intelligence policy proposals of interdepartmental interest and for developing such policy proposals for the CCSI.

Reporting to the ICSI are the Security Advisory Committee (SAC) and the Intelligence Advisory Committee (IAC).

Chaired by the Deputy Solicitor General, SAC has responsibility for security matters having implications across government. It is supported by a small secretariat. SAC assists in formulating security policy that has interdepartmental scope. It advises ICSI on security requirements and priorities. It carries out some of its functions through four sub-committees that study specific issues. These are 1) the Counter-Terrorism Committee, 2) the Security Equipment Advisory Committee, 3) the Public Communications Committee, and 4) the Special Threat Assessment Group.

Chaired by the Deputy Clerk, Security and Intelligence, and Counsel, the IAC co-ordinates the production and dissemination of foreign and security intelligence assessments of broad governmental interest and is supported by a Secretariat. Drafts are written by officials in the departments or agencies responsible for intelligence analysis, primarily External Affairs, National Defence, and CSIS. These assessments are reviewed and revised by IAC sub-groups before approval by the IAC. The IAC also advises the ICSI as required on intelligence policy issues.

The IAC has a principal sub-committee, the Assessment Review Group (ARG), which reviews all intelligence assessments prior to meetings of the IAC. The ARG is chaired by the Executive Secretary, IAC Secretariat, and members are officials of the IAC member departments and agencies. There is also a series of Specialized Assessment Review Groups (SARGs) which are working level drafting committees. They are chaired by a member of the IAC Secretariat, and members are drawn from IAC member departments and agencies as well as other government departments as required.

5.2.3 *The Need for Change*

In its proposals to the Committee on amending the *CSIS Act*, SIRC expressed some concern that the co-ordination, assessment and dissemination of intelligence in the government may not be functioning as well as it should be. By way of a solution, SIRC recommended that Parliament examine the feasibility and merits of establishing an institution similar to Australia's Office of National Assessments (ONA). The ONA has

primary responsibility for collating and evaluating information on many political, economic and strategic matters. It is not a producer of intelligence. Rather, it assesses what Australia's intelligence agencies produce by way of intelligence assessments and reports. The ONA in turn produces reports on specific issues that are disseminated throughout government. These assist the Prime Minister, Ministers and bureaucrats in formulating policy. The ONA also assists the government in setting its intelligence priorities and requests the collection agencies to obtain specific information it lacks. The ONA consists of a mix of analysts from both the public and the private sector.

The SIRC recommendation reflects positions articulated by the McDonald Commission and the Senate Special Committee on Terrorism and Public Safety in their reports. The McDonald Commission recommended in 1980 that a Bureau of Intelligence Assessments be established to prepare estimates of threats to Canada's security and vital interests. These estimates would be based on intelligence received from the intelligence collecting departments and agencies of the government and from allied countries. The Bureau would be established in the Privy Council Office, and its Director General would report to the Prime Minister through the Secretary to the Cabinet. Likewise, the Senate Special Committee recommended that:

> . . .the Security and Intelligence Secretariat of the Privy Council Office be expanded and strengthened to provide a single focus for the gathering of intelligence and assessments from federal departments and agencies for review by the Intelligence Advisory Committee and for dissemination to the relevant federal departments and agencies.

5.2.4 *Research Undertaken by the Committee*

To evaluate the possibility of establishing the equivalent of an ONA in Canada, the Committee did a number of things. It held informal discussions with officials of the Australian High Commission in Ottawa. It discussed the issue with Members of the Parliament of Australia visiting Ottawa and involved in the oversight process in that country. It received an informal briefing from His Excellency Michael Cook, the previous head of the ONA and now Australia's Ambassador to the United States. It received correspondence from Senator William Kelly on his Committee's research on the subject. It obtained and reviewed various documents released under the *Access to Information Act*. It received an informal briefing from Ward Elcock, the current Deputy Clerk, Security and Intelligence, and Counsel, on PCO premises. Finally, it heard testimony from Blair Seaborn, the former Security and Intelligence Co-ordinator at PCO.

5.2.5 *Conclusion*

Despite these efforts, the Committee is unable to assess to its complete satisfaction whether the current system for co-ordinating, assessing and disseminating intelligence in the government is meeting Canada's security and intelligence needs. The Committee is also unable to determine to what extent the Prime Minister's Office or Cabinet make use

of security or foreign intelligence. Finally, the Committee is unable to assess how useful the security or foreign intelligence product is for consumer departments in the government.

The Committee considers that the co-ordination, assessment and dissemination of intelligence by the Government are matters of crucial importance to the national interest of Canada. Substantial changes are now occurring in the world. These changes may involve the emergence of new threats and the abatement of the more traditional challenges to national security. The Government of Canada must be in a position to assess these events and their resulting challenges. With this in mind, the Committee believes that these matters should be referred to the Independent Advisory Team whose establishment was recommended earlier in this Chapter.

RECOMMENDATION 25

The Committee recommends that the Independent Advisory Team examine the co-ordination, assessment and dissemination of intelligence in the Government of Canada.

RECOMMENDATION 26

The Committee recommends that the Independent Advisory Team examine the security and intelligence function in PCO with a view to determining whether it is accomplishing its work in this area efficiently and effectively.

RECOMMENDATION 27

The Committee recommends that the Independent Advisory Team examine the feasibility of establishing in Canada an independent Bureau of National Assessments.

NOTES

1. Peter H. Russell, "Should Canada Establish a Foreign Intelligence Agency?", Security Intelligence Review Committee, December 1988, p. 17.

CHAPTER SIX

Management Practices — Human Resources

6.1 Introduction

An organization is only as good as the people who form it. This applies to the Canadian Security Intelligence Service in the same way as it does to other agencies and departments of the government of Canada. The difference between the Service and other organizations, however, is the delicate nature of its work. The Service is one of the guardians of Canada's national security. Its work is therefore not only important, but also demanding of those who must accomplish it. In this context, human resource management practices in the Service take on added significance. A healthy work environment and a committed labour force are vital factors in determining the efficiency and efficacy of CSIS and, *de facto*, the security of Canada.

This chapter examines human resource management practices in the Service. This includes recruitment, training, career paths, and employee assistance programs. The chapter is organized into three major parts. The first part examines the legislative framework governing personnel management in the Service. The second sets out the salient events in the history of human resource management practices in CSIS. The third part analyzes the issues and problems now facing the Service with respect to human resources and establishes a series of recommendations for improving the existing situation.

It should be noted that some of the issues and problems pertaining to human resource management practices in the Service do not lend themselves easily to statutory amendments. Where necessary, therefore, the Committee will make recommendations for improvements that go beyond legislative changes to address managerial practices in the Service.

6.2 Legislative Framework Governing Personnel Management in the Service

The legislative framework governing the management of human resources in CSIS is in section 8 of the *CSIS Act*. Section 8(1) reads as follows:

> 8. (1) Notwithstanding the *Financial Administration Act* and the *Public Service Employment Act*, the Director has exclusive authority to appoint employees and, in relation to the personnel management of

employees, other than persons attached or seconded to the Service as employees,

(*a*) to provide for the terms and conditions of their employment; and

(*b*) subject to the regulations

(i) to exercise the powers and perform the duties and functions of the Treasury Board relating to personnel management under the *Financial Administration Act*, and

(ii) to exercise the powers and perform the duties and functions assigned to the Public Service Commission by or pursuant to the *Public Service Employment Act*.

This section establishes the Service as a separate employer from the rest of the public service. For security and operational reasons, the Service does not operate under the same conditions as line departments of the government of Canada. This section therefore gives the Director of the Service the power to exercise the personnel authority found in the *Financial Administration Act*.[1] These include appointment, selection standards, promotion and transfer, release, dismissal, and probationary periods. The section also authorizes the Director to exercise the authorities contained in the *Public Service Employment Act*,[2] which include training and development, position classification, rates of pay, hours of work, leave, standards of discipline, person year control, working conditions, and travel expenses.

There are several reasons for giving the Service greater flexibility than the rest of the public service in some of the major personnel areas:

1) position classification: to enable rapid re–deployment of personnel;

2) probationary period: to allow for longer periods in order to confirm reliability;

3) hours of work and working conditions: to ensure appropriate support of operational activities;

4) standards of discipline: to verify that operations and individuals are within the law and are acting in the best interests of national security;

5) staffing: to permit higher standards than those found in the public service and ensure proper psychological attitudes; and

6) training: to provide appropriate entry instruction and discipline.

Another provision governing human resources management in CSIS is section 8(4)(*a*), which states that:

> 8. (4) The Governor in Council may make regulations
>
> (*a*) governing the exercise of the powers and the performance of the duties and functions of the director referred to in subsection (1)...

This section authorizes the Governor in Council to make regulations dealing with any of the personnel management powers of the Director. It should be noted that such regulations have yet to be promulgated.

6.3 Historical Perspective

The first three years of the Service's existence witnessed difficult moments with respect to the management of human resources in CSIS. This was in part a direct consequence of the transition from the Security Service of the RCMP to the new organization that was CSIS.

More than 95 per cent of CSIS's members were transfers from the Security Service. As such, the new agency not only inherited the expertise of the Security Service, but also some of its shortcomings. The McDonald Commission noted that the lack of political acumen and analytical refinement of the members of the Security Service were two of the main reasons why the Security Service committed illegal acts and other improprieties in the 1960s and 1970s.

The subculture inherited by CSIS manifested itself in the way the Service conducted some of its activities. Early on, CSIS was criticized by the Security Intelligence Review Committee (SIRC) for casting its net too widely in the area of counter-subversion. SIRC noted in its 1986–87 Annual Report that "CSIS is expending money and effort on too many counter-subversion targets and it is intruding on the lives and activities of too many Canadians in this area." While recognizing the need for the Service to rely on some RCMP accommodations and services, SIRC saw a real necessity "to keep prodding CSIS along the civilianization path" by recruiting new members with backgrounds in areas other than investigative policing.

Two special reports, prepared early in the life of CSIS, had a significant impact on the way the Service manages its human resources: one was produced by SIRC, the other by the Independent Advisory Team (IAT).

In March 1987, SIRC presented to Solicitor General James Kelleher a Special Report dealing with official languages and staff relations in the Service. An expurgated version of the report was made available to the public in June of the same year under the title *Closing the Gaps*: *Official Languages and Staff Relations in the Canadian Security*

Intelligence Service. In it, SIRC described the situation inside CSIS with respect to official languages and staff relations.

In the area of official languages, SIRC found that a culture gap prevailed within CSIS. The Review Committee reported that despite good intentions at the top, there had not been enough real commitment among some key players within the Service to the federal government's official languages policy. In particular, SIRC noted a serious lack of understanding of Francophone culture within the Service. "CSIS too often acted like an essentially Anglophone institution," the Review Committee reported, "with French-language capability as a troublesome frill." Some of the problems noted by SIRC were under-representation of Francophones; insufficient training for Francophones in their language; and an incapacity or unwillingness by certain elements in Headquarters to communicate in French with its regional offices in Quebec.

On the staff relations side, the Review Committee remarked that a communications gap separated management and staff. SIRC noted that the situation was such that management and some employees "came to suspect the worst of each other". The communications gap manifested itself in a variety of ways. The Review Committee found that the possibility of lateral transfers within CSIS was ill-explained to employees and that there was widespread belief that competitions for promotions concealed favouritism. The Review Committee also discovered that Service employees felt frustrated by their inability to enter job competitions in the public service. All of this was a serious cause for insecurity among CSIS employees. The communications gap was blamed partly on transition, which forced managers to make decisions "founded more on intuition and experience than on planning or policy." Decisions seemed arbitrary and "lent credibility to whisperings about discrimination and favouritism." But the problem went deeper, SIRC noted, to habits of secrecy and nostalgia for a hierarchical command structure inherited from the RCMP Security Service where staff participation in the decision-making process was kept to a minimum.

The IAT's report, *People and Process in Transition*, was made public in October 1987, shortly after *Closing the Gaps*. One of the things the IAT attempted to establish was whether the Service's policies on recruitment, training and personnel management were "providing CSIS with the proper mix of skills, education and experience to meet the intelligence needs of the Government".

The IAT observed that the decision-making process within CSIS was excessively hierarchical and formal in that it tended to isolate the Director from the rest of the Service. As SIRC had done in its Special Report, the IAT reported that the organizational structure of CSIS, as well as a proclivity for secrecy within the Service, inhibited effective communication between various elements of the agency. The IAT noted that the Service had not made significant progress in improving the skills mix of its intelligence officers and that the representational picture with respect to Francophones and women was disappointing. Training and career development were observed to be "curiously lacking". The Service's management information systems were deemed inappropriate for effective

personnel management. Finally, CSIS's corporate culture was not considered to be substantially different from that of the RCMP Security Service. "After three years of transition," the IAT remarked, "CSIS still looks very much like the Security Service."

Both *Closing the Gaps* and *People and Process in Transition* made numerous and important recommendations for improving human resource management practices in CSIS. In general terms, they urged the Service to review its organizational and management structures with a view to improving communications; to correct its representational imbalances, especially with respect to Francophones, women and minorities; to diversify the skills mix of its personnel by way of a new and vigorous hiring strategy; and to provide adequate training to its employees as well as a complementary program of advancement from within.

6.4 The Present and the Need for Change

Over the past two years, the Service has undertaken a number of initiatives to correct some of the problems with its human resource management practices identified by SIRC and the Independent Advisory Team.

One such initiative is a new Human Resources Management Plan approved by CSIS in October 1988. The Plan constitutes a framework for integrating existing policies and practices and developing and implementating new ones based upon eight themes over a period of five years. These eight themes are official languages promotion; employment equity initiatives; management of employer/employee relations; career streams planning; continuous training and skills development; executive management development; automation of the work environment; and a two-way commitment between management and employees to ensure an efficient Service and a healthy work environment. Underlying the Plan is an internal communications package aimed at informing all CSIS employees of the Service's new initiatives in human resource management.

Despite this positive development, however, the Committee has found that a number of issues and problems in the area of human resource management remain to be addressed if the Service is to carry out its mandate with efficiency and aplomb in the 1990s and beyond. This part of the chapter addresses these issues as they relate to 1) recruitment and the required personnel for the Service, 2) training, 3) career paths, and 4) organizational structure.

6.4.1 *The Required Personnel for the Service*

A discussion of human resource management begins necessarily with a reflection on the personnel a security intelligence agency such as CSIS requires. The personnel needs of the Service lead in turn to consideration of two points.

The first is the security intelligence requirements of Canada as it enters the twenty-first century. The nature of present and future threats to the security of Canada

are key elements in determining the type of analysts and intelligence officers the Service needs. The world is changing at a rapid rate, and with it the nature of the threats to the security of Canada.

The second point that needs to be considered is the diverse nature of Canada's socio-cultural fabric. From a country where essentially two cultural and linguistic groups shared the benefits of a rich and varied land, Canada has now evolved into a cultural mosaic. The country has been enriched by the arrival of many ethno-cultural groups and the increased prominence of other groups, much longer established but also long ignored.

The Service must be able to adapt in the face of such change. The degree to which CSIS can acclimatize itself to new events and circumstances is in direct relation to the capacity of its people to adapt to such changes.

6.4.1.1 *Representation within the Service*

The Committee notes with approval the steps taken recently by CSIS to diversify its personnel. In September 1989, the Service undertook the most important recruitment campaign in its history. The campaign emphasized the interdisciplinary recruitment of future analysts and intelligence officers. Recruitment is being carried out by way of career shows, liaison with universities and the mass media. For instance, the Service ran advertisements in 105 newspapers across Canada in late 1989. The recruiting criteria set out in the advertisements were that applicants be Canadian citizens, possess a university degree, be prepared to work in any Canadian city, and be willing to "undergo a stringent selection and training process." The Service is using attrition as a partial basis for opening positions for recruitment. Attrition now stands at 3 per cent in the professional category (Intelligence Officers) and 7 per cent in the administrative support category.

Representation within the Service remains problematic with respect to women, visible minorities, aboriginal people, and disabled persons. It would also appear that there may still be a problem regarding the representation of Francophones in the Service.

In evidence provided to the Committee by CSIS, the Service reported on steps taken to redress representational imbalances with respect to Francophones. The Service claims that its workforce is currently 69 per cent Anglophone and 31 per cent Francophone. When CSIS was established in July 1984, Francophones represented only 15 per cent of the workforce. The Service also asserts that the percentage of Francophones in the management category rose from 20 per cent to 29 per cent in 1989-90. According to the Service, the senior management team is now 67 per cent Anglophone and 33 per cent Francophone, while in 1987 it was 83 per cent Anglophone and 17 per cent Francophone.

These numbers represent a significant improvement in the representation of Francophones within the Service. However, according to Mr. Bernard Marentette, Regional Representative, CSIS Employees' Association, Quebec Region, Francophones continue to be under-represented.

In his supplementary brief to the Committee, the regional representative claimed that Francophones are under-represented in the management category, both at Headquarters in Ottawa and in the Quebec Region. He also stated that Francophone employees of the Service in Quebec are over-represented in the administrative support group. "The most highly paid positions [in the Quebec Region]", wrote Mr. Marentette, "are generally granted to Anglophones, whereas the lowly positions are reserved for Francophones." In a letter to SIRC dated January 2, 1990, the regional representative stated that "the CSIS reports, and more particularly those on bilingualism, are pure fabrication and fiction and have been since 1984." As a result, he claims that SIRC's review of the Service's language situation, contained in the Review Committee's annual reports, are not based on complete information.

Mr. Marentette's analysis of the language situation in the Service involves more than just a review of the representational picture. He claims that Francophones receive inadequate services in their language from the CSIS Employees' Association. In his letter to SIRC, the regional representative wrote that:

> Francophone CSIS employees were never able to obtain services from their national representative in the language of their choice. Francophones continue to receive the same poor services. This injustice unfortunately persists and is due in large part to the Service's inertia in supporting the "bilingual imperative" classification of the [President, CSIS Employees' Association] position. As a result, the position remains without any linguistic designation. It is the only position in the entire organization that is not classified and that has no bilingual designation...

Finally, Mr. Marentette gave several examples in his supplementary brief of harassment by the Service of Francophone employees in the Quebec Region. He claimed that the purpose of the harassment has been to ensure that Francophone employees in Quebec reduce the number of language complaints they make, both to Service Headquarters and to the Office of the Commissioner of Official Languages. According to the regional representative, the Service's intimidation of Francophone employees in the Quebec Region has had the effect of eliminating language-related complaints:

> . . .employees can no longer complain, either inside or outside the agency, of linguistic violations or of violations of their rights. Consequently, veiled threats, intimidation and harassment have produced results: no complaints were sent to the Commissioner of Official Languages in 1989. However, the problems arising from the agency's failure to respect Francophones and comply with the *Official Languages Act* nevertheless remain intact.

Because it had only limited access to CSIS material and officials, the Committee was unable to ascertain with any certainty the state of language relations within the Service. The Service claims that the language situation is improving. However, according to the regional representative, serious problems still persist in the Service.

The Committee believes that a review of the language situation within the Service should be undertaken. Certainly, the difficulties raised by Mr. Marentette justify such a

response. The Committee believes that SIRC should assume this project because of the unlimited access it enjoys to Service officials and material. This could be done by way of a follow-up review of the section in SIRC's report, *Closing the Gaps*, dealing with language issues within the Service.

RECOMMENDATION 28

The Committee recommends that SIRC undertake a follow-up review of, and prepare a report on, language issues within the Service. SIRC's review should address 1) the possibility of representational imbalances with respect to Francophones; 2) the adequacy of services in both official languages within CSIS; 3) the accuracy of CSIS reports regarding official languages, and 4) the possibility of harassment by CSIS management of employees who make language-related complaints. A public version of SIRC's final report on official languages within the Service should be tabled in Parliament within a reasonable period.

Women represented 41 per cent of all CSIS employees as of February 1990. At first glance, this proportion appears somewhat positive, even though women do not constitute half of the Service. Further analysis yields a less encouraging picture, however. At the management level, women make up only 7 per cent of employees. Female representation at the Intelligence Officer middle management level is even less satisfactory: 2.2 per cent. These numbers are an improvement; one year ago, 3 per cent of management employees were women, while in 1988, 1 per cent of the Service's middle managers in the Intelligence Officer category were women. Yet given the importance of the representational imbalances in the Service, these improvements are minimal. The Committee believes the Service should take decisive action to correct the under-representation of women.

Disabled persons currently account for 0.9 per cent of the Service's employees, while Aboriginal persons constitute 0.2 per cent. These numbers are low when compared with those in the general population in Canada. According to the latest update of the 1988 census by Statistics Canada, disabled persons represent 12.8 per cent of Canada's population and Aboriginal persons 2 per cent. To its credit, the Service has undertaken some initiatives to correct these discrepancies. Following government guidelines, the Service aims to increase its representation of disabled persons to 5.3 per cent and aboriginal persons to 2.5 per cent by 1990. The Committee commends the Service for this undertaking.

The situation with respect to members of visible minorities is somewhat more perplexing. Members of racial minorities now make up 1.6 per cent of the Service's employees. According to the 1988 census, they account for 6.8 per cent of Canada's population. In his reply to the Committee's written questions, the Director of the Service indicated that "although the Service is still developing an employment target in this area, it is expected that we will closely follow the federal objective of 3.1 per cent representation by 1991". Why is the Service only willing to commit itself to approximating the federal

government's goals in this area? The Committee believes that the Service's intention of "closely following the federal objective" with respect to visible minority representation is not good enough. The Service should aim to achieve the federal objective in this area.

During its hearings, the Committee received evidence from organizations representing ethnic groups in Canada. Many of these, such as the World Sikh Organization and the Assembly of First Nations, manifested enmity toward the Service because of suspicions that they are being investigated unjustly by CSIS. In its brief to the Committee, the World Sikh Organization of Canada commented on whether the Service should have more or fewer investigative tools at its disposal. Its answer to this question is indicative of its feelings toward CSIS:

> It is not more or fewer investigative tools available which matter. We believe the quality of available tools should be improved. We are concerned, however, that the tools are being misused on Sikhs in Canada. For example, over 800 wire tapping of telephone calls in Hamilton case; interrogation of Sikhs at random without a just cause and forming opinions on the hearsay or unauthenticated documents. The Canadian security is not at risk from the Sikh community and we take the random interrogations a very serious violation of our individual rights. We would like this to be stopped.

The Committee believes that one way to improve the Service's image with visible minorities in Canada is to recruit more members from these communities.

The Public Service Commission (PSC) has undertaken a series of employment equity initiatives that the Service should emulate. The PSC maintains employment equity co–ordinators in its regional offices across Canada to search for and recruit qualified candidates for federal government employment. The PSC has also adopted four special measures programs. The Options Program aims to increase the representation of women in the Public Service. Positions in departments for disabled persons can be filled using the Access program, aimed at integrating people who believe that a physical, mental, psychiatric or learning disability decreases their opportunities for employment. The National Indigenous Development Program and the Visible Minorities Employment Program similarly help Aboriginal people and members of visible minorities to integrate more fully into the public service. Successful candidates who avail themselves of these programs are appointed on the basis of merit on either a term or permanent basis. The programs allow candidates the opportunity to develop new skills and qualifications through on–the–job training.

The Committee understands that the Service is in the process of developing or implementing various segments of an employment equity program. The Committee commends the Service for this and believes the implementation of this program should be completed as soon as possible. The Committee also believes the Service should not wait for women and members of minority groups to apply for positions with CSIS. On the contrary, the Service should actively seek out these people, if it does not do so already. For example, the Service could establish liaison arrangements with organizations

representing women, Aboriginal people, visible minorities and disabled persons as part of its efforts to correct its representational picture. The purpose of such liaison arrangements could be twofold: 1) to communicate to all those concerned that the Service is an equal opportunity employer, ready to recruit new, qualified members from all groups in society, and 2) to seek the help of women and minority group organizations in recruiting new members. The programs established by the Public Service Commission are also good examples of employment equity initiatives that should be emulated by CSIS.

RECOMMENDATION 29

The Committee recommends that the Service complete the development and implementation of its employment equity program by December 31, 1991. The program should aim to increase the representation of women, visible minorities, Aboriginal people, and disabled persons.

RECOMMENDATION 30

The Committee recommends that the CSIS employment equity program be based on an active, rather than a reactive strategy, in that the Service should actively seek out women and candidates from minority groups.

6.4.1.2 *Facing the Future*

While the representational picture of CSIS is important, it is only one of two factors that should be taken into consideration in recruiting new members. The other element is the ability of candidates to adapt to a new international reality and the changing nature of threats to security this implies. As indicated in the brief to the Committee prepared by the Strategic Studies Program of the University of Manitoba:

> . . .an effort is being made to have CSIS reflect the various societal elements within Canada as a whole. This effort, as well as the recent educational level of recent recruits, is to be applauded. However, a note of caution must be injected. In confronting threats to national security, the quality of the individual is paramount. It would be detrimental to Canada, and the morale of the Service, to forgo highly educated and analytically skilled individuals for the sake of too formalistic a personnel policy.

In its Second Report, the McDonald Commission addressed the issue of the desirable qualifications of an intelligence officer and analyst. The Commission noted that having a university degree should not be a requirement for joining a security intelligence agency. "University training," the Commission wrote, "is no guarantee of competence in the analytical, investigative or other types of skill required in security work."[3] The Commission recommended nonetheless that Canada's new security intelligence agency actively seek university graduates on the assumption that many who attend university will

have both the inclination and the ability required for security intelligence work. The Commission also remarked that a security intelligence agency requires people with training in a wide array of intellectual disciplines, including languages, social sciences, physical sciences, liberal arts, administration and law:

> . . .no particular degree should be declared irrelevant to the agency's work: an essential requirement is rather a capacity to obtain and weigh evidence, a capacity which may be developed in any of the intellectual disciplines.[4]

The Committee agrees with the comments of the Program in Strategic Studies and the McDonald Commission. The Service should not exclude qualified individuals who do not possess a university degree. This applies especially to people who have worked as investigators and who may have special skills that can be useful to the Service. Yet a university degree is a useful indicator of the research and analytical abilities of candidates, qualities that are of particular relevance to an agency such as CSIS.

When CSIS Director Reid Morden appeared before the Committee, he testified that the Service had virtually doubled the size of its strategic analysis unit "in the last few years". Indeed, SIRC's Annual Report for 1988–89 indicates that CSIS is now recruiting more new members with university degrees. Twenty–one of the 25 recruits for the year under review held post–graduate degrees in a variety of disciplines such as law, political science, business administration, international affairs, philosophy, geography and modern languages.

The Committee commends the Service for increasing its strategic analysis capacity and the skills mix of its employees. Given the dramatic changes occurring in the world, the Committee believes strategic analysis is a critical area for the Service in the future. The Committee was unable, however, to obtain information about the actual number of individuals working in the area of strategic analysis in the Service. It therefore cannot make a determination as to whether the resources dedicated to this function are sufficient.

A note of caution is also required. The Committee believes the Service requires a specific type of intelligence officer and analyst: someone capable of understanding the dramatic changes now taking place in the world and their impact on threats to the security of Canada. In particular, the Service needs recruits who can grasp the social, cultural, political and economic contexts from which the changing threats to the security of Canada emerge. This last point is worth expanding upon.

In a paper presented at the 1989 Annual Conference of the Canadian Association for Security Intelligence Studies (CASIS), Professor Adda Bozeman examined Asian, Middle Eastern, South American, Caribbean and African approaches to intelligence. She described what should be the characteristics of Western intelligence officers and analysts in response to security threats originating from these parts of the world. In her mind, a vital attribute is a capacity to understand the cultures, moral values, and political systems that influence and inspire security threats to Western countries:

> . . .no general intelligence schemes or particular intelligence agendas can be either constructed or deciphered unless one has come to terms with the political system and the cultural matrix in which the intelligence matter is enclosed.
>
> It is thus important to identify component elements of culture such as language, race, religion, shared historical experiences and ways of thinking, or attachment to a particular spot on earth, if one wants to learn, for example, whether a given intelligence design is authentic and apt therefore to be a constant factor in foreign affairs or whether it has been installed, decisively influenced or surreptitiously captured by forces from without — in which case it may well be perceived by knowledgeable outsiders as unpredictable but malleable.
>
> And the same preparatory homework is required if one is challenged to come to politically or academically successful terms with such particular manifestations of a given intelligence scheme as deception, covert action, or terrorism. In either instance the intelligence specialist must tap the sources of such operations in the mindsets of the counterplayers on the world's intelligence board. That is to say, he must be familiar with their basic beliefs, values and behaviour patterns as these have become registered over time before he can reliably estimate a threat, or chart a realistic counter policy or course of action.[5]

The Committee believes the required personnel for the Service should possess the analytical refinement to understand the changing nature of threats to the security of Canada. As such, the Committee believes that certain spheres of academic training and intellectual discipline are more appropriate than others if CSIS is to accomplish this goal.

To respond properly to the changes occurring in Eastern Europe and to their impact on threats originating in that part of the world, the Committee believes that CSIS should recruit individuals with backgrounds in Eastern European studies. An understanding of Soviet politics and society is not sufficient. The Service should recruit individuals who fully grasp the causes of and consequences for Canadian security of events in Eastern Europe. Individuals with backgrounds in Eastern European economics, history, sociology, philosophy and arts should be sought by the Service.

The developing world is another area where new challenges to security can emerge. The ethnic, national and religious conflicts in many regions of the developing world are in a constant state of change. The Committee believes the Service should find recruits with experience in development studies.

The question of language skills also requires some thought. SIRC noted in its 1988–89 Annual Report that of the 25 new CSIS recruits for the year under review, six were knowledgeable in at least one language other than French and English. The Committee commends the Service for this and encourages it to continue. The Committee believes that CSIS should put special emphasis on recruiting individuals cognizant of East European, Middle Eastern and Far Eastern languages in addition to those who know West European languages.

RECOMMENDATION 31

The Committee recommends that the Service continue to recruit individuals with knowledge of languages other than English and French.

6.4.2.1 *Psychological Assessments*

Psychological evaluation is an important technique for selecting recruits. It can facilitate the detection or prediction of psychological disorders. Ideally, it should identify those who may not be able to cope with the stresses associated with security intelligence work and predict non-performance or inappropriate behaviour over a career. Psychological assessment thus can help reduce training costs by giving some indication of which new members might drop out soon after recruitment.

The Service currently administers the following psychological tests when selecting new employees:

Cognitive test:	Raven's Progressive Matrices
Personality tests:	California Psychological Inventory
	Minnesota Multiphasic Personality Inventory
Vocational interest test:	Strong-Campbell Vocational Interest Inventory

Evidence received by the Committee suggests that the Service's psychological tests may be inappropriate to meet its needs. The tests used have been marketed in the public and private sectors and have been developed with a view to being applied to a wider, more general population, not a specific group such as future intelligence officers. As a result, they may have little, if any, predictive value with respect to who will develop into a good intelligence officer.

In Vancouver, the Committee heard evidence from Professor Peter McLean of the University of British Columbia. He argued that if psychological testing is to have any predictive value, it must view psychological traits as stable and enduring predispositions to behave in certain ways:

> I point this out only because some forms of psychological screening do not do that. They simply do a status report right now: currently this person is not crazy; currently this person is well adjusted.... It does not say what they are going to be like in a year or two years or three years, when they are subjected to marital problems, shift-work problems, excessive travel problems, compromise from a variety of sources.

Professor McLean claimed that the Service needed to look at three "predictor variables" or sets of information when recruiting new members. The first of these is cognitive and intellectual abilities, such as general I.Q., reading skills and certain perceptual and memory abilities. The second set of variables is personality traits that determine an individual's predisposition to depression, stress, paranoia, aggression and other traits incompatible with security intelligence work. The final set of "predictor variables" involves bio–demographical information, such as criminal convictions or job records.

The Committee is not in a position to determine whether the Service's psychological assessment program for employment purposes is adequate. The tests administered by the Service are purchased off–the–shelf and as a result may not be suited to its needs. It may be that the Service should develop its own tests to serve its specific purposes. This is increasingly the practice in the private sector.

RECOMMENDATION 32

The Committee recommends that the Service review the psychological assessment program it administers for employee selection purposes with a view to determining whether it is still current and appropriate for its needs and report to the Solicitor General on this issue within a reasonable period.

6.4.2.2 *The Polygraph*

The polygraph — commonly referred to as the lie detector — is used by most major police forces in Canada as an investigative tool to eliminate the innocent and narrow the list of suspects. It has been useful in obtaining confessions in some cases. It is also used in the workplace on prospective or current employees. Unlike in the United States, however, polygraph evidence has been considered inadmissible in Canadian courts since a ruling of the Supreme Court of Canada to that effect. The province of Ontario banned polygraph testing for screening personnel in 1983 with an amendment to its *Employment Standards Act*.

The use by the Service of the polygraph in the vetting of personnel is controversial. Currently, the polygraph is used to verify the "loyalty" of applicants for intelligence officer positions with the Service. It has already been dispensed with in vetting in–Service personnel and for enquiring into the lifestyle of candidates for positions with CSIS.

SIRC has consistently criticized the Service in its annual reports for its use of the polygraph. The Review Committee believes that the error rate associated with polygraph test results, largely recognized to be in the area of 10 per cent or more, is unacceptable. "It is too high," writes SIRC in its 1987–88 Annual Report, "to justify the mantle of science that polygraph testing can wrap around arbitrary and damaging decisions about the careers of loyal Canadians."

In the course of its work, the Committee received testimony on the reliability of the polygraph from Professor Harry Stevens of Simon Fraser University, and Dr. Ed Kramer of Psychological Services, RCMP "E" Division. The conclusion of these witnesses was that while the polygraph may be useful for criminal investigations, it is unreliable as a method for screening new recruits. Dr. Kramer observed that:

> When you use the polygraph in selection, it is very different from using it in a criminal investigation. A criminal investigation is what is called a guilty knowledge test, so you can actually look at responses to particular questions. But in a kind of general interview you do not know what the person may feel guilty about, if they have something to be guilty about, so it is a very broad questioning process.

It should be noted that the use of the polygraph by the Service is only one of many steps in the selection process to which new members are currently subjected. In testimony before the House of Commons Standing Committee on Justice and Solicitor General in 1986, Ted Finn, the Director of CSIS at the time, stated that:

> I think were it so that the polygraph was used as the single tool for determining whether someone is being reticent or untruthful in terms of the answers provided, it would be quite wrong, and if that were the case we would not be using it.

SIRC believes that the polygraph may have an impact on the selection process that is not commensurate with its level of reliability. In its 1986–87 Annual Report SIRC stated:

> Because of their false appearance of scientific rigour, the results of polygraph examinations would more often than not be accepted at face value. There would be a strong temptation to discount a contrary result from investigation, because it was subject to "human fallibility".

Finally, there is some evidence that polygraph test results can be manipulated; people can train themselves to respond dishonestly and not be detected. If this is true, the effectiveness of the polygraph in preventing foreign penetration of the Service is dubious.

The Committee understands that the Service has hired outside consultants to prepare a report on the use of the polygraph. The Committee also understands that SIRC prepared a report on the matter in June 1986. The Committee believes that the polygraph should not be used.

RECOMMENDATION 33

The Committee recommends that the polygraph not be used by the Service for employment screening purposes.

6.4.3 *Training*

The Service has undertaken a series of initiatives to improve its training programs and career development policies. Many of these are the result of recommendations made by the IAT in 1987. Information on these programs and policies was provided in the Director's written responses to the Committee's questions.

All new intelligence officers are required to attend a recently created Intelligence Officer Entry Training Course offered by the Service at its training school, the Sir William Stephenson Academy, now in Ottawa. The focus of the course is on training analysts. The course is structured in seven inter-connecting modules and lasts 13 weeks. It is delivered in a bilingual format: some sessions are provided in French, some in English and some in both official languages. Reference material is available in both French and English, and assignments can be submitted in either official language. On completion of the entry training course, the new intelligence officer is assigned a post at one of the operational units at Headquarters in Ottawa. This posting is for two years, after which the intelligence officer is moved to a different operational unit. After the third or fourth year, the intelligence officer attends the Service's Intelligence Officer Investigator Course. The course is nearing completion of its developmental stage and will be ready in the summer of 1990. Upon completion of the course, the intelligence officer is eligible for a rotational posting to a regional office as an investigator.

In the area of continuous training, the Service offers a variety of operational courses, seminars and workshops for which all intelligence officers are eligible. These relate directly to the requirements of the operational components of the Service. External courses, seminars, workshops and conferences are also available to intelligence officers.

In 1989, CSIS initiated a three-year career and skills development program for senior managers. The program aims to send all senior management staff to the Public Service Commission's Management Orientation Courses for SM and EX level employees.

Finally, monthly orientation courses are currently being offered to all new employees, in the language of their choice, at the CSIS Training Centre in Ottawa.

The Committee commends the Service for its initiatives in the area of employee training and development and encourages it to continue along this path. None of the evidence collected by the Committee indicates, however, whether the Service has in place a procedure for its training and development programs. The purpose of such a validation procedure would be to verify the impact of the Service's training and development programs on performance in the field. The Committee believes that a validation procedure would be useful to the Service, if it does not have one already, in ensuring that its training and development programs stay relevant to employee needs and pertinent to CSIS requirements.

The Committee heard evidence in Vancouver from various witnesses on simulation training, which it found most interesting. Simulation training is a teaching technique that

allows students to learn through role-playing. Trainers create and put their students in fictitious situations where one or more problems need to be resolved. The simulations imitate circumstances that might arise in the course of an employee's work life. The trainees are required to use the skills learned in the classroom to resolve the problems put to them in the simulation. Simulation training is a new but increasingly popular pedagogic method, especially with police forces.

The Committee was unable to ascertain to its full satisfaction whether the Service provides some form of simulation training to its recruits. The Committee believes that the Service should consider putting in place such programs. Simulation training has many advantages over instruction techniques based on lectures. Simulation engages trainees in an activity where the skills they need most can be developed through realistic situations. The Committee believes that a combination of didactic teaching and simulation training is best. As Professor John Yuille of the University of British Columbia told the Committee:

> Any job that is like police work needs a very large component of this kind of simulation training in which someone defines in advance the skill sets necessary to do the job, then every attempt is made to supply training techniques that improve them. I think an hour of simulation training is probably worth ten hours in the classroom.

Finally, as Professor Yuille pointed out to the Committee, simulation training provides advantages from a cost benefit point of view. Without simulation training, CSIS officers may end up having to learn their job in the field. This trial and error way of learning may lead to the inculcation of bad habits and out-of-date practices. In the end, the taxpayer is likely to be the loser in that employee performance during the initial stages after recruitment may be poorer than it would otherwise be.

A final issue that needs to be considered is language training within the Service. When Paul Gibson, President of the CSIS Employees' Association, appeared before the Committee, he testified that only part-time French language training is available to CSIS employees in Toronto and in areas west of Toronto. This apparently creates frustration among some CSIS employees in these regions as many promotional opportunities within the Service require a level of proficiency in French that they find difficult to reach through part-time training.

If the career development system is to be fair and equitable, the Committee believes that full-time second language training should be available to all members of the Service wherever they work.

RECOMMENDATION 34

The Committee recommends that the Service establish full-time second language training programs in all regions of the country. In particular, the Committee recommends that immediate action be taken by the

Service to provide full-time French language instruction to its employees in Toronto and areas west of Toronto.

An excellent way to improve proficiency in a second language is to use it every day. Recruits who graduate from the Intelligence Officer Investigator Program are posted to one of the Service's regional offices. The Committee believes that the Service should encourage CSIS employees to obtain a posting in a region of Canada where the official language of the majority is different from their own. English-speaking intelligence officers could avail themselves of a posting in Quebec, and Francophone intelligence officers could be posted to predominantly Anglophone areas.

RECOMMENDATION 35

The Committee recommends that the Service make available to its intelligence officers postings in areas of the country where the language of the majority is different than their own language.

6.4.4 *Career Paths*

A number of deficiencies have come to the Committee's attention regarding career paths and possibilities for employee advancement within the Service.

One of the problems raised is the difficulty faced by employees of the Service in transferring to or competing for jobs in the rest of the public service. The Service enjoys the status of a "separate employer" in the federal government. This means that CSIS employees cannot compete for public service positions unless a competition is specifically open to them. With respect to transfers to the public service, it would appear that the difficulty lies in the wording of sections 66(1), (6) and (7) of the *CSIS Act* (transitional provisions and consequential and related amendments). These read as follows:

66. (1) Subject to subsection (5):

(*a*) all officers and members of the Force, and

(*b*) all persons appointed or employed under the *Public Service Employment Act* assigned to the security service immediately prior to the coming into force of this section become employees of the Service on the coming into force of this section.

66. (6) Every person mentioned in subsection (1) who was employed or appointed pursuant to the *Royal Canadian Mounted Police Act* is, in the period of two years after the coming into force of this section, deemed to continue to be employed in the Force pursuant to that Act

for the purpose of being eligible to request in writing a transfer to perform duties and functions under that Act.

66. (7) Every person mentioned in paragraph 1(*b*) is, in the period of two years after the coming into force of this section, deemed to be employed in the Public Service within the meaning of the *Public Service Staff Relations Act* for the purpose of being eligible to be transferred under the *Public Service Employment Act*.

It has been argued by the Public Service Alliance of Canada (PSAC) that because the transitional measure under section 66(7) expired two years ago, employees of the Service provided for under that section have no guarantee that they can transfer to other positions in the public service.

The difficulty of transferring to the public service or competing for jobs in other departments and agencies of the government is a source of frustration for CSIS employees. As Paul Gibson, President, CSIS Employees' Association, stated before the Committee:

> Most of our membership does not wish to pursue a career in the rest of the Public Service. However, most of them would like access, in order to improve their skills so they could gain promotion within the Service. They would like secondment, temporary assignments.

The Committee sympathizes with the employees of the Service on the issue of access to public service positions and believes that action should be taken immediately to correct this situation. CSIS employees should be able to transfer to or compete for positions in the public service in the same way as the majority of government employees. Access to the public service would also give employees who are unlikely to obtain promotion within the Service a chance to develop useful and rewarding careers elsewhere. Finally, public service access would be beneficial to CSIS by allowing its personnel to upgrade their skills through secondment. For these reasons, therefore, the Committee believes Service employees should be allowed complete access to employment opportunities in departments and agencies of the federal government.

SIRC advised in *Closing the Gaps* that the Service should explore ways of permitting its employees to enter the public service more easily. The IAT also suggested in its report that "the career path of CSIS staff should provide for movement within both the security intelligence community and the Public Service generally when the qualifications are appropriate to the position/opportunities available...". The Committee is surprised that more than three years after these two reports were made public, the impediments to access to the public service for CSIS employees are still present. The Committee believes that legislative guarantees should be given to employees of the Service so that they can transfer to or compete for positions in the public service. This would assure employees of the Service access to the public service regardless of CSIS policy on the issue.

RECOMMENDATION 36

The Committee recommends that the employees of the Service be given access to all public service competitions and an opportunity to participate in secondment and temporary assignments in the public service.

Another problem faced by CSIS employees concerns career progression within the Service. In documentation titled *Proud to Serve* a collection of brochures explaining the Service's Human Resources Management Plan — CSIS states that "one of the top resource management priorities is career streams planning for every employee." However, career advancement within CSIS is not always applied to the satisfaction of the employees of the Service. PSAC stated in its brief to the Committee that:

> Prior to and since transition, CSIS has espoused that it was a career oriented employer. Employees were led to believe that they could progress from the entrance levels to the management levels, as long as they possessed the necessary skills, education and knowledge. Now, more and more frequently they face roadblocks and changing policies which do not allow for career progression.

PSAC has gone so far as to conclude that "the merit system is non–existent within the Service."

The reasons for this difficulty lie in the fact that the Service is a relatively small organization when compared with other departments and agencies of the federal government. Recently, the Service and the CSIS Employees' Association have put a good deal of effort into producing a "Career Streams" policy, which will soon be released. The policy will provide a framework for the development of careers in the context of the Service's organizational needs. According to the CSIS Employees' Association, however, the policy does not necessarily view "career" and "promotion" as synonymous. There are a finite number of supervisory/management positions in an organization the size of CSIS, and employees are more likely to face the prospect of horizontal, rather than vertical, career moves. The CSIS Employees' Association accepts this constraint. What it cannot accept is that despite this situation, the Service continues to hire individuals from outside CSIS to fill middle and senior management positions:

> . . .employees perceive career to mean promotion and the blocking of the diminishing number of supervisory/management positions by outside people is frustrating and demoralizing to Association members committed to pursuing a future with CSIS.

The Committee sympathizes with the difficulties faced by CSIS employees on this issue. It is important to understand, however, that the Service has been under great pressure over the past few years to diversify the skills mix of its personnel at both the intelligence officer and the management level. The Committee approves of this diversification process and encourages the Service to continue along this path.

Nonetheless, the Committee recognizes that a problem may exist with respect to the career paths of Service employees, especially former RCMP members who joined CSIS fully expecting to be able to fulfil their career ambitions within the new agency.

The Committee believes that the Service should recognize the aspirations of these employees, while continuing to pursue its objective of diversifying the skills mix of its personnel. As the IAT stated in its report, any program to improve the mix of skills and talent from the outside must not be seen as unduly restricting advancement. "A good career development program," the IAT remarked in its report, "is essential."

RECOMMENDATION 37

The Committee recommends that the Service recruit from the widest possible population base — that is both within and outside government — for all middle and senior management positions with the Service, while making every effort to identify qualified candidates already inside CSIS who may possess the required qualifications.

6.4.5 *Employee Assistance Programs*

Emotional stability and adaptability are important requisites for intelligence work. Intelligence officers often operate in stressful situations where even their personal security may be in danger. In addition, the rapidly evolving nature of threats to the security of Canada carries its share of anxieties. These stresses are compounded by the isolation intelligence officers and analysts often face in their work. Professor Peter McLean of the University of British Columbia put it this way in describing to the Committee the impact of isolation on security service members:

> They do not have available to them the same kind of support. They may not be able to go home and talk to their spouses about what they did that day. They may not be able to chat over the fence and get the same sort of social support the rest of us do in the conduct of our routine activities. These folks have to be "lone rangers" from time to time from the point of view of being quiet and so on, which induces a fair amount of stress.

It is therefore essential that CSIS intelligence officers have adequate employee assistance programs available to them, and in particular psychological counselling services, if they are to carry out their work effectively.

The Service has a contract with CanCare, a private referral company for individuals who may require counselling. CSIS employees may call CanCare from anywhere in Canada and request a referral for counselling on issues such as psychological problems, alcohol abuse, financial difficulties and family problems.

When Paul Gibson appeared before the Committee, he testified that, in his opinion, the Service's employee assistance programs were good. He assured the Committee that

employee problems are handled with the strictest confidentiality in the Service. He did admit, however, that the Committee would have a better idea of the effectiveness of the Service's employee assistance program if it addressed the program's consumers.

The Committee was unable to talk to CSIS employees who have used the services provided by CanCare. When in Vancouver, however, the Committee heard testimony from experts in the area of employee assistance programs. Professor Harry Stevens of Simon Fraser University put it this way before the Committee:

> I do not have any great detailed knowledge about CanCare per se, and I do not mean to select them and criticize them; but an organization of that nature simply works primarily on a referral basis without having individuals, be they psychologists, psychiatrists, social workers, or whatever, who may be within CanCare, selected specifically to meet the type of problem that a law enforcement community individual is going to have or a security individual is going to have. I could be wrong, but that is my belief. I do not think they have that level of specialty in their organization.

The Committee did not examine the quality of the services provided by CanCare. The Committee nevertheless believes that the Solicitor General's Department should review the services rendered by CanCare with a view to determining whether these are appropriate to the needs of CSIS employees.

The Committee understands that the RCMP has a well established internal employee assistance program. The Solicitor General's Department may wish to consider whether it would not be better for employees of the Service to avail themselves of the RCMP employee assistance program. Given that the Service and the RCMP are both investigative agencies, this may prove to be a more efficient and cost-effective way of making employee assistance available to CSIS members.

RECOMMENDATION 38

The Committee recommends that the Solicitor General's Department study the feasibility of extending the RCMP Employee Assistance Program to members of the Service.

NOTES

1. RSC, 1985, c. F–11.

2. RSC, 1985, c. P–33.

3. Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (McDonald Commission, 1981), Second Report, Volume 2, p. 709.

4. McDonald Commission, Second Report, Volume 2, p. 710.

5. Adda Bozeman, Non–western orientations to political intelligence and their relevance for western national interests, Paper presented at the CASIS Annual Conference, Ottawa, September 28–30, 1989.

CHAPTER SEVEN

Management Practices — Labour Relations

7.1 Introduction

The Committee is interested in labour relations within the Service for a variety of reasons.

First, good labour relations can have a positive impact on efficiency and effectiveness. Healthy labour relations therefore help ensure that the Service properly fulfils its responsibility to protect national security. Second, labour relations can influence the state of morale in the Service and affect how members of the Service carry out their duties.

The Committee is also interested in labour relations within the Service because it is an issue that has received little attention over the past few years. The Special Committee of the Senate that reviewed Bill C–157 did not fully tackle the issue in its report, nor did the McDonald Commission delve into it in any great detail.

The Service has put in place new programs and policies to improve its labour relations. For instance, in each regional office, CSIS has instituted Local Management Consultation Committees. They deal with issues raised by either management or employees and lead to National Labour Consultation meetings held four times a year. The Service has also established an Occupational Health and Safety Council which provides a monthly opportunity for management and labour to discuss working conditions within CSIS. Finally, the Service has signed a Memorandum of Understanding with the CSIS Employees' Association enabling employees to bring disciplinary issues to the Public Service Staff Relations Board.

The Committee commends the Service for these initiatives. However, evidence received by the Committee from organizations representing the members of the Service indicate that CSIS employees are disadvantaged in two respects compared with workers in the rest of the public service. First, they are excluded from the right to collective bargaining and to the legal entitlements that accompany it. Second, they do not have recourse to the same grievance and adjudication procedures as other members of the public service.

This chapter reviews the structure of labour relations within the Service; examines the restrictions on the right to collective bargaining and the limitation on the right to grieve imposed on employees of the Service; and makes observations about the application of "grandfathered" benefits in the Service.

7.2 The Structure of the Labour Force in the Service

The Service's labour force is divided into those who may avail themselves of the rights and entitlements provided for under the *Public Service Staff Relations Act* and those who may not. The *Public Service Staff Relations Act* governs collective bargaining, grievance hearings and adjudication in the public service. Section 2(*f*) of the interpretation section of the *Public Service Staff Relations Act* excludes certain types of people from the rights and entitlements available under the Act. It states that:

> 2. In this Act, "employee" means a person employed in the Public Service, other than...
>
> (*f*) an employee of the Canadian Security Intelligence Service who is not within the occupational category described as administrative support..."

One of the impacts of section 2(*f*) of the *Public Service Staff Relations Act* is to exclude from union membership and collective bargaining some 800 CSIS employees in occupations ranging from chauffeurs to cleaners to psychologists as well as all the Service's intelligence officers. These employees, about 75 per cent of the Service's total work force, are represented by the CSIS Employees' Association. The Association is not a certified bargaining agent under Canadian labour legislation. It exists solely by virtue of agreements between the Director and the Association and is provided for in the Service's Administration Policy Manual. About 500 of the Service's employees — those in the administrative support category — are represented by the Public Service Alliance of Canada (PSAC). These include clerks, typists, secretaries, and duplication equipment operators. They all have the right to collective bargaining.

7.3 Collective Bargaining

Two sections of the *CSIS Act* affect collective bargaining in the Service. The more important of these is section 8(1)(*a*). It states that:

> 8. (1) Notwithstanding the *Financial Administration Act* and the *Public Service Employment Act*, the Director has exclusive authority to appoint employees and, in relation to the personnel management of employees, other than persons attached or seconded to the Service as employees,
>
> (*a*) to provide for the terms and conditions of their employment...

The terms and conditions of employment of members of the Service represented by PSAC are provided for by collective agreements. Since 1984, there have been four collective agreements between PSAC and the Service. The current collective agreement was signed on March 30, 1990 and expires December 31, 1990.

The general employment framework for members of the Service represented by the CSIS Employees' Association is found in the Administration Policy Manual of the Service. The CSIS Employees' Association makes representations to the Director on pay, benefits and working conditions. In his testimony before the Committee, Paul Gibson, President of the Association, referred to this process as a discussion rather than a negotiation. The CSIS Employees' Association is moving in the direction of co–operative initiatives with the Service. An example of this is the "Career Streams" policy, a career development scheme developed jointly by the Service and the Association.

The second section in the CSIS Act that affects collective bargaining is section 9(1). It states that:

> 9. (1) Notwithstanding the Public Service Staff Relations Act,
>
> (*a*) the process for resolution of a dispute applicable to employees of the Service in a bargaining unit determined for the purposes of that Act is by the referral of the dispute to arbitration...

This section provides that the employees in the bargaining unit established for CSIS — i.e., those in the administrative support category — do not have the right to strike. The only route available for the resolution of collective bargaining disputes is through arbitration by the Public Service Staff Relations Board.

The inability to form a collective bargaining unit is a cause for concern for many 95 CSIS employees, both unionized and non–unionized.

One of the consequences of the present legislative framework governing collective bargaining in the Service is that the existence of the CSIS Employees' Association is very tenuous. Because the Association owes its existence to the Administrative Policy Manual, changes to the Association's composition, mandate and structure can be made unilaterally by CSIS management. Indeed, there is nothing to keep the Service from abolishing the Association if it wants to do so. A statement by Paul Gibson when he appeared before the Committee is revealing on this issue:

> In the past, our relationship with management has not been that good. We have been up and down, and in the future, I am sure things will be up and down.
>
> At the present time I think we are on a pretty even keel. We have like–minded people within the Association and in management ... Our concern lies in the fact that in the event the personalities change — as you heard the union people say — and the philosophies change, we could be out. We could be done away with the stroke of a pen...

The restrictions on the right of CSIS employees to unionize also creates problems for PSAC. In its brief to the Committee, PSAC indicated that the Service may be willing to

reclassify occupations out of the administrative support group category, which would have the effect of restricting the right to collective bargaining of certain CSIS employees. Under the *Public Service Staff Relations Act*, an employer is required to argue, on merit, for such an exclusion. PSAC was unable to provide evidence that the Service had undertaken any initiatives of this sort because of the secrecy it says applies to routine affairs within CSIS. Nonetheless, PSAC states in its brief to the Committee that:

> . . .when we asked CSIS to provide job descriptions and other relevant information pertaining to an exclusion request in the past, the application was withdrawn and the affected positions were unceremoniously reclassified out of the bargaining unit.

The Committee believes the legislative framework affecting collective bargaining within the Service is wanting. In particular, section 2(*f*) of the *Public Service Staff Relations Act*, which restricts the right to collective bargaining for 75 per cent of the employees of the Service, is inappropriate. All employees of the Service should have the right to enjoy labour representation similar to that provided to employees in the rest of the public service. Members of the CSIS Employees' Association should have the same rights to collective bargaining as those now enjoyed by their fellow employees represented by PSAC.

7.4 Grievance and Adjudication Rights

Section 2(f) of the *Public Service Staff Relations Act* also has the effect of restricting the adjudication rights of CSIS employees not in the occupational category described as administrative support. Under the *Public Service Staff Relations Act*, an employee has the right to present a grievance to either the employer or the Public Service Staff Relations Board. A grievance may deal with the interpretation or application, in respect of the employee, of a statute, regulation, by-law, direction or other instrument; a provision of a collective agreement or an arbitral award; or any occurrence or matter affecting the terms and conditions of employment of the employee. If the grievance has not been dealt with to the satisfaction of the employee, the employee may refer the grievance to adjudication by the Public Service Staff Relations Board. Matters referred to adjudication can deal only with the interpretation or application in respect of the employee of a provision of a collective agreement or an arbitral award, or disciplinary action resulting in discharge, suspension or a financial penalty. These procedures are not available to CSIS employees because section 2(*f*) of the *Public Service Staff Relations Act* does not recognize them as employees for the purposes of that Act.

Section 8(2) of the *CSIS Act* governs the conduct of grievance procedures within the Service and reads as follows:

> 8. (2) Notwithstanding the *Public Service Staff Relations Act* but subject to subsection (3) and the regulations, the Director may establish procedures respecting the conduct and discipline of, and the

presentation, consideration and adjudication of grievances in relation to, employees, other than persons attached or seconded to the Service as employees.

This section provides that the Director may, subject to regulations passed by the Governor in Council, determine procedures respecting the conduct, discipline and the presentation of grievances by employees.

When the Service was established, certain rights formerly enjoyed by members of the RCMP Security Service disappeared, among them the right to submit grievances to three-member grievance committees. These committees were created as the need arose and were composed of one person representing the employees and two other high-ranking employees acceptable to both parties. Grievances filed by non- unionized employees of the Service are now resolved at one of three levels within CSIS: the Regional Director, the Director of Human Resources and Official Languages, or the Director of the Service. Grievance committees are struck only rarely, and when they are, it would appear that their membership is drawn exclusively from management. Bernard Marentette, Regional Representative of the CSIS Employees' Association for the Quebec Region, stated in his brief to the Committee that:

> In only one case over the past few years was it possible to have the matter referred to a review committee. However, the three members of the committee are appointed by management, and the extremely restrictive guidelines do not allow representatives of the employee involved to take part. The committee normally comprises one or two employees from Personnel and the immediate supervisor of the employee at the centre of the investigation. There are serious doubts about the objectivity of these committees because some of their members may be in a conflict of interest, notably the manager who is investigating the quality of his own management skills. He would not want to lose face by acknowledging the validity of the complaints filed by his subordinate. Nor would he want to admit that the complaints about his employee were legitimate as this would affect his efficiency bonus.

The Committee believes it is inappropriate for employees of the Service not to have the same grievance and adjudication rights as employees in the rest of the public service. CSIS employees are virtually alone among full-time, permanent, federal public servants in not having access to the adjudication procedures provided for under the *Public Service Staff Relations Act*. Members of the Royal Canadian Mounted Policed are also excluded, but now have their own grievance process under Part III of the *Royal Canadian Mounted Police Act*.

7.5 The Right to Unionize

It has been argued that members of a security intelligence agency should not, for security reasons, be allowed to unionize. In particular, the McDonald Commission, in its Second Report, discussed the possibility of union-management relations becoming so

embittered "that the risks of damaging leaks of information, or even an enemy penetration, become unacceptably high."[1] The Committee understands this argument, but does not agree with it. If anything, the absence of a union creates frustration among the members of the Service, which in turn may lead to anger and resentment. The presence of a union and the recognition of collective bargaining rights provide a mechanism whereby issues causing friction and frustration can be addressed effectively and resolved.

The Director of CSIS, when he appeared before the Committee on June 5, 1990, stated that he would not oppose the unionization of members of the Service represented by the CSIS Employees' Association, provided that there was some form of arbitration to cover potential strikes.

RECOMMENDATION 39

The Committee recommends that all persons employed by the Service should have the right to unionize under the *Public Service Staff Relations Act*.

7.6 The Right to Strike

The Committee also agrees with the Director that it would be inappropriate to grant employees of the Service the right to strike. The Service has a duty to protect Canada against threats to its security, and it should not be frustrated in the conduct of this activity by strike action by its employees. However, the Committee believes that the determination as to which employees of the Service should have the right to strike should be left to the Public Service Staff Relations Board. The *Public Service Staff Relations Act* provides that an employer may request the Public Service Staff Relations Board to designate some or all of its employees as persons necessary in the interests of the safety or security of the public. Any employee so designated loses his or her right to strike but keeps all other collective bargaining rights.

RECOMMENDATION 40

The Committee recommends that the determination of who in the Service should have the right to strike should be left to the Public Service Staff Relations Board.

7.7 Designation – Management Category

It is accepted practice that an employer, in establishing a framework for management–labour relations, should be able to designate certain persons within an organization as being part of the management category. The *Public Service Staff Relations Act* provides that an employer may request the Board to designate employees as

"person[s] in a managerial or confidential capacity". The impact of this is that such employees do not form part of any bargaining unit. Section 2 of the *Public Service Staff Relations Act* stipulates that a person employed in a managerial or confidential capacity is any person who is employed in the public service "who should not, in the opinion of the Board, be included in a bargaining unit by reason of the duties and responsibilities of the person to the employer".

The difficulty with the "managerial or confidential" designation category of the *Public Service Staff Relations Act* is that the Service could request, and the Board could rule, that all CSIS employees, not just those in the managerial category, be designated "confidential employees", simply by virtue of the work they do. All employees of the Service could thus lose the right to collective bargaining and their right to grieve the interpretation or application of their collective agreements. While the Committee believes that it is appropriate for the Director to request his senior managers be excluded from bargaining units within the Service, the Committee holds that to use the designation "managerial or confidential" in an overly broad sense would be inappropriate.

RECOMMENDATION 41

The Committee recommends that the *CSIS Act* or the *Public Service Staff Relations Act* be clarified to confirm that employees of the Service are not to be excluded from collective bargaining under section 2 of the *Public Service Staff Relations Act* as "managerial or confidential" employees only because the employees have access to confidential matters concerning national security.

7.8 Collective Bargaining Rights

The recognition of collective bargaining rights necessitates consequential amendments to the *CSIS Act* and the *Public Service Staff Relations Act*.

Section 9(1) of the *CSIS Act* excludes CSIS employees in a bargaining unit from the right to strike and provides arbitration as the only means for the resolution of a dispute applicable to that bargaining unit. In order that the employees of the Service may have the same rights and entitlements under the *Public Service Staff Relations Act* as their counterparts in the rest of the public service, section 9(1) should be repealed.

RECOMMENDATION 42

The Committee recommends that, to ensure that employees of the Service have the same collective bargaining rights as workers in the rest of the public service, section 9(1) of the *CSIS Act* be repealed.

The Committee also believes that section 2(*f*) of the *Public Service Staff Relations Act* should be repealed. This would accomplish two things. First, it would give all employees

The Committee also believes that section 2(*f*) of the *Public Service Staff Relations Act* should be repealed. This would accomplish two things. First, it would give all employees of the Service the same collective bargaining rights and entitlements as those enjoyed by employees in the rest of the public service. Second, it would give members of the Service the same grievance and adjudication rights as those given employees in the rest of the public service.

RECOMMENDATION 43

The Committee recommends that section 2(*f*) of the *Public Service Staff Relations Act* be repealed, thus recognizing the same collective bargaining, grievance and adjudication rights for all employees of the Service as are granted to workers in the rest of the public service.

The Committee believes these modifications constitute an improvement over the existing situation. The Committee also believes that if the proposed legislative framework governing labour relations in the Service is to function properly, CSIS management must be well informed about the acts, regulations, agreements and recourse procedures pertaining to members of the Service. PSAC has suggested to the Committee that CSIS management may not be as familiar as it should be with the rules and regulations pertaining to the unionized portion of the Service.

7.9 Employment Benefits

Section 66(2) of the *CSIS Act* (Part V: Transitional Provisions and Consequential and Related Amendments) provides that all employees of the Service who were formerly with the Security Service of the RCMP will continue to have employment benefits equivalent to those they had before joining CSIS,

> 66. (2) . . .until such a time as those benefits are modified pursuant to a collective agreement or, in the case of persons not represented by a bargaining agent, by the Service.

Representatives of the CSIS Employees' Association have taken issue with this provision. They object to the fact that CSIS may unilaterally modify benefits acquired in transferring from the RCMP to the Service. According to the CSIS Employees' Association, many of the employees it represents fear they may eventually lose their benefits because of section 66(2).

The CSIS Employees' Association recommended to the Committee that section 66(2) be rewritten to prohibit the Service from modifying these benefits unilaterally. The Committee agrees with this recommendation. The Committee believes that the Service should seek the consent of CSIS employees individually before modifying their benefits.

RECOMMENDATION 44

The Committee recommends that section 66(2) of the *CSIS Act* be amended to provide that the benefits accruing to former members of the RCMP be modified or removed only after management has obtained the prior consent of the individual employees concerned.

NOTES

1. Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (McDonald Commission, 1981), Second Report, Volume 2, p. 724.

CHAPTER EIGHT

Control of and Accountability for the Security and Intelligence Process

8.1 Control and Accountability

Accountability and control are frequently used as if they were interchangeable terms. In the security and intelligence context, they should not be. Whereas control is exercised by a variety of participants — some political, some bureaucratic — and involves efforts to ensure that operational activities of government departments and agencies occur as effectively and efficiently as possible within an approved set of rules, accountability concerns the process of making individual participants within a system answerable for the activities for which they are politically or bureaucratically responsible.

8.1.1 *Rules*

Security and intelligence functions performed by arms of the government of Canada are effected by way of three general categories of rules — statutes, policies and protocols. Functions performed by agencies for which the Solicitor General is responsible and accountable are governed largely by statute. The *Department of the Solicitor General Act*, the *Canadian Security Intelligence Service Act*, the *Royal Canadian Mounted Police Act*, the *Security Offences Act*, the *Criminal Code* and a number of other acts collectively provide specific authority to establish control over CSIS and the RCMP. By comparison, functions performed across government, such as administrative security — that is, the process by which certain types of national assets are protected and individuals vetted for their loyalty to Canada — have generally been governed by policy instruments, not statutes. Both statutes and policies differ from certain foreign intelligence gathering activities, which have been governed historically by secret protocols and agreements between Canada and its allies.

8.1.2 *Accountability*

While controls have always resulted in practice from statutes, policies and protocols, the capacity to call responsible people to account for the activities of Canada's security and intelligence community has, until recently, existed largely only in theoretical terms. Traditionally, most states, even liberal democracies like Canada, have been reluctant to divulge information about security and intelligence matters. This cult of secrecy grew out of a period — World War II — when intelligence was seen initially as a prerequisite for

Allied survival and later for victory. With the emergence of the so–called Cold War, the rationale for secrecy was all too easily justified. Not until the 1970s, when intelligence agencies in several countries were seen to have gone beyond their mandates, was there any attempt to make such agencies more accountable.

Despite the subsequent change in climate during the 1970s and early 1980s, legislators in Canada, as elsewhere, have experienced a continued reluctance on the part of security and intelligence agencies to reveal information about their activities. Likewise, those responsible and accountable for them have persisted in not giving full and clear answers when elected representatives have attempted to obtain information through avenues that were normally available to them, such as question period and committee hearings on the Estimates.

The passage of the *CSIS Act* and the *Security Offences Act* in 1984 tipped the balance dramatically in favour of greater public access to those involved in security intelligence work by placing certain political actors who were responsible for one sector of the security and intelligence community under an obligation to provide reports. This was achieved by establishing review bodies that were obliged by law to provide the Solicitor General, the Minister responsible for the new agency, with reports detailing the degree to which CSIS had complied with the law and had operated effectively and efficiently. Further, in the case of the Security Intelligence Review Committee (SIRC), the Minister was obliged to table a copy of its annual report with Parliament within a fixed period.

True accountability, that is, where the responsible ministers are forced to account for the actions of the public servants who report to them, does not result merely because there is a law placing a particular political actor under an obligation to provide a specific report. It depends, in the long run, on Members of Parliament, the people with the authority to call for accounts, exercising their prerogative. This exercise of prerogative, it should be emphasized, depends in turn on two elements. Both relate to the knowledge possessed by those with the authority to exercise the prerogative. They need to know the full extent of the powers available to them. In the case of Members of Parliament, it also includes the right to call for people, papers and records and to recommend a reduction of items in the Estimates. But such a capacity is of value only when those exercising such powers have knowledge of the area in question and know which persons to call before them and which records to demand.

The work of the Committee gave its members an ideal opportunity to extend their knowledge of security and intelligence matters. This opportunity was limited, however, by the actions of members of the intelligence community who limited their contribution to what they saw as being strictly necessary for the review, not what members of the Committee and its staff thought was appropriate.

Largely because the Committee was unsuccessful in gaining access to all it believed was appropriate for it to see, the Committee is recommending certain changes to the *CSIS Act*. These changes will make it possible for future committees of Parliament not only to

call responsible ministers and senior public servants to account, but also to be informed in full and material detail about the whole field of endeavour.

The core of these recommendations concerns the roles of SIRC, the Inspector General of CSIS, and Parliament. These recommendations are laid out in detail later in the Report.

First it is important to set out the Committee's views concerning the current roles performed by key participants under the *Department of the Solicitor General Act*, the *CSIS Act*, and the *Security Offences Acts*.

8.2 The Department of the Solicitor General Act

8.2.1 *The Ministry as a Whole*

Until the mid-1960s, the Minister of Justice and the Attorney General of Canada had responsibility for all policing, penitentiary and parole matters falling within the federal domain. Following the publication of the Glassco Report, Parliament passed legislation — the *Government Organization Act* — transferring responsibility for the agencies that carry out these functions to a new ministry, the Department of the Solicitor General.

Just five sections in length, the *Department of the Solicitor General Act* provided for the appointment of a Solicitor General with general managerial and directorial responsibilities for the department as a whole, and for the appointment of a Deputy Solicitor General.

Unlike other departments, where the deputy minister has managerial responsibility for departmental activities, the Act did not require the agency heads to report to the Deputy Solicitor General. Instead, they report directly to the Solicitor General as the minister responsible. The impact of this may have been to limit the Deputy Solicitor General's function to that of performing an advisory, research, and policy role through the work of a departmental secretariat.

When the McDonald Commission examined the role of the Department in relation to the RCMP, it noted two reasons why the Minister had little access, other than through members of the Force itself, to informed opinion about RCMP policies. One reason concerned the legal framework that established the Department. This, the McDonald Commission said, created doubts and controversy regarding the powers of the Deputy Solicitor General in relation to all the agencies for which the Minister had responsibility.

The other contributing factor identified by the McDonald Commission was the tradition of independence from government direction that had hitherto characterized police-government relations. Underpinning this notion was the quite proper belief that elected officials should not be allowed to use the police for their own ends by providing

instructions concerning what crimes to investigate and which persons to arrest. The principle of police independence does not mean, however, that the police can or should be a law unto themselves.

The McDonald Commission placed considerable emphasis on reaching an understanding of what members of the Government of Canada knew and should have known about the activities of Canada's federal police, particularly those in relation to security matters. The Commission's solution, which was later adopted by Parliament, was to sever the security intelligence function from the police, to put it firmly under political control and direction, and to make it subject to independent review. In so doing it largely avoided the issue of the Deputy Solicitor General status.

At that time, few could foresee that terrorism would eventually require the level of co-operation and consultation that it now does between those charged with preventing such acts and those prosecuting suspected offenders. In fact, such matters really came to the fore only after the release of the *Report of the Special Committee of the Senate on Terrorism and Public Safety* in July 1987. Soon after, the Government created an inter-departmental task force to review and improve counter-terrorism arrangements, particularly in the areas of contingency planning and crisis management.

The Committee reviewed the 1988 draft report of the Counter-Terrorism Task Force entitled *National Counter-Terrorism Plan*, which was released to the Committee under the *Access to Information Act*.

The Committee endorses the view that terrorist acts should be addressed under provisions of the *Criminal Code* and it agrees with the premise that responses to such incidents should be primarily the responsibility of the federal government. In addition, the Committee supports the idea that the Department of the Solicitor General should act as the lead ministry for all terrorist incidents occurring within Canada, should house the National Security Co-ordination Centre (NSCC), and should manage the National Policy Centre (NPC) in the event of major protracted terrorist threats or incidents.

An important element of Canada's counter-terrorism program is the RCMP's Special Emergency Response Team (SERT). At the invitation of the Commissioner of the RCMP, the Committee visited the RCMP's training centre for SERT. The Committee was impressed with the dedication of the team, the state of readiness of its members, the resources and training available to them, and the exhibited expertise. The Committee acknowledges that the function of SERT is a specialist one and outside the realm of most police officers' experience. It therefore concludes that special measures are required to cover SERT's deployment and use. These are discussed under the *Security Offences Act*.

8.2.2 *The Solicitor General of Canada*

The Committee believes that meticulous security planning, sound intelligence, and the careful orchestration of responses are essential ingredients of any effective

counter-terrorism program. To ensure that this occurs, the Solicitor General should play a central role in the direction, management and control of the government's counter-terrorism program. The Special Committee of the Senate on Terrorism and Public Safety expressed concern regarding how effectively the Department of the Solicitor General can co-ordinate the counter-terrorism structure:

> The abilities of successive Solicitors General notwithstanding, the portfolio is a junior one, having less prominence and power within Ottawa than many of the departments it is supposed to co-ordinate. Second, although CSIS and the RCMP report to the Minister, the Department has no operational role *per se* in implementing counter-terrorism policies... Finally, the co-ordinating role of the Department is inadequately recognized or comprehended by other departments and agencies within the federal government, particularly by External Affairs.[1]

The Committee agrees with the observations of the Special Committee of the Senate. It believes that the Solicitor General will not be able to perform his or her role properly without changes in the statutory mandate.

RECOMMENDATION 45

The Committee recommends that the *Department of the Solicitor General Act* be amended to give the Solicitor General of Canada a mandate for the direction, control and management of Canada's counter-terrorism program; and that the amendment indicate the lead ministry responsibilities of the Department and, more particularly, those of the National Security Co-ordination Centre and the National Policy Centre.

Since 1984, the period during which CSIS has been in existence, there have been five Solicitors General and one acting Solicitor General. During the previous decade, when the RCMP ran the Security Service, the turnover rate was almost as rapid. The Committee learned by experience how long it takes to grasp the complexities of the issues involved in security and intelligence matters. The Solicitor General's portfolio includes other complex and time-consuming issues requiring the Minister's attention. Without adequate time to become familiar with the intricacies of the portfolio, a Solicitor General will find it difficult to provide proper direction to the agencies under the Minister's responsibility.

Because the Solicitor General has a crucial responsibility for ensuring that the fundamental freedoms of Canadians are not abused, the Committee believes that the Prime Minister should try to ensure that Solicitors General stay in the portfolio longer than has been the norm.

8.2.3 *The Deputy Solicitor General*

Twenty years ago, D.R. Yeomans drew attention to what he referred to as a "unique situation where one minister has three departmental officials who report to him." He

went on to observe that "one can imagine the pressures a minister may face as the result of this distribution of authority."[2]

It is now time to take up the question of the Deputy Solicitor General's status within the statutory framework.

When Bill C-9 was adopted by Parliament in 1984, section 95 amended the *Department of the Solicitor General Act* to give the Solicitor General responsibility not only for the Royal Canadian Mounted Police, the National Parole Board and the Correctional Service of Canada, but for CSIS as well. Since 1984, successive Solicitors General have had five persons with deputy head status reporting to them.

The responsibilities of the Deputy Solicitor General must be placed within the wider context of the Ministry as a whole and of the Government of Canada. The Solicitor General's ministry has an unusual organizational structure when compared with other departments in the federal government. While there are now four major line management responsibilities — federal policing, corrections, parole, and security intelligence — all these functions are under the control and management of agency heads with deputy head status, not the Deputy Solicitor General. With the exception of the Inspector General of CSIS, the Deputy Solicitor General has no line management responsibilities.

The Deputy Solicitor General's primary function lies in providing the Minister with two forms of advice: that of a corporate and strategic nature, and that concerning the overall policy direction of ministry programs. To develop and co-ordinate such policy in conjunction with the four agencies, the Deputy Solicitor General heads three branches: Planning and Management, Police and Security, and Corrections.

Relations between the relatively new Canadian Security Intelligence Service and the RCMP have not always run smoothly. While the Committee has not found any recent evidence of what SIRC described in its initial reports as a "turf battle",[3] it has observed marked differences of interest and opinion between the two agencies. The Committee therefore concludes that the Deputy Solicitor General will continue to be called upon to perform two critically important functions in the future. One is to provide informed, impartial advice to the Minister. The other is to fashion compromises between the Commissioner of the RCMP and the Director of CSIS whenever the need arises.

The Committee found the testimony of the Honourable Robert Kaplan, one of the longest serving Solicitors General in recent years, compelling on this point. He suggested that there should be a change in structure within the Solicitor General's ministry whereby the four agency heads currently holding deputy head status would report to the Solicitor General through a Senior Deputy Minister, the Deputy Solicitor General.

RECOMMENDATION 46

The Committee recommends that consideration be given by the Solicitor General to conducting a review within his ministry to establish whether agency heads should report to the minister through a senior deputy minister.

8.3 The Canadian Security Intelligence Service Act

8.3.1 *Roles of Government Actors*

In this section, the roles of three actors in the *CSIS Act* scheme are discussed. These are the Director of CSIS, the Deputy Solicitor General and the Solicitor General of Canada.

8.3.2 *The Director of CSIS*

The vesting of powers in the Director and the Director's responsibilities are established by sections 3 to 11 of the *CSIS Act*. Section 6, arguably the most important insofar as the Director is concerned, gives control and management of the Service to the Director. The exercise of this authority, and most other powers, is given to the Director and is subject to the approval of the Minister. Section 8, however, gives the Director **exclusive** authority to appoint employees and to set terms and conditions of employment.

The present Director, Reid Morden, took over the Service at a difficult time. The first Director, Ted Finn, resigned in 1987 following alleged warrant irregularities in British Columbia. Soon after, the Independent Advisory Team (IAT) reported to the Solicitor General making thirty-four recommendations for change. The Solicitor General at the time, the Honourable James Kelleher, accepted the entire Report and all its recommendations, including the one urging elimination of the Counter-Subversion Branch within the Service. The ensuing changes have at times been dramatic and have had an important impact on the corporate culture of the Service. These changes have not always been readily accepted. Nevertheless, the Committee is pleased to note that, based on information provided by the Service, most of the IAT recommendations appear to have been implemented fully. If this is the case, much of the credit for this dramatic restructuring must go to the present Director.

The reports that the Act requires from CSIS are important elements by which the Service and its employees can be called to account. Under section 19(3) of the *CSIS Act*, the Director is obliged to submit a report to SIRC where there has been an unlawful disclosure of information. In his written responses to the Committee's questions, the Director informed the Committee that "from a judicial point of view, no employee has been found to have disclosed information under section 17."

Likewise, under section 20 of the *CSIS Act*, there is an obligation for the Director to provide a report to the Minister where the Director is of the opinion that an employee of the Service may have acted unlawfully in his or her purported duties and functions. In his written responses to the Committee's questions and in his testimony before the Standing Committee on Justice and Solicitor General in April 1990, the Director acknowledged that there have been seven occasions on which he has made such reports. In five instances, the Service itself claimed to have brought alleged incidents of unlawful activity to light. In the other two cases, a private citizen and a municipal police force were responsible for so doing. All these cases had disciplinary consequences but so far, none has resulted in criminal prosecution.

Despite a formal request by the Committee, the Director did not supply copies of reports sent to the Minister and to SIRC on grounds that to do so would infringe the *Privacy Act*, national security, on-going investigations, cases *sub judice*, and advice to Ministers.

At the request of the Committee, the Director did, however, supply documents which in his opinion reflected the Service's code of conduct and discipline. These were taken from Volume II, Part 10, of the Service's Administrative Manual and were entitled "Conduct and Discipline". The Committee reviewed these documents, which have also been released under the *Access to Information Act*. In general terms it finds the principles laid out adequate for the Service's needs.

Section 33 of the *CSIS Act* requires the Director to submit, at least annually, a report to the Minister concerning the operational activities of the Service. It is by far the most onerous of the Service's reporting functions. It forms an essential feature of the overall accountability scheme of the *CSIS Act*. Although copies of the Director's annual report find their way, as a matter of course, to the Inspector General and SIRC, they were not made available to the Committee despite a formal request for access to them. The Committee cannot, therefore, make a full and fair assessment of whether these reports are as useful as they should be to the reviews conducted by the Inspector General and SIRC.

Certain deductions can, however, be drawn from the heavily censored versions of the three annual reports that have so far been released under the *Access to Information Act*. Because much of the material in the reports is not blacked out, the most obvious point is that a substantial part of the information in the reports could quite easily be made public. In this regard, Australian officials drew the attention of the Committee to the reporting process in Australia. There, the Director General of Security, the head of the Australian Security Intelligence Organization (ASIO), provides the Attorney General with a report "which may be made available to Parliament." Committee staff reviewed some of these reports with a view to assessing their utility. They found them in many respects to be comprehensive documents. They run to more than fifty printed pages and cover a wide range of topics including not only matters relating to ASIO and its activities but also such issues as the release of archival material, a matter raised before this Committee by Canada's academic community. The Committee considers that these reports provide an

important public service and make a significant contribution to informed public debate on security and intelligence matters. It also believes that if similar reports were prepared in Canada, they would give CSIS an opportunity to state its case publicly, particularly where it disagrees with the views put forward by SIRC in its annual report.

RECOMMENDATION 47

The Committee recommends that the Solicitor General require the Director of CSIS to provide the Minister with an additional annual report that can be tabled in Parliament.

8.3.3 *The Deputy Solicitor General*

The principal responsibilities of the Deputy Solicitor General with regard to CSIS are set out in sections 7 and 30 of the *CSIS Act*. They define the relationship of the Deputy with the Director and with the Inspector General. Section 7 places the Director under an obligation to consult with the Deputy Solicitor General on matters relating to the general operational policies of the Service, on certain ministerial directions, and before the Service obtains a warrant. The essential purpose of this consultation was broached originally by the McDonald Commission. The Commission said it was to ensure that the Deputy Solicitor General was in a position to advise the Minister. In fact, special provision was made in the *CSIS Act* for the Deputy Solicitor General to impart such advice. Besides requiring consultation, section 7 puts the Deputy under an obligation to advise the Minister, either where directions have already been issued or where the Deputy thinks they should be issued.

In October 1987, the IAT made recommendations concerning actions that should be initiated by the Deputy Solicitor General. Of critical importance were recommendations 17, 18, 19, 20, 26 and 27 of its report. Two important observations need to be made in this regard. First, the Committee is pleased to note that action appears to have been taken, through written directions, to limit the scope and intensity of the security intelligence net; to define the principles and policies governing the conduct of investigations, especially those using human sources; and to reconfirm the roles and responsibilities of the major office holders in the national security framework. Second, essential aspects remain to be addressed. As discussed elsewhere in this Report, there is still no ministerial direction that provides an operational framework for the interpretation of the definition of threats to the security of Canada contained in section 2 of the *CSIS Act*. And there is still no legal policy framework relating to section 12 that identifies how CSIS should interpret the relationship between the "strictly necessary" criterion of that section and the targeting and intelligence-gathering processes. The Committee believes that the Secretariat should rectify these deficiencies as quickly as possible.

8.3.4 *The Solicitor General of Canada*

The lack of ministerial control over the RCMP Security Service before 1984 was seen by many observers as a fundamental reason for the abuses perpetrated by that agency in the 1960s and 1970s. Section 6 of the *CSIS Act* places the Solicitor General firmly in the driver's seat by making the Director's control and management of the Service subject to written ministerial directions.

During its visit to Washington, the Committee was impressed by remarks made by representatives of Congressional intelligence oversight committees and by members of various intelligence agencies that Congress oversees. While both groups acknowledged an initial reluctance on the part of the principal intelligence agencies to be governed by written guidelines, they now recognize their value.

Clearly, the provision of written directions to the Service constitutes a crucial mechanism by which control over CSIS is exercised by the Minister responsible. Written directions, by identifying what the Service's instructions are at any particular time, also give CSIS and its employees important protections against charges of inefficiency or impropriety that may stem from changes in the portfolio or in the Government.

Section 6(3) of the *CSIS Act* exempts such written directions from the ambit of the *Statutory Instruments Act*. The implications of this section are two–fold. First, the normal process by which Parliament gets to review the exercise of regulation–making powers by ministers — that is, through its Standing Joint Committee on the Scrutiny of Regulations — does not apply. Second, the normal process by which Canadians are alerted to the contents of statutory instruments, that is, through publication in the *Canada Gazette*, does not occur.

For information on CSIS's ministerial directions, Parliament and Canadians have had to rely on the work of SIRC and the willingness of ministers to be forthcoming. Under section 38(*a*)(ii) of the *CSIS Act*, SIRC is obliged to review all ministerial directions provided to the Service under section 6(2). This section may be problematic for two reasons. First, SIRC is obliged to review only written directions. It is not difficult to envisage circumstances in which the Service might be given oral instructions. The Committee, in fact, received an admission from the Service that oral instruction does occur. The Service's report to the Committee on the implementation of the IAT's recommendations stated at one point, regarding the security intelligence net in relation to counter– subversion activities, that "written Ministerial direction was issued to the Director which elaborated on and formalized previous oral direction...".

Second, written instructions to the Service may be provided with different labels and thus escape the review process on a technicality. The IAT Report, for example, uses both terms, 'ministerial directive' and 'ministerial direction'. SIRC has also used both terms. In its annual report for 1986–87, the Review Committee attempted to differentiate between the two. It described directives as "policy statements" that lay down how

operations of a given class are to be handled. These, it noted, normally require certain matters to be referred to the Solicitor General for decision on a case-by-case basis. Directions, on the other hand, it defined as "correspondence on specific cases in which the Solicitor General may incidentally provide policy guidance or establish precedents that can be applied to other cases." SIRC now uses only the term 'direction' to refer to ministerial instructions.

The Committee has been led to believe that the Government now uses only the term 'ministerial direction' in relation to giving instructions to CSIS. It is also the Committee's understanding that oral instructions to CSIS are now limited to occasions when the Minister chairs meetings where no notes are taken. Where the Minister or the Service believes instructions have been given by such methods, it is now normal practice for them to be put in writing shortly after. While the Committee is satisfied that the process of providing ministerial instructions appears to be working, it believes that the legislation should confirm the current practice.

RECOMMENDATION 48

The Committee recommends that Section 6(2) of the CSIS Act be amended to require the Minister to issue all instructions to the Service in writing. Provision should, however, be made for emergency oral instructions. In such circumstances there should be an obligation on the Minister to confirm the instructions so given in writing within 48 hours. The amendment should also require that all instructions be termed 'directions' and be forwarded to SIRC.

The Review Committee has identified in its annual reports most of the written directions issued by the Minister to CSIS. Some fifty directions are now in existence. According to officials at SIRC, the Service continues to operate under eighteen directions it inherited from its predecessor, the Security Service of the RCMP. Apparently, these directions are being reviewed and updated to meet CSIS's requirements.

The former Solicitor General, the Honourable Pierre Blais, indicated in his testimony before the Committee that there were four general categories of issues that may be covered by ministerial directions: 1) accountability and control, 2) security operations and methods, 3) information management, and 4) domestic and foreign liaison.

In his responses to written questions from the Committee, the Solicitor General defined a "written direction" as: "(i) a written instruction issued under the Solicitor General's prerogative, which (ii) relates to policies, standards or procedures, and (iii) conveys instructions of a continuing nature to the Service."

The Committee recognized the singular importance of ministerial directions. As a result, it not only took careful note of what the IAT Report had to say on the matter and sought written responses from the key participants in the security intelligence system, it also requested a briefing in a secure environment on ministerial directions.

The Committee's objectives in asking for this briefing were four-fold. First, the Committee wanted to establish whether the directions were in compliance with the letter and the spirit of the *CSIS Act*. Second, the Committee wanted to confirm whether the directions were clear, unambiguous and readily understandable by members of the Service. Third, the Committee wanted to verify whether certain terms that SIRC and others had previously identified as being problematic in the *CSIS Act* were, in fact, defined adequately in directions. Of particular interest in this regard were: "detrimental to the interests of Canada", "foreign influenced", "leading ultimately", "clandestine", "deceptive", "espionage", "sabotage", "strictly necessary", "foreign intelligence", and "security intelligence". Finally, the Committee wished to evaluate the degree to which the Deputy Solicitor General had considered the scope of directions as a whole and thus fulfilled his mandate under section 7(3) of the *CSIS Act*.

The Solicitor General's Secretariat provided the Committee, but not its staff, with a briefing (in a secure environment) that was conceptual in format. It identified the main themes covered by the directions. Subsequently, the Solicitor General provided Committee staff with a copy of the speaking notes used at the briefing that had been processed under the *Access to Information Act*.

RECOMMENDATION 49

The Committee recommends that the *CSIS Act* be amended to require the Minister to table a report in Parliament at least once each fiscal year concerning the status of written directions provided to the Service and that the Standing Committee to which it is referred consider the report in an *in camera* session.

With regard to the issue of whether the directions are in compliance with the letter of the law, the Committee is unable to reach a conclusion because it did not get to read the actual directions. In two instances, however, the Committee was able to form some very tentative impressions about ministerial directions from its own observations and from the comments of others.

In its annual report for 1988–89, SIRC indicated that the Solicitor General had tried to find a way for members of CSIS to brief elected officials without being in breach of section 19 of the *CSIS Act*. While the Committee believes that Solicitors General should receive every encouragement when it comes to providing briefings to parliamentarians, it does not agree that this should be accomplished by circumventing section 19 through a written direction. The Committee is therefore in agreement with SIRC's recommendations concerning the release of information (#28 and #29) put forward in its submission to the review Committee.

RECOMMENDATION 50

The Committee recommends that the limits prescribed by section 19 of the *CSIS Act* apply equally to the Solicitor General and to all officials and exempt staff in the Ministry of the Solicitor General having access to information obtained by CSIS in the performance of its duties and functions.

RECOMMENDATION 51

The Committee recommends that section 19(2)(*d*) of the *CSIS Act* be amended to permit disclosures to members of the Senate and the House of Commons on the same basis as to ministers of the Crown and to a "person in the public service of Canada".

The other instance concerns the written direction on "national requirements for security intelligence", issued by the Solicitor General in September 1989. This direction is useful not only because of what it has to say about compliance with the law, but also the impressions it leaves regarding the clarity of directions. In this instance, the Committee received a copy of the version of the direction that had been released, with deletions, to a journalist under the *Access to Information Act*. The main thrust of this direction was laid out in a speech by the Solicitor General at a conference hosted by the Canadian Association for Security and Intelligence Studies in Ottawa at the end of September 1989. This speech made an important contribution to the theme of the conference, security and intelligence needs for the 1990s. While the direction itself is quite general in nature, the Committee fully recognizes the impetus given by the formulation and release of this direction to the development of informed public debate on security and intelligence matters in Canada. It therefore wishes to commend the Government for this initiative.

The Committee wishes to raise one matter relating to the national requirements direction. The direction identifies five national interest areas as public safety, integrity of the democratic process, security of government assets, economic security, and international peace and security. The Committee has no quarrel with the identification of these interests. They all seem appropriate for the times. Where the Committee wishes to take issue is in the translation of one of those interests into national requirements for security intelligence. Under the heading "economic security" the direction lays out the following:

> K. Protection of classified technology; and
>
> L. Protection of other sensitive scientific and technical information.

The Committee is in partial agreement here with the brief submitted by the Law Union of Ontario, which stated, "we do not believe that the prevention of industrial

espionage is a proper function of a national security agency like CSIS." While the Committee believes it is properly within the purview of government agencies to help protect classified technology, it does not agree that it should necessarily be a job for CSIS to protect sensitive scientific and technical information belonging to the private sector. More important, the Committee is not sure whether the *CSIS Act* currently gives CSIS such a mandate.

With regard to the issue of whether the directions provided by the Minister adequately cover the necessary ground, the Committee was guided by the conclusions reached by the IAT Report and by CSIS's report on the implementation of its recommendations. These clearly imply that the Service still requires important guidance on a number of issues. Besides the elements noted above and elsewhere in the Report, the Committee observed that there did not appear to be a direction indicating to the Service what types of intrusive investigations require a warrant. Nor did there appear to be adequate ministerial guidance on how the Service should develop targets.

Comments made both by SIRC and during the briefing on directions by the Solicitor General's Secretariat indicated that the manner in which directions were developed, and the reasons for them, had changed significantly since the establishment of CSIS in 1984. Initially, there had been an emphasis on bringing old RCMP Security Service directions up to date and providing ministerial instructions regarding specific operational problems as they arose. It appears that directions now tend to be geared to providing general policies for the Service. The Committee believes that this represents a natural and proper progression and reflects a maturing environment. Nevertheless, it has gained the impression that the process of developing policy for the Service by the Secretariat, and the process of translating that direction into operational terms by the Service, have not progressed as far and as fast as they might have.

In discussions with SIRC, it became clear to the Committee that SIRC believes it has a limited role regarding directions. Apparently, the Review Committee believes that its obligation extends only to reviewing written directions to ensure that they are in compliance with the *CSIS Act*. It does not attempt to establish whether there are areas requiring direction or whether directions are elastic enough to ensure efficiency and effectiveness.

The Review Committee may be right in its interpretation of the Act. The Committee believes, however, that it is important that there also be an independent review of ministerial directions to determine whether they properly provide the Service with the range of instructions and interpretations it requires, as well as to consider their impact on operational efficacy.

RECOMMENDATION 52

The Committee recommends that section 38(*a*)(ii) of the *CSIS Act* be amended to require SIRC to review ministerial directions, not only with a

view to confirming compliance, but also to establish whether the directions provide adequate and appropriate instructions to the Service.

8.4 The Security Offences Act

8.4.1 *Introduction*

The original legislation adopted by Parliament in 1984 contained a number of specific parts. Part IV of Bill C–9, as it was then known, concerned "An Act Respecting Enforcement in Relation to Certain Security and Related Offences"; its essential features involved provisions for law enforcement and prosecutorial jurisdiction. Since Parliament enacted the Revised Statutes of Canada in 1985, this now exists in its own right as the *Security Offences Act*.

The Law Reform Commission of Canada has recommended that the *Criminal Code* be revised to group so–called "crimes against the state" together in a special section. As a result, the Committee considered whether it would now be appropriate to incorporate the *Security Offences Act* into the *Criminal Code*. On this issue, the Committee found the response to the Committee's written questions by Dr. Richard Gosse, the first Inspector General of CSIS and now the Chairman of the RCMP Public Complaints Commission, persuasive. He wrote as follows:

> The *Security Offences Act* deals with criminal offences and, conceptually, I would think that it would be more appropriate to incorporate the whole Act into the *Criminal Code*. While it covers offences found in the *Criminal Code*, it is also related to the enforcement of offences contained in other statutes, such as the *Official Secrets Act*. Its main provisions concern the powers of the Attorney General of Canada and of the Attorney General of the provinces, and the role of the RCMP. In practical terms, to incorporate the Act in the *Criminal Code* would result in burying the provisions in a large statute which would be detrimental, as these provisions require a certain profile that the *Criminal Code* would not provide. I am of the view that the *Security Offences Act* should be retained as it is.

RECOMMENDATION 53

The Committee recommends that the *Security Offences Act* not be incorporated into the *Criminal Code*.

8.4.2 *Roles of Government Actors*

In this section, the roles of four federal government actors are reviewed: the Attorney General of Canada; the Commissioner of the Royal Canadian Mounted Police (RCMP); the Deputy Solicitor General of Canada; and the Solicitor General of Canada. In addition, the roles of provincial attorneys general and relevant solicitors general are discussed with a view to describing responsibilities for the prevention, law enforcement and prosecution of security offences.

Under the *Constitution Act, 1867* the Parliament of Canada has jurisdiction for enacting legislation concerning the criminal law as well as for measures that ensure peace, order and good government.[4] Provincial legislatures, on the other hand, normally have jurisdiction over the administration of justice. The *Security Offences Act* represents an accommodation between these two constitutional jurisdictions.

8.4.2.1 *The Attorney General of Canada:*

Under sections 2, 4 and 5 of the *Security Offences Act*, the Attorney General of Canada has certain procedural and prosecutorial powers in relation to security offences. In her response to the Committee's written questions, the Attorney General of Canada, the Honourable Kim Campbell, indicated that no guidelines or interpretive aids have so far been issued concerning the application of these sections, and that no formal arrangements have been reached with either provincial or territorial attorneys general. Since the Committee wrote requesting submissions from provincial authorities and none were received, the Committee concludes that the provinces and territories are satisfied with this situation.

Section 4 of the Act gives the Attorney General of Canada the discretionary power to issue a *fiat* to the attorney general of a province where there is reason to believe that an offence outlined in section 2 has been committed.

According to the response of the Attorney General of Canada to the Committee's written questions, this right of *fiat* has been exercised only once since the enactment of the *Security Offences Act*. This involved an assault against an internationally protected person, the Acting High Commissioner of India, near the legislative buildings in Winnipeg, Manitoba, only two days after the Act came into force.

According to the Attorney General, "there have been other instances which could fall within the scope of section 2... for which no *fiat* was issued." Apparently, in some of these instances there was federal-provincial consultation, while in others provincial attorneys general proceeded to prosecute without consultation.

The Committee shares the view expressed by the Attorney General of Canada that the use of the *fiat* should be reserved for special or compelling circumstances.

Section 5 of the *Security Offences Act* requires the Attorney General of Canada, where a *fiat* is issued, to provide the court in which the proceedings are conducted with a copy of that *fiat*. In view of the fact that the Committee is recommending an increased role for SIRC, it makes the following recommendation.

RECOMMENDATION 54

The Committee recommends that section 5 of the *Security Offences Act* be amended so that a copy of each *fiat* issued is referred to SIRC.

8.4.2.2 *Provincial Authority and Jurisdiction*

Section 3 of the *Security Offences Act* reaffirms the authority of provincial attorneys general to conduct proceedings relating to any offences outlined in section 2 where the Attorney General of Canada has not issued a *fiat*. The Committee is of the opinion that this is an appropriate section and should be retained.

8.4.2.3 *The Commissioner of the RCMP*

It has long been accepted that the provinces of Canada have the right to establish police forces and that this power includes the right to "appoint, control and discipline" members of these organizations.[5] It is also accepted that such forces would enforce provincial penal laws as well as the criminal law.

Canada is currently policed by some 450 different police forces. They operate at three jurisdictional levels: federal, provincial and municipal. They range in size from a handful of officers to forces of many thousands.

The RCMP has responsibility for policing the territories and for the enforcement of all federal statutes, except the *Criminal Code*, across Canada. The RCMP also provides policing services under contract to eight provinces and to 192 municipalities. Ontario and Quebec have their own provincial police forces, while Newfoundland has its Constabulary. Most of the independent municipal police forces are located in Quebec and Ontario.

When the RCMP operates as a federal force, it is governed entirely by the *RCMP Act*. When it acts under contract, however, provincial laws regulating policing also come into play. In such circumstances, RCMP officers find themselves subject to direction from two quarters. On one hand, the authority of the provincial minister responsible for policing may be exercised. But on the other hand, officers of the Force are bound by regulations made under the *RCMP Act*, and specifically by section 5 of that Act, which gives the Commissioner of the RCMP the authority to control and manage the force subject to the direction of the Solicitor General of Canada.

The security function in Canada has consisted historically of three specific elements. One is security intelligence work and security screening. Here the primary purpose is to warn the Government of Canada about possible threats to national security. A second is the process of conducting criminal investigations, including the collection of criminal intelligence, regarding matters with a national security dimension or related to offences under the *Official Secrets Act*. The third element is protective security. This incorporates not only measures to safeguard particular persons, federal property and information, but also the provision of advice on technical and protective security.

The enactment of the *CSIS Act* in 1984 did not remove the RCMP from the security business. Nor did the passage of the *Security Offences Act* create new offences. Rather,

they reaffirmed in legislation certain aspects of the role of Canada's federal police in the overall security process. Section 6 of the *Security Offences Act* specifically allotted primary responsibility to members of the RCMP who are peace officers to perform the duties that are assigned to peace officers in two important respects. First, it placed within the RCMP's jurisdiction all alleged offences arising out of conduct constituting a threat to the security of Canada within the meaning of the *CSIS Act*. Second, it gave the RCMP responsibility for the apprehension of the commission of such offences.

It should be noted that section 6 of the *Security Offences Act* does not make the RCMP totally responsible for dealing with security offences. It only makes the Force primarily responsible. The Committee has become aware that questions of jurisdiction have arisen in the past while a criminal offence was in progress.[6]

As a result, the Committee attempted to establish whether such matters had been resolved to the satisfaction of all concerned. Although requested to make a submission to the Committee, representatives of the Canadian Association of Chiefs of Police and certain municipal forces chose not to do so. However, in his responses to the Committee's written questions, the Commissioner of the RCMP confirmed that particular investigations may now be assigned to local police forces and that "provisions to this effect are contained in arrangements between the Federal Government and the provinces". Legislative provision to facilitate consultation and co–operation is provided for under section 6(2) of the *Security Offences Act*. The Committee understands that there are now agreements in place with all the provinces, except Quebec.

RECOMMENDATION 55

The Committee recommends that the federal government continue to pursue, as a matter of urgency, a policing agreement with the Province of Quebec, along the lines of that with the Province of Ontario.

In a briefing provided by the RCMP, members of the Committee were given an opportunity to review one of these agreements. According to the Commissioner, the contents of this agreement cannot be made public as it was entered into in confidence with a provincial government. The Committee can report, however, that the agreement appears to be satisfactory.

The Committee believes that there should be consistency between section 6(2) of the *Security Offences Act* and section 20 of the *RCMP Act*. Subsection 20(1) of the *RCMP Act* states that:

> 20. (1) The Minister may, with the approval of the Governor in Council, enter into arrangements with the government of any province or, with the approval of the lieutenant governor in council of any province, with any municipality, for the use or employment of the force, or any portion thereof, in aiding the administration of justice in the province or municipality...

Section 20(3) of the *RCMP Act* requires that:

> 20. (3) The Minister shall lay before Parliament a copy of every arrangement made under subsection (1) within fifteen days after it is made or, if Parliament is not then sitting, on any of the first fifteen days next thereafter that Parliament is sitting.

Section 6(2) of the *Security Offences Act* allows the Solicitor General of Canada to enter into arrangements with a province regarding the enforcement of security offences. The section states:

> to facilitate consultation and co-operation in relation to the carrying out of duties assigned to the Royal Canadian Mounted Police under subsection (1), the Solicitor General may, with the approval of the Governor in Council, enter into arrangements with the government of a province concerning the responsibilities of members of provincial and municipal police forces with respect to the performance of duties assigned to peace officers in relation to any offence referred to in section 2 or the apprehension of the commission of such an offence.

It does not require that the arrangement be made public. The Committee believes that there is no reason why such arrangements should not be tabled in Parliament.

RECOMMENDATION 56

The Committee recommends that Section 6(2) of the *Security Offences Act* be amended to require the Solicitor General of Canada 1) to lay before Parliament a copy of every arrangement made under this subsection and 2) to provide the Security Intelligence Review Committee with a copy of each such arrangement.

Section 6 of the *Security Offences Act* specifically allotted primary responsibility to members of the RCMP who are peace officers to perform the duties that are assigned to peace officers regarding offences arising out of section 2 of the *Security Offences Act*. Consequently, the Committee set out specifically to establish what exactly these duties are. In his response to written questions, the Commissioner drew the Committee's attention to "those peace officer powers set out in section 18 of the *RCMP Act*." Section 18, particularly paragraph 18(a), is problematic for outsiders to the Force for two reasons. First, such duties are subject to the orders of the Commissioner. Second, the duties assigned to peace officers in relation to the preservation of the peace and the prevention of crime and of offences against the laws of Canada are not all spelled out clearly in legislation.

Some additional guidance regarding the intention of section 18 is found in the 1990-91 Main Estimates for the RCMP. This suggests that the peace officer concept guides the Force and is reflected in its objectives: "To enforce laws, prevent crime, maintain peace, order and security." It further notes that the RCMP program can be divided into four sub-objectives:

> to prevent, detect and investigate offences against federal statutes; provide investigational assistance and protective security to other federal departments and agencies; and protect internationally protected persons and Canadian dignitaries;
>
> to prevent and detect crime, enforce laws and maintain law and order in provinces, territories and municipalities under contract;
>
> to assist Canadian law enforcement agencies by providing specialized police training, forensic laboratory service, identification and criminal information services, and integrated automated information services; and
>
> to provide co-ordinated and common support services to program objectives.[7]

The Committee took careful note of the view expressed by the Commissioner in his written responses to questions posed by the Committee concerning counter-terrorism. He stated that "the primary role of the police in all law enforcement activity is to prevent crime."

If any program to prevent crime is to be successful, an important ingredient must be sound intelligence. Clearly, the RCMP is still in the intelligence business. This was acknowledged by the Commissioner during his testimony and in his written responses to the Committee's questions. Asked specifically whether the RCMP's work overlapped with that of CSIS, the Commissioner stated that he preferred to see it as a "shared responsibility". Equally clearly, the National Security Investigations Directorate (NSID) and its divisional sections collect intelligence that could be broadly described as relating to Canada's national security. The Force draws a distinction, however, between the type of intelligence it gathers and security intelligence. It collects criminal intelligence, not security intelligence. It defines criminal intelligence as information

> that is in support of an allegation of criminal wrongdoing, a criminal conspiracy, or something of that nature, which would be the natural interest of peace officers. In other words, we would gather our criminal intelligence with a view to building on that intelligence until it become evidence, and then that evidence would be presented in court.

In collecting this intelligence, the Force uses a full range of investigative police techniques, including human and technical sources, liaison functions, forensic methodologies and interviewing techniques.

Given that it was acknowledged that the RCMP is still in the business of collecting intelligence for national security purposes, the Committee was very interested in finding out what control procedures are in place to prevent abuse. The Committee was informed that there was nothing similar to CSIS's Target Approval Review Committee (TARC) within the RCMP. The Committee also learned that policies governing intrusive investigations by NSID sections were the same as for all other RCMP investigations.

The Committee was informed about and presented with a copy of a new policy relating to the National Security Investigations Program. Because the Committee had become aware of certain investigations related to national security that appeared, on their face, to be of a questionable nature, the Committee reviewed the program document carefully. On reflection, the Committee wishes to commend the RCMP on its clarity and overall direction. Certain points made in the new policy are worth enumerating here. First, national security investigations must always be related directly to the gathering of information that leads to the identification of a criminal offence or to the evidence-gathering process. Second, NSIS officers are not to solicit from the public information that has only a security intelligence character. Third, human source development and tasking must always be done within the parameters of criminal activity. Fourth, the RCMP will not tolerate RCMP officers conducting counter-subversion investigations from which CSIS members are precluded. Finally, NSIS officers are not permitted to target groups.

One concern is that through the formation and expansion of the RCMP's National Security Investigations Directorate (NSID) and subsequent sections (NSIS) at the divisional level, the RCMP has maintained a stake in the security intelligence business.

The Committee attempted to establish whether this was the case and, if so, to understand why. To this end the Committee heard testimony from the Commissioner, sought written responses to questions, and at the Commissioner's invitation, received a briefing at RCMP headquarters with Committee staff present.

During this briefing, the Committee's attention was drawn to the fact that the RCMP's "security-related responsibilities" extend beyond the *Security Offences Act*. The Memorandum of Understanding between CSIS and the RCMP defines it as

> the prevention, detection, investigation and laying of charges in relation to any offence referred to in Section 2 of the *Security Offences Act* or the apprehension of the commission of such an offence included in the *Criminal Code*, *Official Secrets Act*, *Export and Import Permits Act* or any other federal statute having a national security dimension.

In this way, the RCMP's national security role extends beyond the boundaries of the *Security Offences Act* and hence into the areas in which CSIS is required to have an interest.

In addition to this role, the RCMP also provides protective security for VIPs, federal properties and airports; advice to departments and agencies concerning security measures; and threat assessments in order to provide protection for VIPs and security for special events, such as the meeting of the G7, the Olympic Games, and Expo '86. This latter responsibility for threat assessments, a process that requires the collection of information and intelligence, much of it from open sources, CSIS, other Canadian agencies and police forces, as well as foreign sources, is also carried out by NSID.

While the RCMP can call upon all its resources at moments of crisis, it should be emphasized that regular membership in the Force's National Security Investigations Directorate is relatively small when compared with that of CSIS.

On this basis, the Committee believes that the capacity of NSID to intrude on the rights and freedoms of Canadians, while not non-existent, is likely to be limited.

A second concern frequently cited is that relationships between the RCMP and CSIS have not always run smoothly. In its early annual reports, for example, SIRC talked of turf battles arising between the two agencies. As evidence of this, the Review Committee frequently referred to CSIS's lack of access to Canadian Police Information Centre (CPIC) data.

The Committee adopted the view that a good working relationship between CSIS and the RCMP is essential to national security. Consequently, it made every effort to assess how well the current relationship is working and whether there has been a noticeable improvement since 1984.

The Committee noted that the transmission of CPIC data to non-police agencies requires the authority of the CPIC Advisory Committee, which is made up of member forces, not just the RCMP. The original Memorandum of Understanding signed in 1984 by CSIS and the RCMP was replaced in August 1989 with one that is significantly more robust. The Committee has reviewed this agreement and believes that it represents a positive step. It also heard comments that the liaison program appears to be working well.

Despite these encouraging signs, the Committee also came across evidence of a worrying nature during its visits to regional offices. While RCMP officers acknowledged that CSIS complied with the letter of the agreement and reported incidents where it was likely that a *Criminal Code* offence had taken place, they claimed that the information received was often "too massaged" to be of much real use.

In one case, senior RCMP officers suggested that the intelligence received was insufficient to prevent a very serious event from occurring. Under ideal circumstances, the Committee would have liked to visit all the regional offices. Because of time constraints, this was not possible. As a result, the Committee was unable to assess whether this was an isolated incident.

The incident is nevertheless worth considering because it raises a number of important issues. One concerns how the RCMP can get raw or "unmassaged" intelligence without, at the same time, putting CSIS sources in jeopardy. Another is whether evidence obtained directly from CSIS sources and methods can be used successfully in court without a *Charter* challenge.

At least three options present themselves on the first issue. Two involve collapsing the law enforcement and security intelligence functions back into a single organization,

either the RCMP or CSIS. Both CSIS and the RCMP seem to be against such a reorganization. The third option entails giving information sources protection under the *Criminal Code* against breaches of confidence.

On the second issue, the Director of CSIS informed both the Standing Committee on Justice and Solicitor General and the Committee that a task force had recently been established in the Department of Justice to review the matter. A subsequent letter to the Committee from the RCMP Commissioner confirms the existence of a working group of officials from the Department of Justice, the Secretariat of the Solicitor General, CSIS and the RCMP. As noted elsewhere in the Report, this Technical Committee has broad terms of reference and an open deadline for completion of its work, which will focus on *Charter* implications as well as issues arising from operational matters.

As far as the Committee has been able to establish, the Memorandum of Understanding between the RCMP and CSIS has created an environment in which a positive working relationship is developing. The Committee believes, however, that there are serious technical problems to be overcome regarding the process by which intelligence generated by CSIS can be transformed into criminal evidence, especially in cases where politically motivated violence is concerned. The Committee wishes to commend the departments and agencies involved for establishing the working group. It urges the Minister of Justice and the Solicitor General to keep Parliament apprised of both the evolving nature of the CSIS–RCMP working relationship and the progress of the Technical Committee.

8.4.2.4 *The Solicitor General of Canada*

The Solicitor General acquires his authority over federal policing from three pieces of legislation, the *Department of the Solicitor General Act*, the *RCMP Act* and the *Security Offences Act*.

The *Department of the Solicitor General Act* is but five sections in length. Section 2 gives the Minister managerial and directorial responsibilities for the department as a whole. Section 4 allots such powers, duties and functions regarding the RCMP that fall within the ambit of Parliament that are "not by law assigned to any other department, board or agency of the Government of Canada."

By comparison, the *RCMP Act* is of broader compass and gives the Minister specific powers. Section 5 places the Commissioner's control and management of the Force under the direction of the Minister. Section 20 allows the Minister to enter into arrangements with provincial governments and municipalities regarding "the use or employment of the force, or any portion thereof." The Act also gives the Cabinet broad regulatory powers concerning the governance of the Force.

The *Security Offences Act* also gives the Solicitor General an important authority. Subsection 6(2) allows the Minister, with Cabinet approval, to enter into arrangements

with provincial governments to facilitate consultation and co-operation concerning the duties that the RCMP and provincial and municipal police forces are to carry out in the enforcement of the law concerning security offences.

The Committee believes that the *Security Offences Act* should be amended to include a provision for the establishment and use of the RCMP's Special Emergency Response Team (SERT).

RECOMMENDATION 57

The Committee recommends that the *Security Offences Act* be amended to include a section that permits the Government of Canada to establish a Special Emergency Response Team (SERT).

8.4.2.5 *The Deputy Solicitor General*

The Deputy Solicitor General has no direct relationship with the RCMP. The Deputy's responsibility with regard to policing is simply to provide the Minister with appropriate advice. There is no statutory obligation on the part of the Commissioner of the RCMP to consult with the Deputy Solicitor General as there is with the Director of CSIS under the *CSIS Act*. The Committee believes that this is inappropriate and should be rectified. It further believes that such consultation would not offend notions of police independence.

NOTES

1. Senate of Canada, Special Committee on Terrorism and the Public Safety, *Terrorism*, 1987, p. 68.

2. D.R. Yeomans, "Decentralization of Authority", *Canadian Public Administration* 16 (1969), pp. 19–25.

3. See, for example, Security Intelligence Review Committee, *Annual Report* 1986–87, p. 15.

4. Peter Hogg, *Constitutional Law of Canada*, 2nd Edition (Toronto: Carswell, 1985, pp. 425–426).

5. Hogg, *Ibid.*

6. See, for example, Peter Moon, "Feuding Policemen Upset the Hostage-taker", *The Globe and Mail* (June 13, 1986) p. A1.

7. Royal Canadian Mounted Police, *1990–91 Main Estimates, Part III Expenditure*, p. 18.

CHAPTER NINE

The Control of Investigative Techniques

9.1 Introduction

Perhaps no area of activity by CSIS poses a greater potential threat to the rights and freedoms of Canadians than the use of intrusive investigative techniques by secret organizations. This chapter outlines the controls that have been imposed both by the Service itself and by the *CSIS Act* on the use of such techniques.

9.2 Historical Background

9.2.1 *Electronic Surveillance*

The RCMP started the practice of intercepting telephonic messages in the 1930s. It was not until World War II had come to a close, however, that telephone tapping and electronic eavesdropping became a common practice among Canadian police forces. The RCMP Security Service was authorized to intercept telephonic communications under the *Emergency Powers Act*, which empowered the Minister of Justice to "require a communications agency to produce or make available, any communication that may be prejudicial to or may be used for purposes that are prejudicial to the security or defence of Canada".[1] The *Emergency Powers Act* expired in 1954; after that, interception of telephone communications proceeded under the authority of the *Official Secrets Act*. The McDonald Commission noted that wiretapping was a common and frequently used investigative technique throughout Canada immediately prior to section 16(2) of the *Official Secrets Act* coming into effect in 1974.[2]

9.2.2 *Protection of Privacy Act*

Section 16 of the *Official Secrets Act* was passed as part of the *Protection of Privacy Act*. The statute as a whole made it an offence under the *Criminal Code* to

> intercept a private communication wilfully by means of an electromagnetic, acoustic, mechanical or other device, unless the person intercepting has the consent of one of the parties or a judicial authorization.[3]

Section 16(2) was enabling. It stated that

> 16. (2) The Solicitor General of Canada may issue a warrant authorizing the interception or seizure of any communication if he is satisfied by

evidence on oath that such interception or seizure 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.

In the Annual Report of the Solicitor General for 1983, the last full year for which detailed information on interceptions under the *Official Secrets Act* is available, 525 warrants were issued under section 16(2). The average length of time for employing such warrants was 253 days. The Solicitor General's report also indicated that section 16 interceptions provided an invaluable source of information with respect to the following:

1) in the prevention and detection of subversive activity directed against or detrimental to the security of Canada;

2) for the purpose of gathering foreign intelligence essential to the security of Canada;

3) for the gathering of information relating to violent, terrorist or criminal activities directed towards accomplishing governmental change in Canada or elsewhere;

4) for the purpose of verifying or disproving information derived from other sources.[4]

The interception of private communications by the RCMP Security Service continued under the authority of the *Official Secrets Act* until the enactment of the *CSIS Act* in 1984.

9.2.3 *Precursors to the CSIS Act*

In the aftermath of the McDonald Commission, two Bills (C-157 and C- 9) were presented to Parliament with a view to creating the first civilian security intelligence service in Canada. The Bills gave rise to heated debate, especially regarding the warrant provisions. The Special Committee of the Senate that reviewed Bill C-157 noted that the Bill fell "considerably short of providing a sufficiently rigorous set of controls on warrants."[5] In particular, the Senate Special Committee proposed five major recommendations for change:

- incorporation of additional requirements similar to those contained in Part VI of the *Criminal Code* before judicial authorization could be approved for the use of intrusive techniques

- the addition of a test whereby a judge would decide whether the intrusion on privacy is outweighed by the threat (the "gravity" test)

- that the legislation fix a time limit for the duration of warrants
- that the Chief Justice of the Federal Court designate judges to consider warrant applications to prevent "judge-shopping"
- that the warrant application should include details of previous applications to prevent "judge-shopping".[6]

The Senate Special Committee also recognized that the warrant provisions lacked ministerial involvement, failed to differentiate between foreign and Canadian targets, and failed to control the use of undercover agents, informers and infiltrators. A number of the criticisms identified by the Special Committee were rectified when Bill C-9 was later presented to Parliament.

9.2.4 *The Enactment of the CSIS Act*

The enactment of the *CSIS Act* in 1984 was accompanied by the repeal of section 16 of the *Official Secrets Act*. The powers reflected in the provisions of the *Official Secrets Act* not only found their way into the new Act but were also extended by it. Section 21(3) of the *CSIS Act* not only empowered the Service to engage in techniques authorized under the preceding legislation but extended the Service's range of intrusive investigations into new areas. Section 21(3) states:

> 21. (3) Notwithstanding any other law but subject to the *Statistics Act*, where the judge to whom an application under subsection (1) is made is satisfied of the matters referred to in paragraphs (2)(*a*) and (*b*) set out in the affidavit accompanying the application, the judge may issue a warrant authorizing the persons to whom it is directed to intercept any communication or obtain any information, record, document or thing and, for that purpose,
>
> (*a*) to enter any place or open or obtain access to any thing;
>
> (*b*) to search for, remove or return, or examine, take extracts from or make copies of or record in any other manner the information, record, document or thing; or
>
> (*c*) to install, maintain or remove any thing.

The powers provided by the *CSIS Act* were largely in accordance with those that the McDonald Commission believed were necessary for a security intelligence service to fulfil its mandate:

> Because of the secrecy maintained by those who pose the most serious threats to Canada's internal security, the security intelligence agency must be authorized to

> employ a variety of investigative techniques to enable it to collect information. The means available to it must range all the way from studying open sources of research material and obtaining information from citizens (foreign and domestic) to using much more covert and intrusive methods that may involve the use of powers not available under the law to the ordinary citizen.[7]

It should be recognized that at the time the McDonald Commission published its final reports in 1981, the *Canadian Charter of Rights and Freedoms* was not yet in place. Although the warrant provisions have since been challenged in a number of court cases, these statutory powers have survived scrutiny under the *Charter*.

9.3 Internal Controls of Investigative Techniques

As a result of the *Atwal* case and the report to the Solicitor General by the Independent Advisory Team (IAT), a number of changes took place within CSIS regarding the 'internal' approval process for targeting and seeking a warrant. The Target Approval and Review Committee (TARC) and the Warrant Review Committee (WRC) now provide the internal approval and regulatory structure for controlling the use of intrusive techniques by the Service. This process is governed ultimately, in the case of a warrant, by the Federal Court. Nevertheless, other intrusive techniques, such as the use of human sources, are undertaken in the absence of judicial control.

9.3.1 *The Target Approval and Review Committee (TARC)*

The choice of targets for investigation is overseen by TARC, which is now chaired by the Director of CSIS. TARC consists of senior CSIS managers and representatives of the Department of Justice and the Solicitor General's department.[8] Its role is to authorize targeting for specified periods of time and to approve the use of various investigative techniques.

The Committee understands that CSIS' operational policy on targeting was revised after consultation with the Deputy Solicitor General, and a new "Targeting Directive" was issued as internal policy in April 1988. In addition, ministerial directions have been issued on the following matters:

1) the conduct of investigations;

2) the use of human sources; and

3) the requirement of ministerial approval prior to intrusive investigation by CSIS of activities described in paragraph 2(3).

The Director of the Service noted in his written responses to the Committee's questions that TARC policy "governs how CSIS implements the 'strictly necessary' provision [of the *CSIS Act*]. The CSIS application of 'strictly necessary' is, of course, subject to monitoring by the Inspector General and SIRC."[9]

The Director of CSIS indicated that once an individual or group has been identified as engaging in threatening activities, collection of information and investigations "may only be conducted after proposals for targeting have been given formal consideration and approval under Targeting Policy." Approvals for targeting under CSIS policy respect the 'strictly necessary' principle as enunciated under section 12 of the *CSIS Act*, which provides for

> levels of increasing intrusiveness and the use of various methods of investigation according to the gravity and immediacy of the threat. In other words, approval for investigation at a low level of intrusiveness may be given, but should an investigator believe that it is "strictly necessary" to employ more intrusive techniques, a further submission under the TARC policy would have to be made to obtain approval for a higher level of intrusiveness.

The Director's written replies to the Committee's questions also note that authorization to investigate is given for "limited periods of time from 90 days to 2 years."

The TARC investigatory approval process permits three levels of intrusiveness. The first level allows the Service to conduct an investigation using open sources of information, which would include conducting interviews. It is not clear at what point a low-level investigation must first be brought to the attention of the TARC. Greater clarity exists, however, as more intrusive techniques are employed. The second level, for example, includes the use of human sources, while investigations requiring warrants are designated at the third and highest level of approval. Accordingly, each level of investigation requires an increasing level of approval by TARC.

9.3.2 *The Warrant Review Committee (WRC)*

The Committee understands that before an investigator can seek a judicial warrant under Part II of the *CSIS Act*, the TARC must approve an investigation at the highest level. During his testimony before the Committee, the Director of CSIS indicated that:

> The targeting committee has to be satisfied that this is a very serious threat that should be very thoroughly investigated before it will grant the top level which is the level 3 investigation. The investigators must have that level 3 before they can begin writing a warrant or an application for a warrant.

The Committee received information regarding the WRC during *in camera* and public sessions and in written replies to its questions. The Committee was informed that the process by which warrant applications are approved within CSIS has been the subject of "many adjustments and much fine-tuning" over the past five years. For example, the IAT made the following recommendations:

> 24. The membership of the Warrant Review Committee should be expanded to include representation from the Privy Council Office or the Department of Justice at the Assistant Secretary/Assistant

Deputy Minister level. The Ministry Secretariat should be represented by the Assistance Deputy Solicitor General, Police and Security Branch.

25. The warrant review process should include a fully independent warrant review function staffed by Counsel directly responsible to the Deputy Solicitor General. Counsel should have unrestricted access to CSIS/Ministry Secretariat information relevant to the proposed investigation in order to challenge the reliability of operational information supporting warrant applications.[10]

As a result of these recommendations, the Director of the Service now chairs the WRC. Other members include the Assistant Deputy Solicitor General (Police and Security Branch) and senior members of the Department of Justice. The recommendations made by the IAT that there be an 'Independent Counsel' has been implemented by engaging a lawyer from the Department of Justice who performs this function.

A number of steps must be followed before a warrant application is finally approved. In his written responses to the Committee's questions, the Director of the Service indicated that the warrant application process is initiated by the regional investigator who identifies what powers pursuant to Part II of the *CSIS Act* are required. A request is forwarded to the regional Director General, who in turn sends the request and any recommendations considered necessary to CSIS Headquarters in Ottawa.

The application is received through the Warrant Control Unit at CSIS Headquarters. The Warrant Control Unit, in conjunction with CSIS Legal Services, prepares an affidavit, and the following questions are addressed:

1) Are the powers requested in the warrant application proportionate to the risks posed by the threat?

2) Are the facts contained in the warrant supported by accurate information?

3) Is it feasible to grant the requested powers, given the availability of resources?

4) Is the warrant application consistent with the intelligence requirements of the Service?

5) Are the sources of information reliable? and

6) Is the warrant application in accordance with the plans and priorities of the Service?[11]

Once these issues have been addressed and certified, the application is reviewed by the Independent Counsel. The Service has indicated that, in practice, the Independent Counsel receives a copy of the warrant application prior to the meeting of the WRC. The Counsel meets with the affiant and the case analyst(s) and CSIS counsel to review the application. The Independent Counsel questions the individuals involved in the preparation of the materials with a view to challenging the reliability of the information contained in the application. If anyone considers that an amendment to the supporting affidavit is required as a result of the meeting with the Independent Counsel, the affidavit is presented to the WRC. Any outstanding issues that cannot be resolved during the consultation between the Independent Counsel, the affiant, the case analyst and the CSIS counsel are referred to the WRC for its consideration.

The Independent Counsel is required to make a written report to the Deputy Solicitor General on each case, which may raise any outstanding concerns that remain.

According to material prepared for the Committee by CSIS, the WRC has the ultimate responsibility for amending, rejecting or approving the application for onward consideration. As a penultimate step in the process, the affidavit is then the subject of a meeting between the Director and the Solicitor General. At that time, the Solicitor General may approve or reject it. The warrant application is then presented by CSIS to a Federal Court judge for final approval.

The Director of CSIS indicated in testimony before the Committee that a warrant application has never been rejected by the Minister. However, in his written response to the Committee's question concerning whether any warrant applications have been sent back for more work or analysis, former Solicitor General Pierre Blais noted that:

> on occasion, I have stipulated, as have previous Solicitors General, that further work and analysis be conducted in relation to applications before they were approved for presentation to the Court.

9.4 The Role of the Federal Court

The Federal Court is composed of two branches: the Trial Division and the Appeal Division. Matters involving national security can come before the Court in a number of ways.

Litigious matters involving national security concerns may arise under sections 38 or 39 of the *Canada Evidence Act* or by way of judicial review under sections 18 or 28 of the *Federal Court Act*. Applications for warrants or renewal of warrants may be made to designated judges of the Court under Part II of the *CSIS Act* (sections 21–28). Section 27 of that part provides for applications made under sections 21, 22 or 23 to a judge to be heard in private in accordance with regulations made under section 28 of the Act. No such regulations have yet been adopted by the Governor in Council.

All CSIS warrant applications before the Federal Court are heard in a courtroom located in a secure government building in Ottawa. Within that building is a room that is considered to be a 'secure environment'. The Federal Court relies on CSIS personnel to ensure that security concerns surrounding the hearing of warrant applications are satisfied. The Federal Court has also devised a number of methods for ensuring the security of court documents.

Although CSIS appears to be responsible for court security in relation to warrant applications at the Federal Court, it appears to be doing so without statutory authority. Under section 59 of the *Federal Court Act*, it is provided that:

> 59. Such services or assistance in connection with the conduct of the Court's hearings, the security of the Courts, its premises and staff, or the execution of its order and judgments ... shall be provided, at the request of the Chief Justice, by the Royal Canadian Mounted Police or such other police force as the Governor in Council may designate.

The Committee believes that it is a proper role of the RCMP to provide court security during warrant applications under the *CSIS Act*. Accordingly, the Committee urges the Solicitor General to clarify this matter in order to ensure that the RCMP provides court security as described under the current authority of the *Federal Court Act*.

The Committee is concerned that the current arrangements for hearing warrant applications under the *CSIS Act* are inadequate. The current location of the secure courtroom may indeed pose difficulties insofar as the perceived independence of the Court is concerned. The Committee understands that the Federal Court is involved in a multi-year plan to construct new premises, with a secure courtroom in each courthouse, at a number of locations across Canada. The Committee supports the efforts of the Federal Court to establish new premises throughout the country and accordingly makes the following recommendation.

RECOMMENDATION 58

The Committee recommends that the government give priority to the establishment of a secure courtroom environment for the hearing of warrant applications under the *CSIS Act* or any other matters that involve national security issues.

9.5 Part II of the *CSIS Act* and the Developing Case Law

9.5.1 *The Charter*

The most important case to date that has challenged the judicial control provisions of the *CSIS Act* is *Atwal* v. *The Queen*.[12] This case came before the Federal Court Trial

Division twice and was also heard once by the Federal Court of Appeal. The impact of this case, in addition to the recommendations of the Independent Advisory Team, led to the establishment of extensive internal review procedures for the processing of warrant applications within the Service.

In *Atwal*, the Federal Court of Appeal dealt directly with the constitutionality of the warrant provisions of the *CSIS Act* with respect to the "search and seizure" provisions in section 8 of the *Charter*. Writing for the majority of the Court, Mr. Justice Mahoney referred to Mr. Justice Dickson's opinion in *Hunter* v. *Southam* where he stated:

> The State's interest in detecting and preventing crime begins to prevail over the individual's interest in being left alone at the point where credibly-based probability replaces suspicion. History has confirmed the appropriateness of this requirement as the threshold for subordinating the expectation of privacy to the needs of law enforcement. Where the State's interest is not simply law enforcement as, for instance, where State security is involved, or where the individual's interest is not simply his expectation of privacy as, for instance, when the search threatens his bodily integrity, the relevant standard might well be a different one.[13]

Mr. Justice Mahoney referred to the reasoning in *Hunter* to argue that a different standard may be operative where national security is involved. To do so is not necessarily to apply a lower standard but rather one that takes account of reality:

> Since the *CSIS Act* does not authorize the issuance of warrants to investigate offences in the ordinary criminal context nor to obtain evidence of such offences, it is entirely to be expected that s. 21 does not require the issuing judge to be satisfied that an offence has been committed and that evidence thereof will be found in execution of the warrant. [The] Act [authorizes] investigation of threats to the security of Canada and, *inter alia*, the collection of information respecting activities that may, on reasonable grounds, be suspected of constituting such threats.[14]

As can be seen from the majority judgment of the Federal Court of Appeal, the Court accepted the reasoning in *Hunter* that suggests that in matters of national security a different standard should apply. As a minimum criterion for the issuance of a warrant in matters of national security, the majority Court agreed that a judge needed only to be satisfied on reasonable and probable grounds established on sworn evidence that a threat to the security of Canada existed and that a warrant was required to enable investigation.

In a frequently cited dissenting opinion, Mr. Justice Hugessen argued that section 21 of the *CSIS Act* is "incompatible with section 8 of the Charter" and focused on the "test" enunciated by Mr. Justice Dickson in *Hunter* which he believed should apply in such cases. The test stated that where (i) there must be reasonable and probable grounds to believe, (ii) an offence has been committed, (iii) a reasonable and proportionate relationship between a relevant state interest and the proposed intrusion must be demonstrated.[15]

In Mr. Justice Hugessen's view, section 21 of the *CSIS Act* failed to meet the third criterion noted above, as subsections 21(2)(*a*) and 21(3), when read together, require that a judge be satisfied that there are reasonable grounds to believe that a warrant "is required to enable the Service to investigate a threat to the security of Canada." Mr. Hugessen concluded that section 21

> does not provide any reasonable standard by which the judge may test the need for a warrant. There is no requirement to show that the intrusion into the citizen's privacy will afford evidence of the alleged threat or will help to confirm its existence or non-existence. Nothing is required to show a relationship between the information it is hoped to obtain from the intercepted communication and the alleged threat to the security of Canada.[16]

Despite the forceful opinion of Mr. Justice Hugessen, the majority in *Atwal* held that the warrant provisions of the *CSIS Act* were sustainable under the *Charter*.

The Committee believes the issues raised by Mr. Justice Hugessen are important from both a policy and a legal viewpoint. Parliament may wish to take a more detailed look at the matters raised in the *Atwal* decision. This issue is therefore addressed further in the concluding chapter of this Report.

In another issue before the Court, regarding Mr. Atwal's request to seek access to the supporting material for the warrant application, the Court unanimously held that the accused should be granted access to the supporting materials after material from which the identity of a person could be inferred had been deleted. The Court ordered that the case be brought back before the trial judge to deal with the issue of disclosure.

In an unusual turn of events, the respondent consented to the rescission of the warrant, as the Court was advised that extensive and serious errors had been discovered by CSIS in its supporting affidavit. Apparently the consequence of these errors was that "insufficient evidence remained to sustain the warrant."[17] As a result of this revelation and the rescission of the warrant, the charges of conspiracy to commit murder against Mr. Atwal and eight others were stayed.

In 1988, the Inspector General of CSIS produced a lengthy report entitled "The CSIS Warrant Application Process in Respect of Harjit Singh Atwal". The Committee did not have access to this report or to the materials related to the *Atwal* affidavit. The only evidence that came to the attention of the Committee regarding whether any further warrants had been issued on the basis of erroneous information was during SIRC's appearance before the Standing Committee on Justice and Solicitor General on its Main Estimates. At that time, SIRC indicated that no wrongly issued warrants had "come to the attention" of the Review Committee.

9.5.2 *The Application of Criminal Law Standards to the CSIS Act*

It is not clear whether criminal law standards will be accepted by the courts in cases dealing with national security issues. The *Atwal* decision did not resolve this issue,

although the Court identified what is deemed to be different standards where the state's interest is not simply law enforcement. Mr. Justice Heald, during proceedings before the Trial Division, stated quite clearly that:

> In my view, criminal law jurisprudence is not the appropriate jurisprudence to be applied under the *CSIS Act*... Because of the distinctly different legislative purposes, there is, necessarily, a different focus to be applied when interpreting domestic surveillance legislation in contradistinction to the focus to be given to the application and interpretation of normal law enforcement legislation as the *Criminal Code* of Canada.[18]

The difficulty with accepting the contention that national security concerns should be treated on a different footing than criminal law matters is that the courts and Parliament have failed to define satisfactorily what is meant by "national security". Professor M.L. Friedland's opening words in his study for the McDonald Commission noted:

> I start this study on the legal dimensions of national security with a confession: I do not know what national security means. But then, neither does the government.[19]

These words, written in 1979, are as relevant today as they were then.

With respect to the warrant provisions of the *CSIS Act*, the Committee believes that the courts will eventually develop the tests required to provide appropriate checks and balances that take account of the interests of the state and those of the individual. As noted in a legal opinion prepared for the Committee:

> Slowly the courts have developed the tests required in the CSIS warrant situation. They have not reached the level in the *Criminal Code*, by the mere fact that they are a "new" remedy. In time there is every reason to believe that a body of authority will develop providing these checks and balances that now exist in the *Criminal Code*.[20]

The Committee acknowledges that placing CSIS warrants on the same footing as the tests, standards and balances applied in the *Criminal Code* may involve delicate policy choices. It is also apparent, however, that an appropriate case may come before the courts to challenge the long held distinction between "national security" and "criminal law" interests. One such case may be *Chiarelli* v. *The Minister of Employment and Immigration*.

The *Chiarelli* case, which came before the Federal Court of Appeal by way of a reference under the *Federal Court Act*, suggests that the courts will look at criminal law standards in the area of national security concerns. Indeed, Mr. Justice Pratte noted in his opinion on the case that:

> The evidence before us shows that there is as much need to protect the secrecy of police investigations of organized criminal activities as to protect the secrecy of security intelligence investigations.[21]

To give credence to his view, Mr. Justice Pratte cited a commentary from the attending SIRC member who heard Mr. Chiarelli's case:

> This is the first case [before SIRC] involving the RCMP. The principles that have applied to the exclusions [of evidence] are the same. They relate to the techniques employed by investigative agencies. Hitherto, that has been CSIS ... The argument is if human sources or particular information about technical sources are revealed and in the public domain, the ability to continue to employ such techniques would quickly dissolve and disappear.[22]

The majority in *Chiarelli* held that subsection 48(2) of the *CSIS Act* was contrary to section 7 and unsustainable under section 1 of the *Charter*.

The Minister of Employment and Immigration has sought leave to appeal the *Chiarelli* decision to the Supreme Court of Canada. If leave is granted, this case may provide the Supreme Court with an opportunity to address these difficult issues.

In addition, an inter-departmental technical group has been set up under the leadership of the Department of Justice. The group is expected to look at such issues as the use of CSIS information in the criminal courts. The Committee is encouraged by the testimony of the Director of CSIS before the Standing Committee on Justice and Solicitor General on the Main Estimates when he indicated the degree to which the Service considers the *Charter* to have an effect on its operations.

The Committee believes that a number of issues related to the activities of the Service and the *Charter* should be looked at by this technical group.

RECOMMENDATION 59

The Committee recommends that the inter-departmental technical group established under the direction of the Department of Justice be mandated to review 1) the constitutionality of the warrant provisions of the *CSIS Act* and 2) the applicability of criminal law standards to the adjudication of matters involving the *CSIS Act*.

9.6 Part II of the *CSIS Act*: The 'Judicial Control' Provisions

9.6.1 *Operating at a Lower Threshold*

The warrant application and approval process is governed by sections 21 to 28 of the *CSIS Act*. Section 21 requires that ministerial approval be obtained before an application for a warrant can be brought before a judge of the Federal Court. The section also requires that the Director of the Service or any employee designated by the Minister have "reasonable grounds to believe" that a warrant is required to investigate a threat to the security of Canada or perform the Service's duties and functions under section 16 of the

CSIS Act (i.e., collect information concerning foreign states and persons). It is important to recognize that the warrant provisions are qualified by the provisions of the *CSIS Act* where the mandates of the Service are described. Specifically, attention should be brought to section 12 of the Act which provides that:

> The Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyze and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada...

It is the ability of CSIS to carry on its functions on the mere "suspicion" that constitutes a lower investigative threshold than that provided to law enforcement agencies under the *Criminal Code*. As an example, police agencies such as the RCMP must act upon reasonable grounds to believe that an offence has been committed or a conspiracy has been undertaken (as defined in the *Code*) before they can acquire wiretap or search warrants.

As noted in a legal memorandum on the section 12 primary mandate of the Service, prepared for the Inspector General in 1985:

> There is ... nothing in the language of section 12 [of the *CSIS Act*] to suggest that anything other than the ordinary meaning of the word "suspected" was intended by Parliament. Accordingly, the state of mind required by the Service under this phrase is not that of absolute certainty or even genuine confidence or opinion that an activity constitutes a threat to the security of Canada; rather, all that appears to be required is that the Service feel or have a *bona fide* partial belief that a particular activity may constitute a threat ... [T]here must be some evidence that the activity involved may constitute a "threat to the security of Canada".[23]

This same legal memorandum noted that the ability of CSIS to operate at a lower threshold was consistent with the functions of a security intelligence agency, as opposed to a law enforcement agency.[24]

9.6.2 *Specific Requirements of the Warrant Provisions*

Section 21(2) outlines what matters are to be specified in the affidavit accompanying an application for a warrant. Specifically, it requires that the following be included:

1) the facts relied on to justify the belief that the Service has reasonable grounds to believe that a warrant is required to investigate a threat to the security of Canada or to perform its duties under section 16;

2) a statement that non-intrusive methods have been tried and failed or why it appears that they are unlikely to succeed;

3) the types of communication to be intercepted or information obtained;

4) the person who possesses the information or whose communication is to be intercepted;

5) the persons or classes of persons who will execute the warrant;

6) the location of the place where the warrant will be executed;

7) the duration of the warrant;

8) a statement concerning any previous applications concerning the target of the warrant.

The section does not require that the interception techniques or the manner in which information, records, documents or other things are to be obtained be specified in the application.

Section 21(4) requires certain matters to be specified in warrants. These include

1) the type of communication to be intercepted;

2) the type of information, record, document or thing to be obtained;

3) the powers to enter, search and install referred to in subsection 21(3) paragraphs (*a*) to (*c*);

4) the identity of the person whose communication is to be intercepted or who has possession of the information to be obtained;

5) the person or type of person who may execute the warrant and use its powers;

6) the location of the place where the warrant is to be executed;

7) the duration of the warrant; and

8) such terms and conditions as the issuing judge may impose.

Neither this section nor any other section of the *CSIS Act* requires the Service to identify the techniques or methods to be used.

The Director of CSIS, during testimony before the Committee, mentioned two conditions that are often included in warrants granted under the *CSIS Act*. One condition relates to the protection against interception of any communication between the person who is the subject of the warrant and his or her solicitor. Another common condition refers to the interception of communications involving innocent third parties. It is the

Committee's understanding that when either of these types of communications is intercepted it is immediately destroyed by the Service.

The Committee believes that these and other conditions applied routinely by the Federal Court should be codified in the Act. In particular, the Committee agrees that solicitor–client communications and communications involving innocent third parties should be granted statutory protection under the Act.

RECOMMENDATION 60

The Committee recommends that section 21(4) of the *CSIS Act* be amended to provide statutory protection to solicitor–client communications unless the solicitor is the target of a judicial warrant.

RECOMMENDATION 61

The Committee recommends that section 21(4) of the *CSIS Act* be amended to provide statutory protection to communications involving innocent third parties.

RECOMMENDATION 62

The Committee recommends that section 21(4) of the *CSIS Act* be amended to add to the list of warrant limitations those now applied routinely by Federal Court judges.

Section 21(5) of the Act defines the maximum duration of warrants. Currently, warrants involving subversive investigations can be issued for a period not exceeding sixty days, while warrants involving all other forms of investigation may be issued for up to one year. Under the *British Security Service Act, 1989*, warrants can be authorized only for a period of six months.[25] Under British law, warrants that have expired can be renewed for a subsequent six-month period. The Committee believes the current provision in the *CSIS Act*, which allows warrants to be issued for one year, is excessive. The Committee is concerned that allowing CSIS to maintain intrusive surveillance for such a lengthy period may result in the Service conducting exploratory investigations in its efforts to obtain information. The Committee believes that a shorter period, in line with the British model, may give the Service a sufficient length of time to operate intrusive surveillance against a target. At this time, however, the Committee believes this matter should be studied by the government and SIRC.

RECOMMENDATION 63

The Committee recommends that the length of time for which warrants can be issued and renewed under the *CSIS Act* be reviewed by SIRC and by the Government.

Section 22 of the *CSIS Act* deals with renewal of warrants, while section 23 provides for the removal of any thing that was installed either to intercept any communication or to obtain any information, record, document or thing.

Section 24 of the *CSIS Act* states that a warrant issued under section 21 or 23 is to be effective notwithstanding any other law. Section 24 further authorizes "any other person to assist a person who that person believes is acting in accordance with such a warrant".

Section 25 of the *CSIS Act* specifically excludes the *Crown Liability Act* from applying to the use or disclosure of any communication intercepted under the authority of a warrant issued under section 21 or to the disclosure of the existence of any communications.

Under section 26 of the *CSIS Act*, Part VI of the *Criminal Code* is deemed not to apply in relation to any interception of a communication authorized under section 21. Section 27 of the *CSIS Act* provides that an application to a judge, under sections 21, 22 or 23 of the Act, for a warrant or a warrant renewal shall be heard in private in accordance with regulations made under section 28 of the Act.

Section 28 of the *CSIS Act* states that the Governor in Council may make regulations:

> (*a*) prescribing the forms of warrants that may be issued;
>
> (*b*) governing the practice, procedures, and security requirements applicable to hearings or applications for warrants or renewals of warrants; and
>
> (*c*) specifying the places where those hearings may be held and the places where, and the manner in which, records or documents concerning those hearings shall be kept.

No rules, regulations or procedures have been developed under section 28. The Committee believes that specific regulations should be developed with respect to the practice and procedure for warrant applications under the *CSIS Act*. Such regulations should be established to regularize the practice that has developed over the past five years at the Federal Court.

RECOMMENDATION 64

The Committee recommends that the Governor in Council develop regulations in respect of warrants as provided for under section 28 of the *CSIS Act*.

9.7 Related Issues

9.7.1 *Role of the Amicus Curiae*

The Committee believes that the warrant approval process of CSIS's Warrant Review Committee is working well. However, the Committee is concerned about the role of the Independent Counsel.

The Committee believes it would be more appropriate for an independent counsel (or *amicus curiae*) to attend the warrant approval hearing before the Federal Court. The provision of counsel to appear before the judge hearing a warrant application would allow the judge to hear both sides of the argument. It is in the best traditions of the adversary process to allow counsel for each side to present views before an adjudicator. The Committee believes that the absence of an independent counsel appearing before the Federal Court places the judge in the awkward situation of having to play devil's advocate. Indeed, the Committee understands that the Federal Court might be supportive of allowing an independent counsel to attend during CSIS warrant applications.

This view has also been proposed by SIRC and the Canadian Bar Association. The Review Committee stated that:

> A lawyer who is security cleared but who is not employed by the Government of Canada would be perceived as truly acting on behalf of the potential target of the warrant. A lawyer employed by the Department of Justice may provide equally adequate representation to the potential target but is less likely to be perceived as acting in the target's interest since he or she would be, after all, employed by the government which is seeking judicial approval to intrude upon the private life of that individual.[26]

Another criticism raised by SIRC is that, under the current process, the Independent Counsel is concerned with ensuring that the information CSIS intends to cite in its application is accurate. SIRC believes that the Independent Counsel should be concerned instead with challenging the need for the warrant. The Committee agrees. The proper role of an *amicus curiae* is not only to challenge the veracity of the evidence being presented, but to be in a position to challenge the claim of the Service that the use of intrusive techniques is necessary. The Committee believes that choosing appropriate counsel to play the role of *amicus curiae* before the Federal Court is of great importance. In this regard, the Committee recommends that the Federal Court, in consultation with the Canadian Bar Association, forward a list of counsel to the Minister and that the Minister arrange for such persons to be security cleared.

RECOMMENDATION 65

The Committee recommends that the *CSIS Act* be amended to provide that security cleared counsel attend before the Federal Court as *amicus curiae* during each warrant application under Part II of the Act.

RECOMMENDATION 66

The Committee recommends that the Federal Court, in consultation with the Canadian Bar Association, prepare a list of appropriate counsel to take the role of *amicus curiae* during the warrant application process before the Federal Court.

9.7.2 *The Role of the Inspector General and SIRC*

The Inspector General and SIRC have reported extensively on the use of warrants by CSIS. The Committee believes that both the Inspector General and SIRC can play an important role in maintaining additional oversight of the use of warrants by CSIS. For its part, the Service should take comfort in the fact that the reviews and investigations by the Inspector General and SIRC provide a form of quality control of the warrant process, something any agency should welcome as a means of improving its product.

It appears that although no specific statutory provision gives the Inspector General or SIRC jurisdiction to review the warrant process, each agency has interpreted its mandate under the *CSIS Act* to allow these activities. The Committee believes that further statutory refinement is unnecessary.

9.7.3 *Emergency Warrants*

SIRC has recommended that the *CSIS Act* be amended to provide for the issuance of emergency warrants. Such warrants would be issued in emergency situations requiring quick action by the Service and would have a life not exceeding 72 hours. Although SIRC has not provided the Committee with any evidence to indicate that such a procedure would have been necessary during the past five years, the Review Committee has suggested that such powers could prove useful.

Mr. Bernard Marentette of the CSIS Employees' Association (Quebec Region) also testified before the Committee that the current system for obtaining warrants is cumbersome and excessively procedural. Mr. Marentette expressed doubts about whether the warrant approval system could respond quickly in an urgent case. In contrast, the Director of CSIS indicated in his written responses to the Committee's questions that there have been no incidents where CSIS was unable to obtain a warrant in time.

The Committee believes that the Director of the Service may be in the best position to assess whether an emergency warrant power is required. The Committee also has concerns about the constitutionality of emergency warrant provisions that would allow CSIS to employ intrusive techniques, albeit for a short period, in the absence of prior judicial authorization. At this point, the Committee is of the view that an emergency warrant provision is unnecessary.

9.7.4 *The Use of Human Sources*

The Director of CSIS has indicated that a ministerial direction governing the use of human sources was issued on October 30, 1989. The key principles set out in this direction are as follows:

- sources are to be used when and to the extent that it is reasonable and necessary;
- the need to use sources must be carefully weighed against possible damage to civil liberties;
- sources must be centrally directed and controlled;
- sources must act within the law;
- sources are to be managed so as to protect both the security of CSIS operations and the personal safety of the sources; and
- sources should be treated ethically and fairly by CSIS, in terms of compensation and handling.

SIRC's 1988–89 Annual Report noted that:

> We have examined changes that have taken place in the Human Sources Branch and were impressed on the whole by a new approach that stresses the principles to be followed rather than detailed rules ... In general we feel that sources are well managed.[27]

Nevertheless, the Committee does not know the extent to which human sources are used in the day-to-day operations of the Service. Indeed, the Committee does not know how effective or necessary it is for the Service to use human sources.

The Director of CSIS indicated during his testimony before the Committee that the warrant procedure does not apply to human sources and surveillance.

Few would deny that the use of human sources could be the most intrusive of investigative tools employed by the Service. The Committee believes that the use of human sources, like other intrusive techniques, may infringe upon the rights and freedoms of Canadian citizens and landed immigrants if their use is not properly overseen.

The Director of CSIS expressed concern in his written responses to the Committee's questions that "to impose Federal Court warrants on source operations would seriously hamper the Service's collection ability". SIRC has indicated that it believes that requiring

a judicial warrant for the use of human sources "would put too onerous a restriction on the Service. It would be difficult, for example, to fit casual or "walk in" sources, sources under development, and many unpaid sources into such a scheme."[28] In its brief to the Committee, SIRC recommended that the *CSIS Act* be amended to prescribe that the Solicitor General issue precise guidelines to the Service on the use of human sources. The Committee is generally in agreement with SIRC's recommendation.

Requiring judicial warrants for the use of long-term human sources found favour with Professor Jean-Paul Brodeur of the University of Montreal. In testimony before the Committee, he indicated that when an infiltration operation lasts for 12 or 18 months, the possibility of judicial authorization should be considered.

The Committee does not accept that the use of human sources by CSIS should be subject to judicial authorization. The Committee believes, however, that the use of human sources by the Service should be monitored closely by SIRC.

RECOMMENDATION 67

The Committee recommends that SIRC regularly monitor and report on the use of human sources by CSIS.

9.7.5 *The 'Right to Privacy' and the Use of Participant Surveillance*

Recent judgments of the Supreme Court of Canada have recognized the reasonable expectation of privacy of the individual in the context of "participant surveillance" under Part VI of the Criminal Code.[29]

On January 25, 1990, the Supreme Court of Canada in *Mario Duarte* v. *The Queen* characterized the practice of participant surveillance under the *Criminal Code* as an infringement of the rights and freedoms guaranteed by section 8 of the *Charter*. The Court concluded that the surreptitious electronic recording of a private communication, without judicial authority, should be viewed as a search and seizure in all circumstances except where all parties to a conversation have consented to it being recorded. In coming to its conclusion, the Court made the following observations:

> If privacy may be defined as the right of the individual to determine for himself when, how, and to what extent he will release personal information about himself, a reasonable expectation of privacy would seem to demand that an individual may proceed on the assumption that the State may only violate this right by recording private communications on a clandestine basis when it has established to the satisfaction of a detached judicial officer that an offence has been or is being committed and that interception of private communications stands to afford evidence of the offence ...
>
> The *Charter*, it is accepted, proscribes the surreptitious recording by third parties of our private communications on the basis of mere suspicion alone. It would be

> strange indeed if, in the absence of a warrant requirement, instrumentalities of the State, through the medium of participant surveillance, were free to conduct just such random fishing expeditions in the hope of uncovering evidence of crime, or by the same token, to satisfy any curiosity they may have as to a person's views on any matter whatsoever.[30]

In view of the Court's strong characterization of the use of participant surveillance as an infringement of the *Charter*, the Committee believes that the *CSIS Act* should be amended to provide that no electronic surveillance, whether consented to by a participant in the private communication or otherwise, can be carried out except under the authority of a judicial warrant. This recommendation found favour with the Canadian Bar Association during its testimony before the Committee.

The Director of CSIS indicated when he appeared before the Committee that the Service operates on the assumption that "anything that in any way is going to invade somebody's privacy in some manner ... requires a warrant."

RECOMMENDATION 68

The Committee recommends that the *CSIS Act* be amended to provide that the use of "participant surveillance" may be carried out only under the authority of a judicial warrant as described under Part II of the Act.

9.7.6 *Electromagnetic Eavesdropping*

As noted above, the Director of CSIS has indicated that the Service currently seeks a judicial warrant whenever it is likely to invade somebody's privacy. This comment was made in response to a question regarding whether a warrant would be required if someone was intercepting information from electromagnetic radiation given off by electronic equipment such as a computer. This activity, called "electromagnetic radiation eavesdropping", enables someone to intercept electromagnetic radiation emissions from a computer terminal and reproduce the image or text of that information on a monitor.

This technology, which is relatively inexpensive, has important implications with respect to individual rights and freedoms.

It is likely that CSIS uses electromagnetic eavesdropping technology in its operations. The Committee is aware that the Communications Security Establishment (CSE) is capable of employing this technology and that it shares information with CSIS. The question is whether these intrusive techniques are used against Canadian citizens and landed immigrants.

The Committee understands that the use of electromagnetic eavesdropping technology may not in fact constitute an offence under the current provisions of the *Criminal Code*. Indeed, one commentator has indicated that:

> In considering the possible application of *Criminal Code* offences to electromagnetic radiation eavesdropping two points should be borne in mind: (1) it is unlikely that any incidental offences will be committed in carrying out electromagnetic radiation eavesdropping (i.e., there is no need to break and enter or trespass on property to effectively use the technology), and (2) it is very unlikely that those committing the eavesdropping will be detected, since, for example, the eavesdroppers could have the equipment set up in the back of a van several blocks away from the source of the radiation.[31]

Despite the apparent shortcomings of the *Criminal Code*, the Committee believes that the use of this technology by CSIS or the CSE against Canadian citizens or landed immigrants should be subject to the authorization of a judicial warrant. In addition, CSIS should not be allowed to use or rely upon information that it is unable to obtain under its statutory mandate. The requirement that both CSIS and the CSE be subject to judicial authorizations in these limited circumstances would prevent the Service from circumventing the limitations imposed upon itself but not CSE.

The Committee is not sure how this policy mandate should be implemented in statutory form. It may require amendments to the *Criminal Code* and the *CSIS Act*, in addition to implementing it in the statutory mandate suggested for the CSE.

RECOMMENDATION 69

The Committee recommends that the Department of the Solicitor General study the matter of CSIS and the CSE obtaining judicial authorization before using electromagnetic eavesdropping technology for investigative purposes.

9.7.7 *Opening Mail*

Section 40(3) of the *Canada Post Corporation Act* gives the Service the authority to open mail in the course of its operations and states that:

> 40. (3) Notwithstanding any other Act or law, but subject to this Act and the regulations and to *Canadian Security Intelligence Service Act* and the *Customs Act*, nothing in the course of post is liable to demand, seizure or detention.

In its 1986–87 Annual Report, SIRC noted that a formal Memorandum of Understanding was being prepared between CSIS and Canada Post. SIRC also indicated that it had reason to suspect that mail interception by the Service would increase. In the same Annual Report, SIRC expressed concern about the use of mail tracing by the Service—that is, the provision to the Service by Canada Post of a list of names and addresses with which CSIS targets correspond. The Committee believes that the use of such information should be allowed only under the authority of a judicial warrant. The

right to privacy is adversely affected by such a practice. Judicial authorization should be obtained in each instance where mail tracing is required.

RECOMMENDATION 70

The Committee recommends that the *Canada Post Corporation Act* be amended to provide that the acquisition of information by CSIS, obtained by tracing the names and addresses of persons with whom targets correspond, require judicial authorization.

9.7.8 *Statistics Available Under the Official Secrets Act*

Under the provisions of the *Official Secrets Act*, more statistical information concerning the issuance of warrants was required to be made public than is available under current legislation. Although SIRC has attempted to publish the aggregate number of warrants issued under the *CSIS Act*, these figures are not very helpful. As noted in SIRC's brief to the Committee:

> Under the *Official Secrets Act*, generally, each warrant authorized only one covert technique against only one target, whereas one warrant under the *CSIS Act* can authorize the use of many powers against many targets.

The Committee believes it is important to provide the public with information regarding the use of intrusive surveillance techniques by CSIS against Canadian citizens and landed immigrants. The use of intrusive surveillance against Canadian citizens and landed immigrants directly affects the rights of individuals. The Committee believes that the public should know the extent to which such techniques are used. The Committee is aware that, at least under the provisions of the *Criminal Code*, Canadian law enforcement authorities request twenty times more authorizations to conduct electronic surveillance than their American counterparts.[32] The Committee believes that providing more information in this respect will not only inform the public but may assist in the development of appropriate policy choices.

The Committee received a number of briefs that support the view that the *CSIS Act* should be amended to require the publication of more precise warrant statistics. The Committee believes that SIRC should be empowered to compile and report on these findings. Support for this proposal came from the Canadian Bar Association, the Canadian Association of University Teachers, the British Columbia and Ontario Law Unions, the Canadian Jewish Congress and the British Columbia Civil Liberties Association.

RECOMMENDATION 71

The Committee recommends that the *CSIS Act* be amended to provide that SIRC be authorized specifically to compile and analyze warrant statistics and that SIRC be required to publish annually statistics containing the number of Canadian citizens or landed immigrants who have been affected by surveillance powers granted to CSIS under judicial warrants.

NOTES

1. Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (1981) "Freedom and Security Under the Law" (Second Report Volume 1). Ottawa, Supply and Services, p. 150.

2. McDonald Commission, Second Report, Volume 1, p. 161.

3. McDonald Commission, Second Report, Volume 1, p. 177.

4. Parliament of Canada, *Annual Report* of the Solicitor General, as required by subsection 16(5) of the *Official Secrets Act*, 1983.

5. Senate of Canada, *A Delicate Balance: A Security Intelligence Service in a Democratic Society*, 1983, Ottawa, Report of the Special Committee on the Canadian Security Intelligence Service, p. 21.

6. Security Intelligence Transitional Group papers, Volume II, 1981–84, p. 235.

7. McDonald Commission, Second Report, Volume 1, p. 513.

8. Security Intelligence Review Committee, *Annual Report 1986–87*, p. 35.

   Canada, House of Commons, Minutes of Proceedings and Evidence of the Special Committee on the Review of the *CSIS Act* and the *Security Offences Act*, Issue No. 3, (November 2, 1989), pp. 24–25.

9. *CSIS Act Five Year Review*, Implementation Status of the Osbaldeston Report Recommendations, written responses of the Director of CSIS to the Special Committee, February 1990, p. 28.

10. People and Process in Transition, Report to the Solicitor General by the Independent Advisory Team on the Canadian Security Intelligence Service, 1987, p. 36.

11. *CSIS Act Five Year Review*, p. 33.

12. *Atwal* v. *Canada* [1987], 2 F.C. 309 (F.C.T.D.); 78 N.R. 292; Doc. No. CSIS 66–85.

    Atwal v. *Canada* [1988], 1 F.C. 107 (F.C.A.); (1987), 79 N.R. 91; 36 c.c.c. (3d) 161; 59 C.R. (3d) 339; Doc. No. A– 339–87.

    Atwal v. *R.* [1987], 1 F.C. 154 (F.C.T.D.); (1987), 80 N.R. 4; Doc. No. CSIS 66–85.

13. Dickson C.J. as quoted in *Atwal* v. *Canada* [1988], 1 F.C. 107 (F.C.A.), p. 133.

14. *Ibid.*

15. *Ibid.*, p. 150–151.

16. *Ibid.*, p. 151.

17. *Atwal* v. *Canada* [1988], 1 F.C. 154 (F.C.T.D.), p. 157.

18. *Atwal* v. *Canada* [1987], 2 F.C. 309 (F.C.T.D.), pp. 322 and 324.

19. McDonald Commission, *National Security: The Legal Dimensions*, a study prepared for the Commission by M.L. Friedland, Ottawa, 1980, p. 1.

20. Special Committee on the Review of the *CSIS Act* and the *Security Offences Act*, "An Analysis of Sections 2, 12, 21 to 28 of the *CSIS Act*: The CSIS Mandate and the *Charter*", A Legal Analysis submitted to the Committee by L.A. Vandor, March 16, 1990, p. 32.

21. *Chiarelli* v. *Minister of Employment and Immigration*, unreported, February 23, 1990, Court File No. A–219–89, Pratte J.A.'s judgment, p. 19.

22. *Ibid.*, p. 16.

23. "Interpretation of the Scope of the Primary Mandate of the Canadian Security Intelligence Service and, in particular, of the Definition of 'Threats to the Security of Canada', memorandum to Dr. Richard Gosse, Q.C., prepared by E.A. Cronk, March 29, 1985, pp. 54–55.

24. *Ibid.*, p. 55.

25. *Security Service Act, 1989*, c.5, section 3.

26. Written response of the Security Intelligence Review Committee to the Special Committee, January 11, 1990, p. 10.

27. Security Intelligence Review Committee, *Annual Report 1988– 89*, p. 26.

28. SIRC, *Annual Report 1988–89*, p. 74.

29. *R.* v. *Duarte* [1990], 1 S.C.R. 30, as applied in *R.* v. *Wiggins* [1990], 1 S.C.R. 62.

30. *R.* v. *Duarte* [1990], 1 S.C.R. 30, pp. 46 and 48.

31. David A. Steele, "Eavesdropping on Electromagnetic Radiation Emanating from Video Display Units: Legal and Self–Help Responses to a New Form of Espionage", *Criminal Law Quarterly* 32/2 (March 1990), p. 263.

32. Law Reform Commission of Canada, *Electronic Surveillance*, Working Paper 47, Ottawa, 1986, p. 10.

CHAPTER TEN

Review Mechanisms — The Inspector General

10.1 The Office of the Inspector General

Section 30(1) of the *CSIS Act* obliges the Government of Canada to establish an Inspector General. This office is an unusual one in Canada. Although sometimes referred to as the Inspector General of CSIS, the office-holder is not an employee of the Service. On the contrary, the Inspector General, while a public servant, is part of the Secretariat of the Solicitor General's Department. As such, the office holder is responsible to the Deputy Solicitor General.

10.2 Functions

The Inspector General has a number of statutory functions. These are described in sections 30, 33 and 40 of the *CSIS Act*. Subsection 30(2) requires the Inspector General to do three things. The office holder must review the operational activities of the Service; monitor compliance by the Service with its operational policies; and provide a certificate on each occasion that the Director makes a report to the Solicitor General.

Section 30 of the Act does not require the Inspector General to provide reports concerning either the monitoring or the review functions. It must be assumed, therefore, that obligations in this respect extend only so far as instructions are provided to the office holder by the Deputy Solicitor General.

The objective of the certification process is described in section 33(2) of the *CSIS Act*. It requires the Inspector General to state the extent to which he or she is satisfied with the Director's report and whether any activity or thing done by the Service was:

(*a*) not authorized by or under this Act or contravenes any direction issued by the Minister under subsection 6(2); or

(*b*) involves an unreasonable or unnecessary exercise by the Service of any of its powers.

The section also requires that certificates be forwarded direct to the Minister. Section 33(3) further requires the Minister to forward both the Director's report and the Inspector General's certificate to SIRC.

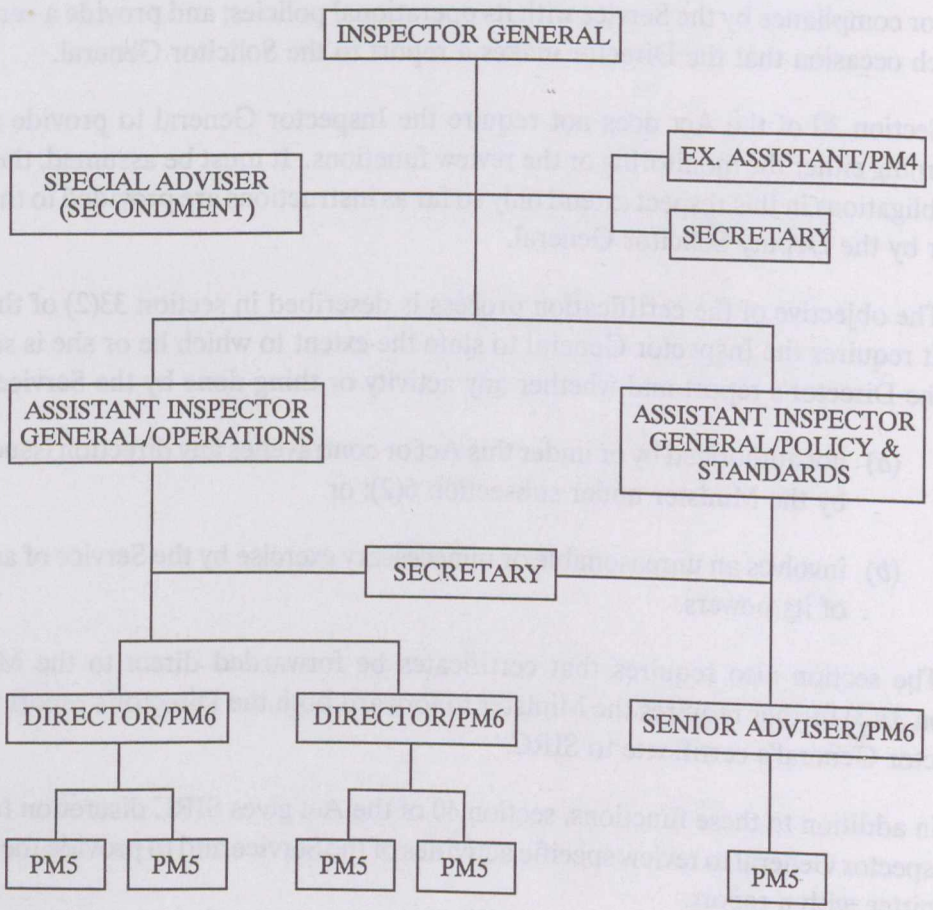
In addition to these functions, section 40 of the Act gives SIRC discretion to direct the Inspector General to review specific activities of the Service and to provide the Review Committee with a report.

The *CSIS Act* does not specifically require the Inspector General to examine the effectiveness and efficiency of the Service. The examination of compliance with the standards imposed by the *CSIS Act*, ministerial directions, Federal Court warrants and operational policies may, however, cause the Inspector General to raise issues of effectiveness and efficiency as well as those of legality and propriety.

10.3 Budget and Staffing

To perform these functions, the Inspector General has an operating and capital budget for 1990–91 of $1,059,000. This represents a 46.3 per cent budgetary increase over the 1986–87 fiscal year. Staffing level, over this period have risen from 9 to 12 person-years. The staff is currently divided into two streams. One is under an Assistant Inspector General, Operations who deals with the monitoring and review functions. The other is under an Assistant Inspector General, Policy and Standards. Each Assistant Inspector General is at the EX2 level and other senior personnel are at the PM6 (Director) and PM5 (reporting to the Director) levels. The organization chart of the Office of the Inspector General is set out in Figure 10.1.

FIGURE 10.1
STRUCTURE OF THE OFFICE OF THE INSPECTOR GENERAL OF CSIS



10.4 Views of the Current and Former Inspectors General

There have been two Inspectors General since the inception of the Office in 1984. Dr. Richard Gosse served from 1985 until 1988. Richard Thompson was appointed in July 1988 and is the present incumbent.

To ensure that the Office of the Inspector General is fulfilling its statutory functions, the Committee asked to see all reports and certificates prepared by or for the Inspector General's Office. Although some of the reports and certificates had already been released under the *Access to Information Act*, the Solicitor General declined to provide the Committee with unexcerpted copies. The Deputy Solicitor General informed the Committee that it was the opinion of legal counsel that all certificates and reports provided by the Inspector General to the Solicitor General constituted advice to the Minister. The Committee subsequently requested a copy of that opinion. At the time of drafting this section of the Report, no reply had been obtained from the Deputy Solicitor General on this matter.

The Committee did eventually receive several substantial legal opinions that had been prepared for the Inspector General by external legal counsel. The Committee found these to be most useful in considering certain aspects of its mandate. With the exception of certain legal opinions, all were classified at either the "secret" or "top secret" level.

The Committee did, however, hear testimony and receive written responses to questions from the current Inspector General, Mr. Richard Thompson, and the former office holder, Dr. Richard Gosse. While the Committee found the testimony and responses of Dr. Gosse relatively enlightening, it did not find those of the incumbent as helpful as it had hoped they would be. As a result, the Committee believes that it is unable to provide a comprehensive review of the Office of the Inspector General at this time.

As indicated in discussion papers released under the *Access to Information Act* concerning the *CSIS Act*, the Government intended in 1984 that the Inspector General should "maintain his/her credibility, before the public and all parties...".[1] The Committee understands the restrictions that the current Inspector General believed he was under with respect to providing material and information. However, the Committee considers that by failing to respond to questions fully during his testimony, the Inspector General did not inspire such credibility.

During his tenure as Inspector General, Dr. Gosse placed considerable emphasis on attracting persons with the appropriate training and background to work in his office, on developing a legal understanding of the role of the Inspector General, and on the certification process. Dr. Gosse recruited staff with a view to providing:

> an appropriate mix of experience and other qualifications to perform a function that requires good judgement, investigational analytical skills, and a sensitivity to national security issues, on the one hand, and the rights of the citizens to liberty and privacy, on the other.[2]

An important appointment in this regard was that of Mr. Bert Giroux, former Deputy Commissioner of the RCMP. Mr. Giroux had an extensive background in police investigations. Moreover, because of his previous experience as Director General of the Security Service, he was able to provide the window on the secret world that Dr. Gosse thought was essential.

It should be noted that the *CSIS Act* does not state explicitly that the rights and freedoms of Canadians should be protected. Yet the Act does place certain restrictions on the Service. It requires, for example, that the collection of information be limited to what is "strictly necessary" and that there be reasonable grounds for suspecting that activities constitute a threat to the security of Canada before an investigation may be undertaken. As a result, Dr. Gosse placed considerable emphasis on developing guidelines with respect to safeguards. To this end, he initiated a number of legal studies that provided opinions on such matters as the meaning of "strictly necessary"; what might constitute "unreasonable or unnecessary exercises of powers by the CSIS"; and a definition of "threats to the security of Canada".

Dr. Gosse's certificates, versions of which have been released under the *Access to Information Act*, tended to be fairly lengthy documents, running on occasion to nearly 300 pages. This was partly because they sometimes contained extensive legal analyses.

In his written response to the Committee's questions, Dr. Gosse observed that, other than identifying the functions of the Inspector General and certain aspects that should be covered, "the *CSIS Act* does not provide any guidelines as to how the Inspector General should prepare his certificate." He also stated that:

> I did not find the Director's report very helpful because it never contained the kind of detailed information that I required. The report did not provide the kind of accounting to the Solicitor General, of the Service's operational activities that enable the Inspector General to provide his certificate, in so far as compliance is concerned.

RECOMMENDATION 72

The Committee recommends that the Solicitor General, after consultation with the Inspector General, the Deputy Solicitor General and SIRC, provide a direction detailing what matters are to be included in the Director's Annual Report.

Dr. Gosse also noted in his written response to the Committee's questions that he had to take certain other steps in order to provide the Minister with a certificate. As a starting point for these other steps, he established an annual work plan for monitoring compliance by CSIS. This included such items as reviewing targeting decisions made by the Target Approval Review Committee (formerly known as the Operational Priority Review Committee) and reviewing all warrants obtained from the Federal Court. In developing his certificates, the former Inspector General paid particular attention to

compliance with the *CSIS Act*, conditions stipulated by the Court in authorizing a warrant, ministerial directions, the operational policies of the Service, and caselaw concerning the use of a permissive (or 'basket') clause in warrant applications. In addition, he conducted an annual non-compliance survey. This was achieved by visiting each regional office and questioning senior personnel as to their knowledge of any contravention of the law, ministerial direction, or operational policy by members of the Service in their region, and by conducting similar interviews at Headquarters in Ottawa. Other sources of information that the former Inspector General found useful for compliance purposes included the internal audit reports of the Service's Comprehensive Management Services Branch and briefings on particular subjects provided at his request by the Service.

With regard to the review and monitoring role, the former Inspector General commented in his written response to the Committee's questions that:

> I could review and monitor only a small fraction of the Service's operational activities, each year, and it would have been unrealistic and unnecessary to try to obtain sufficient staff to cover all of the activities.

He did conclude in retrospect, however, that given all the avenues open to him, he "was reasonably satisfied of being able to provide the Minister with an adequate certificate." Yet it should be noted that Dr. Gosse was unable to provide a certificate for the first two years of the Service's operation. This was largely because he did not have the necessary staff available.

According to the testimony of the current Inspector General, Mr. Richard Thompson, the review and monitoring functions now consume most of the Office's time and energies. In his written response to the Committee's questions, the Inspector General indicated that he does not view his review, monitoring and certification roles in terms of discrete functions. Rather, he sees them as interlocking. However, like his predecessor, Mr. Thompson does not believe it would be "practical to monitor and review all the Service's operational activities every year."

Following directions from former Solicitor General, the Honourable James Kelleher, the current Inspector General gave increased priority to planning his work and focused the certificate more on what the Solicitor General believed was its statutory purpose. To this end, the Inspector General developed a "multi-year review priorities program" and revised the format for certificates so that they could become much shorter (on average, they now run to about 30 pages).

The review priorities program is developed in consultation with the Solicitor General, the Deputy Solicitor General and SIRC. Later endorsed by the Honourable Pierre Blais when he was Solicitor General, the priorities program is now updated on an annual basis. The following list sets out the 30 review priorities identified by the Inspector General in March 1989. It lists them in terms of those begun or to be commenced during the year under review; additional reviews considered to be of high priority; and other review priorities. Solicitor General Blais endorsed 17 of these review priorities.

LIST A — REVIEWS UNDER WAY OR SCHEDULED TO COMMENCE IN 1989

TOPIC:

1. Audit of Intelligence Collected Under Warrants
2. Joint Operations with Foreign Agencies
3. Targeting Activities
4. Affidavit Preparation
5. Briefing Documents for the Solicitor General
6. Execution of Powers Granted in Federal Court Warrants

LIST B — REVIEWS CONSIDERED OF HIGH PRIORITY

TOPIC: (random order)

7. Compliance with Ministerial Direction on File Management
8. Detention, Destruction and Archiving of Information
9. Access to CSIS Information
10. Disclosure of Inf ormation to Foreign Agencies
11. Threat Assessments
12. Warrant Review
13. Warrant Acquisition and Renewal Process
14. Human Source Management
15. Compliance with Ministerial Direction on paragraph 2(d) Investigations.
16. Lawful Advocacy, Protest and Dissent
17. Security Screening - Adverse Reports

LIST C — OTHER REVIEW PRIORITIES

TOPIC: (random order)

18. Security Screening - Review of Operations and Quality Control
19. Security Screening - Order-in-Council Appointments
20. Intelligence Requirements
21. The Intelligence Product
22. Intelligence Versus Evidence
23. Targeting Policy and Practice
24. Retention of Intelligence Collected Under Warrants
25. Relations with Other Agencies in Canada
26. Disclosure of Information under subsection 19 (2) of the *CSIS Act*
27. Human Source Recruitment and Handling
28. Selected Targeting Techniques
29. Interpretation of "Interests of Canada" and "Foreign Influenced Activities" in paragraph 2(b) of the *CSIS Act*
30. Targeting Suspected Foreign Agents within Canada

The *CSIS Act* does not contemplate a particular relationship between the Inspector General and Parliament. Rather, the Act provides an avenue for advice to the Minister on the Service, particularly regarding compliance. Reviewing Bill C-157 in 1983, the Special Senate Committee noted that the role of the Inspector General was to provide:

> for the political masters of the agency, ongoing information as to its functioning. If the Solicitor General is to be politically responsible he must know what is going on in the agency, through his deputy. The Inspector General will be the Ministry's "eyes and ears" on the Service. He will be very much the "minister's man", in order to maintain an appropriate degree of ministerial responsibility, and is not to be regarded as a functionary of CSIS.[3]

The Committee partly endorses this view of the Inspector General's role. Yet it notes that there is a full range of other "eyes and ears" that the Minister can call upon should there be a need to do so. These include the Auditor General, the Comptroller General, the Director of CSIS and the Deputy Solicitor General, as well as SIRC.

The Committee was able to obtain little information about the effect that the Inspector General has had on the Service or on the work of the Secretariat of the Department of the Solicitor General. In this regard, the former Inspector General noted in his written response to questions from the Committee that:

> I have some difficulty in evaluating the impact my work made within the Ministry of the Solicitor General with respect to policy development. In submitting my certificates and reports on specific subjects I have made numerous recommendations that should have assisted the Ministry in making changes with respect to policy... I am unable to recall to what extent the work of the Inspector General had an impact on policy development within the Ministry.

In view of the recommendations made by the Independent Advisory Team concerning the need for specific ministerial directions and the existence of numerous legal studies that were produced during Dr. Gosse's tenure, the Committee is at a loss to explain this situation.

This and other factors lead the Committee to believe that the Inspector General should be totally independent in establishing the review priorities of this office. Although the Committee found no evidence that the Minister, the Deputy Minister, or SIRC has placed any undue pressure on the Inspector General, it believes that the office as now constituted is open to such influence. This could come, for example, from the Deputy Minister when the policies and programs of the Secretariat are at odds with the review priorities of the Inspector General. The Committee believes that this potential difficulty should be addressed directly.

RECOMMENDATION 73

The Committee recommends that 1) the Inspector General be obliged to consult with the Minister and the Deputy Minister of the Department of the Solicitor General and with SIRC concerning the review priorities of the office; and 2) the Inspector General make all decisions regarding the order of review priorities, which decisions shall be conclusive.

The reduction of the length of certificates and the focus on the review and monitoring processes raise important questions about the Inspector General's role. As noted earlier, the *CSIS Act* does not have much to say about what should happen to reports concerning the review or monitoring processes unless they are instigated by SIRC. The Committee believes that this situation should be clarified.

RECOMMENDATION 74

The Committee recommends that section 30 of the *CSIS Act* be amended so as to make it clear 1) that the primary function of the Inspector General is to establish that the activities of the Service are in compliance with the laws of Canada, ministerial directions, regulations, and operational policies and procedures; 2) that the purpose of the certificate is to indicate compliance or non- compliance by the Service; and 3) that any review conducted under this section be for the purpose of establishing compliance or non-compliance by the Service.

Section 39 of the Act gives the Review Committee access to such information, reports, and explanations in the hands of the Inspector General that "the Committee deems necessary for the performance of its duties and functions." It does not place an obligation on the Inspector General or the Minister or Deputy Minister to forward such reports to the Review Committee. The Committee believes this situation should be rectified.

RECOMMENDATION 75

The Committee recommends that the *CSIS Act* be amended so as to make it obligatory 1) on the part of the Inspector General to forward all reports to the Minister; and 2) for the Solicitor General to forward *all* reports provided by the Inspector General to SIRC.

Obviously, it would not be possible for the Inspector General to fulfil the obligations established by the *CSIS Act* without access to crucial information in the hands of the Service. In general terms, the Inspector General has full access to such information. It should be noted, however, that while section 31(1) entitles the Inspector General to access to "any information under the control of the Service that relates to the performance of the duties and functions of the Inspector General", section 31(2) gives discretion to the

Government of Canada to withhold Cabinet confidences from the Inspector General's purview.

During its review of the access to information and privacy legislation in 1987, the House of Commons Standing Committee on Justice and Solicitor General noted that neither section 69 of the *Access to Information Act* nor section 70 of the *Privacy Act* defined what constituted a Cabinet confidence; both provisions merely listed a number of specific categories of documents that were excluded from access under the legislation.[4] Nor is the *Canada Evidence Act* or the *CSIS Act* more helpful in providing a definition.

Professor Peter Russell, the former Director of Research for the McDonald Commission, described the "sheer arrogance" of the provision regarding Cabinet confidences as "simply numbing".[5] As a result, the Committee was interested in establishing what impact section 31(2) has had on the exercise of the Inspector General's duties and functions. In testimony before the Committee, both the current and the former Inspectors General indicated a degree of uncertainty about whether the provision had impeded their work.[6] In his written response to questions from the Committee Dr. Gosse concluded that:

> While I had broad access to CSIS information during the relatively short period I was Inspector General, I am of the opinion that the Inspector General should have access to the confidences of the Queen's Privy Council of Canada which relate to the operational activities and policies of the Service, and are under the control of the CSIS. To withhold Cabinet documents from the Inspector General could deprive him of the ability to fulfil his functions adequately as it is impossible for the Inspector General to test policies or operational activities related to a directive from Cabinet.

RECOMMENDATION 76

> **The Committee recommends that section 31(2) of the *CSIS Act* be repealed so that the Inspector General has a right of access to all Cabinet documents under the control of the Service.**

Section 31 of the *CSIS Act* goes beyond mere access to "any information under the control of the Service that relates to the duties and functions of the Inspector General." It also places an obligation on the Director and employees of the Service to co-operate fully when requested by the Inspector General to provide "such information, reports and explanations as the Inspector General deems necessary...".

The Committee believes that an important aspect of the Inspector General's job should be to provide the Minister with recommendations stemming from the compliance mandate regarding any needed changes to legislation, ministerial directions, regulations, and policies and procedures.

RECOMMENDATION 77

The Committee recommends that a copy of all recommendations made by the Inspector General to the Solicitor General be forwarded to SIRC.

NOTES

1. Material released under File No. 1336–Sec–87006, entitled "Office of the Inspector General Discussion Paper", Revised April 10, 1984.

2. Testimony before the Standing Committee on Justice and Solicitor General, December 11, 1986.

3. Senate of Canada, Special Committee on the Canadian Security Intelligence Service, *Delicate Balance: A Security Intelligence Service in a Democratic Society*", 1983, p. 29.

4. Canada, House of Commons, Standing Committee on Justice and Solicitor General, *Open and Shut: Enhancing the Right to Know and the Right to Privacy*, 1987, p. 30.

5. Peter H. Russell, "The Proposed Charter for a Civilian Intelligence Agency: An Appraisal", *Canadian Public Policy* XI/3 (1983), p. 336.

6. Canada, House of Commons, Standing Committee on Justice and Solicitor General, *Minutes of Proceedings and Evidence*, Issue No. 4 (December 11, 1986), p. 23.

CHAPTER ELEVEN

Review Mechanisms — The Security Intelligence Review Committee

11.1 Introduction

The Security Intelligence Review Committee (SIRC) performs two key functions. One is to review the performance and activities of the Service. The other is to act as an administrative tribunal to hear and investigate complaints under the *CSIS Act*, the *Immigration Act*, the *Citizenship Act* and the *Canadian Human Rights Act*. The complaints function of SIRC is the subject of a later chapter in this Report. The review process is discussed here.

11.2 Jurisdiction and Membership

When the *CSIS Act* became law in 1984, Canada's security intelligence capacity and its control were the focus of attention. As a result, section 34 of the *CSIS Act*, which established the Security Intelligence Review Committee (SIRC), related to the workings of CSIS alone. The Committee believes that it is now time to adopt a wider control and review framework to apply to other intelligence agencies in addition to CSIS. Because the Committee believes that the Review Committee should not only continue to exist but also have jurisdiction over other agencies, the Committee thinks that the name of the body should now be changed.

RECOMMENDATION 78

The Committee recommends that section 34 of the *CSIS Act* be amended so as to rename SIRC the "Security *and* Intelligence Review Committee".

Currently, this body must consist of a Chairman and not fewer than two or more than four other members. Every member must be a Privy Councillor. None can be a sitting member of the Senate or the House of Commons. While the Committee recognizes that it is advocating an increased workload for SIRC, it is not recommending at this time that the maximum number of members on the Review Committee be increased. The Committee believes that this is properly a decision for SIRC to address once it has a clearer understanding of its workload. The Committee does believe, however, that the minimum number of persons on the Review Committee should be increased.

RECOMMENDATION 79

The Committee recommends that section 34 of the *CSIS Act* be amended to set the membership of SIRC at no fewer than five persons.

To appoint members to SIRC, the Prime Minister must first consult with the Leader of the Official Opposition and the leader of every party having at least twelve members in the House of Commons. The Committee is aware that the process by which the current Chairman of SIRC was appointed caused some public concern. As a result, it believes that the Act should be amended to clarify the appointment process. The Committee believes further that SIRC must not only be a non-partisan body, but that it must also hold the confidence of all Canadians.

The Committee believes that confidence in the appointment process is best obtained where there is discussion between the Prime Minister and the leaders of the other parties in the House of Commons, and where appointees are subject to public scrutiny. The Prime Minister should be fully apprised of the views of the other party leaders in the House before proceeding with these appointments. The Committee believes that it is desirable that the appointments have the support of all parties in the House of Commons. The Committee nevertheless holds that the decision on who will be appointed will rest ultimately with the Prime Minister. Finally, the Committee expects that the practice of calling new members of SIRC before the Standing Committee on Justice and Solicitor General to review their appointments will be continued.

RECOMMENDATION 80

The Committee recommends that section 34 of the *CSIS Act* be amended to require the Prime Minister 1) to notify in writing the leaders of each of the parties with more than twelve seats in the House of Commons that an appointment to SIRC is to be made; 2) to request the leaders of each party so notified to put forward a short list of names of persons they believe to be qualified to be a member of SIRC; and 3) to communicate and discuss with the party leaders in the House so as to be apprised of their views on who should be appointed.

RECOMMENDATION 81

The Committee recommends that the current practice of calling newly appointed SIRC members before the Standing Committee on Justice and Solicitor General be continued.

Currently, section 34(3) allows for the re-appointment of SIRC members for terms not exceeding five years. The Committee believes that the review of security and intelligence matters benefits from experience. It also believes, however, that there is a danger in reviewers becoming too familiar with the agencies and individuals under

review. The Committee therefore believes that the members of SIRC should be eligible to be re-appointed for only one term not exceeding five years.

RECOMMENDATION 82

The Committee recommends that section 34(3) of the *CSIS Act* be amended to provide that the Chairperson and members of SIRC be eligible to be re-appointed for one term not to exceed five years.

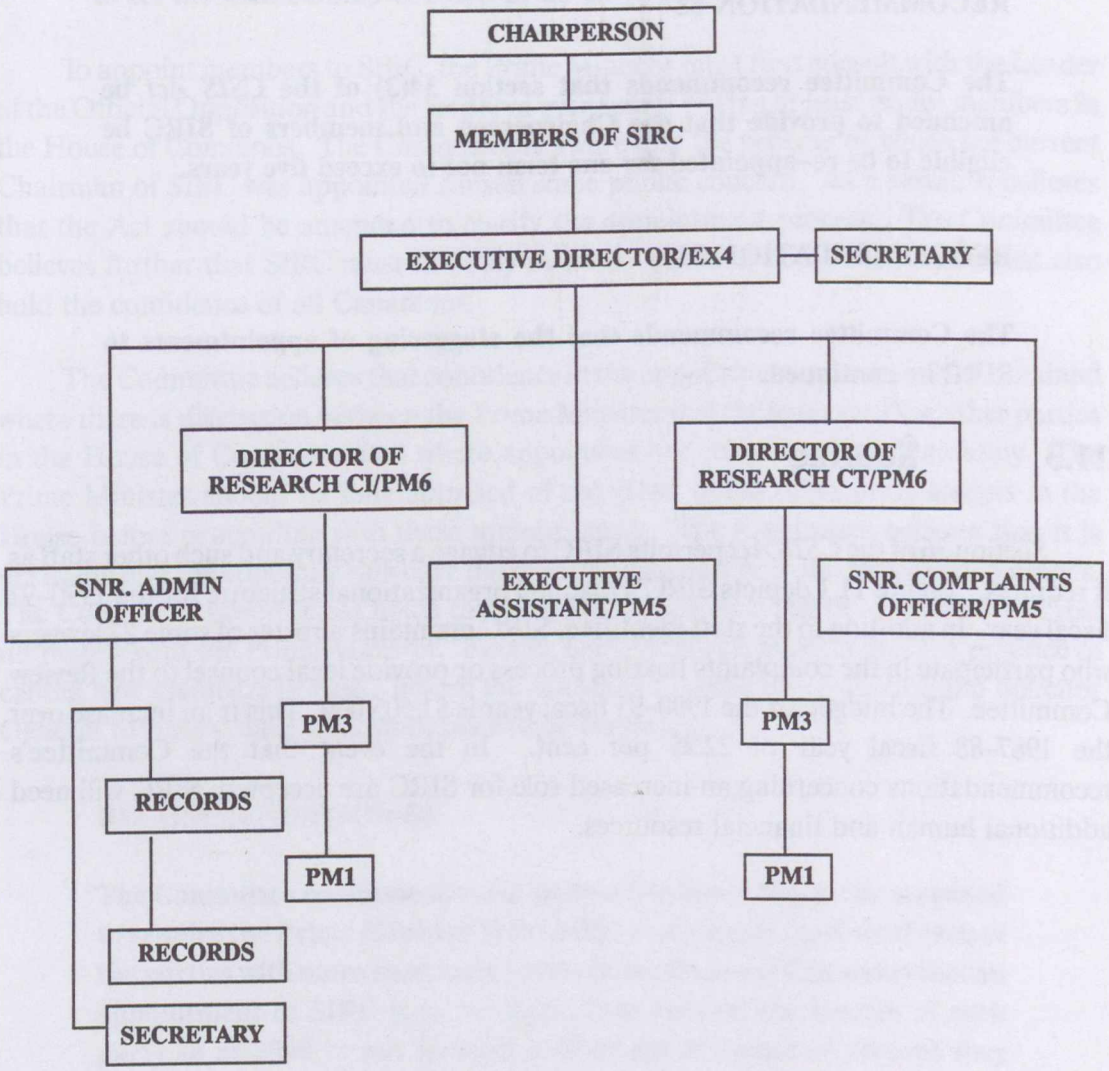
RECOMMENDATION 83

The Committee recommends that the staggering of appointments to SIRC be continued.

11.3 Staffing

Section 36 of the *CSIS Act* permits SIRC to engage a secretary and such other staff as it requires. Figure 11.1 depicts SIRC's planned organizational structure for the 1990–91 fiscal year. In addition to the staff identified, SIRC maintains a roster of some 27 lawyers who participate in the complaints hearing process or provide legal counsel to the Review Committee. The budget for the 1990–91 fiscal year is $1,505,000. This is an increase over the 1987–88 fiscal year of 22.25 per cent. In the event that the Committee's recommendations concerning an increased role for SIRC are accepted, SIRC will need additional human and financial resources.

FIGURE 11.1
STRUCTURE OF SIRC



11.4 Current Functions of SIRC

Sections 38–40 describe the review functions that SIRC is to perform. These are essentially two-fold. Under section 38(*a*), SIRC is to review generally how the Service performs its duties and functions. In particular, SIRC is required to review the Director's reports; the Inspector General's certificates; the Minister's directions; the authorized arrangements that the Service enters into with various governments, their agencies, and international organizations; reports provided to the Attorney General of Canada concerning acts performed by employees of the Service that may be unlawful; and regulations. Section 38(*a*) also allows SIRC to monitor requests from the Minister of National Defence and the Secretary of State for External Affairs for the Service's

assistance in the collection of foreign intelligence within Canada. Finally, SIRC may compile and analyze statistics on the operational activities of the Service.

SIRC has stated that its mandate does not restrict it to reviewing issues related only to propriety. The Review Committee claims that section 38(*a*) also permits it to conduct reviews on whether the Service is operating effectively and efficiently. Others have argued that the section does not allow for such interpretation.

The Committee believes that Parliament intended SIRC's review process to be of wide ambit for a variety of reasons. While it is true that the review and monitoring of effectiveness and efficiency are crucial management tools, such processes have broader ramifications for the accountability and control of the Service. For example, the Committee is aware of incidents in the past when inefficiency led to impropriety. The Committee also believes that by reviewing measures of effectiveness and efficiency, SIRC is able to monitor the state of the Service's organizational culture. This, in the Committee's view, is a critical indicator. Besides suggesting explanations for changes in levels of morale, it can represent a crucial factor in the control of impropriety. Statutes may well define the letter of the law, but it is corporate culture that will determine largely how the spirit of the law is interpreted. The Committee believes, however, that the Act is sufficiently ambiguous as to require clarification.

RECOMMENDATION 84

The Committee recommends that section 38 of the *CSIS Act* be amended so as to make it clear that SIRC has the mandate to monitor and review the effectiveness and efficiency of the Service.

No specific authority is provided by the *CSIS Act* for SIRC to assess the financial performance of the Service. The Committee believes this situation should be rectified. In particular, it believes that SIRC, in co-operation with the Auditor General, should conduct "value for money" audits of the Service, a task that currently falls to the Auditor General alone.

RECOMMENDATION 85

The Committee recommends that the *CSIS Act* be amended to authorize SIRC to undertake financial reviews of the Service in conjunction with the Auditor General.

Section 38(*b*) indicates that the Review Committee has discretion in deciding whether the Service, the Inspector General or SIRC should provide reviews under section 40.

The Committee understands that SIRC continues to operate on the basis that it has, as a result of section 40, a mandate to direct the Inspector General to conduct reviews of

broad scope. The Committee does not agree that this section gives SIRC such broad licence. In the Committee's view, reviews conducted under section 40 should be limited to those that establish whether CSIS has complied with its mandate and has not exercised its powers in an unreasonable or unnecessary manner. Thus SIRC can direct the Service or the Inspector General to conduct reviews only within this limited context.

The Committee recognizes that a limited interpretation of section 40 may cause problems for SIRC. Whereas in the past SIRC apparently has interpreted section 40(*b*) to imply wide discretionary powers to undertake reviews, a narrower interpretation of section 40 would impose a requirement on SIRC to show just cause why it was "inappropriate" for the Inspector General or the Service to conduct reviews under the section. The Committee believes that this limited interpretation should apply and that under normal circumstances SIRC should rely on the Inspector General for reviews of compliance. The Committee also believes that the section should be tightened to encompass reviews for compliance by the Service with the *Canadian Charter of Rights and Freedoms* and generally with the laws of Canada (including provincial laws).

RECOMMENDATION 86

The Committee recommends that section 40 be amended to encompass reviews for compliance by the Service with the *Canadian Charter of Rights and Freedoms* and with the laws of Canada, including provincial laws.

The Committee also thinks that a section of SIRC's annual report should be allotted routinely to describing the compliance function of the Inspector General and the reviews provided by that Office.

11.5 Additional Functions for SIRC

In passing Bill C-9, Parliament hoped to achieve two key goals. First, it wished to establish an accountable civilian security intelligence agency with a statutory mandate in which Canadians could have full confidence. Second, it wanted this new agency to be reviewed by an independent body that would ensure that it stayed within the law. Little thought was given in 1984 to the other members of Canada's security and intelligence community or whether such elements needed similar statutory mandates and review mechanisms.

The Committee believes it is now time to examine the wider dimensions of Canada's security and intelligence community and to impose statutory mandates and review mechanisms where necessary. Several lines of thought underpin the Committee's recommendations in this area.

While the Committee found no evidence of abuse by other agencies, it believes that a number of other collection agencies have a substantial capacity to infringe on the rights and freedoms of Canadians. The capacity of the Communications Security

Establishment (CSE) is a case in point. This organization clearly has the capacity to invade the privacy of Canadians in a variety of ways. It was established by Order in Council, not by statute, and to all intents and purposes is unaccountable. While the Committee understands that this agency must be shrouded in secrecy to some degree, it believes that Canadians should be in a position to understand what the organization does and should not have to wonder whether their rights and freedoms have been infringed. The Committee has evidence that both the RCMP and the Service have asked the CSE for assistance. As such, the Committee believes that the Communications Security Establishment should have a statutory mandate that provides for review and oversight mechanisms for the agency.

RECOMMENDATION 87

The Committee recommends that Parliament 1) formally establish the CSE by statute and 2) establish SIRC as the body responsible for monitoring, reviewing and reporting to Parliament on the activities of the CSE concerning its compliance with the laws of Canada.

In view of the fact that an external review of the Special Investigation Unit of the Canadian Forces is currently in progress, the Committee believes that it would be inappropriate to make specific recommendations regarding security and intelligence units of the Canadian Forces at this time. The Committee sees no reason in principle, however, why the security and intelligence arms of the Department of National Defence should not be reviewed by SIRC.

The Committee recognizes that SIRC is not currently in a position to evaluate adequately particular functions performed by members of Canada's security and intelligence community. For example, the Committee believes that SIRC cannot fully comprehend all the dimensions of the overlap in functions and jurisdiction between CSIS and the RCMP because it cannot look at the subject matter from a police perspective. The Committee believes that the area of overlap, particularly how information produced by CSIS can be transmitted to the RCMP (or other police forces) and converted into evidence, is a critical one that needs greater study. To permit a greater understanding to develop the Committee makes the following recommendation.

RECOMMENDATION 88

The Committee recommends that Parliament establish SIRC as the body responsible for monitoring, reviewing and reporting to Parliament on the activities of those elements of the RCMP that fulfil the Force's security-related responsibilities concerning their compliance with the laws of Canada.

Another instance where SIRC cannot be fully in the picture is administrative security. At present, SIRC is empowered only to review the Service's involvement in the

provision of security assessments. Any comments it makes on the effectiveness of the government's program are likely to be based on partial information. As a result, the Committee is drawn to the conclusion that the time is now right to put the administrative security policy on a firmer footing.

RECOMMENDATION 89

The Committee recommends that the Government Security Policy be replaced by regulations to be adopted by the Governor in Council and to be administered by the Treasury Board.

RECOMMENDATION 90

The Committee recommends 1) that regulations concerning the Government Security Policy (GSP) require the Treasury Board to submit a copy of its reports concerning matters currently identified in the GSP to SIRC at the same time as such reports are submitted to the Cabinet Committee on Security and Intelligence and 2) that SIRC be empowered to request Treasury Board and other departments to supply the Review Committee with such statistical reports as SIRC may consider necessary.

Another set of instances where SIRC is not fully in the picture concerns the gathering of foreign intelligence, the co–ordination and assessment of intelligence generally, and the dissemination of intelligence and the uses to which it is put. The Committee notes that SIRC has made recommendations in the past covering such aspects as 1) an extension of CSIS' foreign intelligence mandate to cover the collection of foreign intelligence outside Canada; and 2) the establishment of an independent intelligence assessment body along the lines of Australia's Office of National Assessments (ONA). While the Committee has already made recommendations concerning the co–ordination, collection, assessment and dissemination of foreign intelligence, it believes some additional comments are warranted concerning SIRC's role in such matters. The Committee believes that SIRC's mandate does not cover the making of recommendations in this area, except in a very peripheral way. Yet the Committee is also aware that no other organization but SIRC is in a position to bring public attention to such matters. For SIRC to do its job better, the Committee believes that the Privy Council Office (PCO) should brief SIRC from time to time concerning the roles performed by the PCO and the various interdepartmental committees on security and intelligence and on such other matters as SIRC may request concerning activities that come under the jurisdiction of the Deputy Clerk, Security and Intelligence, and Counsel.

11.6 The Relationship Between SIRC, The Solicitor General of Canada and Parliament

The Committee believes that Parliament intended that SIRC should perform two critical roles on behalf of Parliament and Canadians generally. On one hand, SIRC has to ensure that CSIS complies with its statutory mandate and does not unreasonably or unnecessarily use its powers to abuse the rights and freedoms of Canadians. On the other hand, it has to monitor the performance of CSIS to see that it operates effectively and efficiently and is successful in maintaining Canada's security. The Committee believes that SIRC should continue to perform these important functions.

To perform these roles, the Committee believes, SIRC must have access to Cabinet confidences that are in the hands of the Service.

RECOMMENDATION 91

The Committee recommends that section 39(3) of the *CSIS Act* be repealed so that SIRC has a right of access to all Cabinet documents under the control of the Service.

When the *CSIS Act* was adopted, Parliament paid little attention to how it would receive information from SIRC beyond the Review Committee's annual reports. In fact, it was not until the Committee tried to get information from SIRC concerning matters relating to the comprehensive review that it recognized there were serious problems in this regard.

Two events illustrate the extent of the problem. First, SIRC had prepared reports concerning the three functions of CSIS' primary mandate counter-intelligence, counter-terrorism, and counter- subversion. The Committee thought that these lengthy reports would be extremely helpful in enabling it to understand how the security intelligence agency discharges its responsibilities. The Committee was denied access to these reports by the Solicitor General and by SIRC. As none of the briefings to the Committee elaborated in any detail on how the key branches of the Service operate and how CSIS has generally performed its duties and functions, the Committee believes that it is no better informed now about such matters than any member of the public would be after reading SIRC's annual reports. More to the point, it has been unable to assess the recommendations made by SIRC concerning improvements that should be made to CSIS' counter-intelligence and counter-terrorism functions, or CSIS' involvement in the protection of science and technology.

Second, when it became clear that SIRC did not agree with the Minister's interpretation of the Review Committee's conclusions regarding its "Report on the Innu Interview and the Native Extremism Investigation", the Committee asked SIRC to provide full details. SIRC refused to do so on the grounds that the Act permitted it to

make reports concerning its reviews in only two ways. Section 53 of the *CSIS Act* requires the Review Committee to report to the Solicitor General by September 30th of each year concerning its activities during the previous fiscal year. In these instances the Minister is obliged to table the annual report in Parliament within 15 sitting days after having received the Report from SIRC.

RECOMMENDATION 92

The Committee recommends that section 53 of the *CSIS Act* be amended so as to require 1) SIRC to submit its annual report direct to the Speaker of each House of Parliament by September 30th of each year and 2) the Speaker of each House to table the annual report in Parliament within 15 sitting days after having received it.

Because SIRC is currently charged with crucial roles in the overall scheme of accountability and control and is in many respects Parliament's surrogate, the Committee decided that the manner in which SIRC conducts reviews and processes complaints should be subjected to the most detailed and careful analysis possible. In particular, the Committee believed that it had to be able to assure itself that SIRC's research techniques were effective and that there was no indication of the Review Committee having been captured by either the executive branch of government or by the intelligence community. Furthermore, the Committee considered that it had to have hard evidence for this. It could not simply take SIRC's word for it.

To understand SIRC's role the Committee received *in camera* briefings from the Review Committee and from its staff. To resolve particular issues, Committee staff met with representatives of SIRC on several occasions. To obtain a balanced picture of how well SIRC functioned as a review body, Committee staff interviewed current and former staff members.

To develop a picture of the type of work SIRC had chosen to perform, the Committee asked for a list of all reports completed for or by SIRC since 1984. During the five-year period, SIRC directed the Inspector General to provide four reports under section 40 of the *CSIS Act*. Apparently it neither asked the Service to provide any section 40 reports nor conducted any itself. By the end of 1989, SIRC had prepared five Annual Reports and had forwarded 15 section 54 reports to the Minister, three of which were based either in whole or in part on section 40 reports provided by the Inspector General. In addition, SIRC itself prepared three reports that were neither section 54 nor section 40 reports. The following are the reports SIRC identified to the Committee.

LIST OF SIRC REPORTS

A. ANNUAL REPORTS:

1984–85
1985–86
1986–87
1987–88
1988–89

B. SECTION 54 REPORTS: (* = also Section 40 Report)

"18 Months After Separation: An Assessment of CSIS' Approach to Staffing, Training and Related Issues," April, 1986 (139 pages/SECRET).

"Report on a Review of Security Screening for Applicants and Employees of the Federal Public Service," May, 1986 (SECRET).*

"Ottawa Airport Security Alert," March, 1987.

"Closing the Gap: Official Languages and Staff Relations in the CSIS," June, 1987 (60 pages/ PUBLIC VERSION).

"SIRC Report on Immigration Screening," January 1988 (32 pages/SECRET) *

"SIRC Report on Immigration Screening," January 1988. Supplement to report November, 1989.

"Report to the Solicitor General of Canada on CSIS's Use of Its Investigative Powers with Respect to the Labour Movement," March, 1988 (18 pages/PUBLIC VERSION).

"The Intelligence Assessment Branch: A SIRC Review of the Production Process," September, 1988. (80+ pages/SECRET).

"SIRC Review of the Counter-Terrorism Program in the CSIS," November, 1988 (300+ pages/TOP SECRET).

"Report to the Solicitor General of Canada on Protecting Scientific and Technological Assets in Canada: The Role of CSIS," April, 1989 (35–40 pages/SECRET).

"Report to the Solicitor General of Canada Concerning CSIS' Performance of its Functions," May 1989.

"SIRC Report on CSIS Activities Regarding the Canadian Peace Movement," June, 1989 (540 pages/SECRET).

"A Review of CSIS Policy and Practices Relating to Unauthorized Disclosures of Classified Information," August, 1989 (SECRET).*

"Report to the Solicitor General of Canada on Citizenship/Third Party Information," October, 1989.

"A Review of the Counter-Intelligence Program in the CSIS," October, 1989 (700 pages).

"Report on the Innu Interview and Native Extremism Investigation," November, 1989.

C. OTHER REPORTS:

"The Security and Intelligence Network in the Government of Canada: A Description," January, 1987 (61 pages/SECRET).

"Counter-Subversion," August, 1987. (350 pages/SECRET).

"Amending the CSIS Act: Proposals for the Special Committee of the House of Commons 1989," September 1989.

Besides its annual reports, SIRC prepared reports for public consumption on its reviews of official languages and staff relations and of CSIS's investigation of the labour movement. In the case of its reviews of staffing and training, immigration screening, and the Innu interview and native extremism investigation, censored versions of the reports were released under the *Access to Information Act*.

In what the Committee believed to be one of the most crucial elements of its comprehensive review, namely an evaluation of all reports prepared by SIRC, it came across insurmountable roadblocks. SIRC informed the Committee that it believed it would be in contravention of the *CSIS Act* if it released any of its reports to the Committee. Members of the Committee could not help but note the irony of the remarks of SIRC's new Chairman when he later appeared before the Standing Committee on Justice and Solicitor General, which was considering SIRC's Main Estimates:

> Finally, Mr. Chairman, I would like to assure you and the members of your Committee my colleagues and I continue to believe that in much of what we do, particularly our work reviewing CSIS operational activities, we act on your behalf. We will continue to examine CSIS activities thoroughly and to try both to ask CSIS the questions you would want us to ask and to answer the questions you put to us as completely and openly as possible.[1]

When the Committee approached the Solicitor General for access to SIRC's reports it was also unsuccessful.

The Committee has come to the following general conclusions. Regarding SIRC's annual reports, it has observed that the earlier ones are much more critical of the Service than the later ones. One conclusion, and it may be the right one, is that there is less to be

critical about. However, less charitable conclusions can also be drawn. The Committee does not believe that it has been able to go behind the annual reports to an adequate degree to draw any conclusions on this score.

Second, too few of SIRC's special reports were available to the Committee for it to draw any conclusions about section 54 reports as a whole. The Committee found the expurgated version of the report entitled "Eighteen Months After Separation: An Assessment of CSIS' Approach to Recruitment, Training and Related Issues", dated April 14, 1986, and the subsequent report entitled "Closing the Gaps: Official Languages and Staff Relations in the Canadian Security Intelligence Service", dated June 1987, well researched, informative, thorough, and, as far as the Committee could tell, fair-minded and useful.

As with "Closing the Gaps" SIRC's "Section 54 Report to the Solicitor General of Canada on CSIS's Use of its Investigative Powers with Respect to the Labour Movement" (the "Boivin Affair") dated March 25th, 1988, was written specifically with a view to its being made public by the Solicitor General of Canada. It was based substantially on information provided by the Inspector General on direction by SIRC under section 40(*a*). Because the Committee was prevented from having access to the original material provided by the Inspector General, the Committee can make no assessment of SIRC's contribution to the analysis presented in its report. It can say, however, that the effect of the interim report provided by the Inspector General to the Solicitor General was sufficient to cause the Solicitor General to issue instructions to the Director concerning the development of a policy on the retention and destruction of files and on the use of human sources like Mr. Boivin.

Among its conclusions on the Boivin Affair SIRC stated that:

> CSIS' tardy response to Mr. Boivin's startling disclosures on Saturday May 30, 1987 that specific and serious criminal offences might be imminent not only breached CSIS policy but also ordinary standards of common sense.[2]

No mention of this matter was made in SIRC's written response to requests for information by the Committee concerning possible unlawful acts on the part of Service employees. This is indeed interesting in view of the fact that the Director of CSIS responded to the same question by indicating that:

> In 1987, a CSIS source contacted his handler and advised that he was in possession of dynamite fuses. The potential unlawful activity of concern in the case is in respect to the advice that the handler gave the source.

SIRC's expurgated report on "Immigration Screening Activities of the Canadian Security Intelligence Service", dated January 1988, has too much excised from it for the Committee to make a useful comment.

It is SIRC's most recent report, concerning the so-called "Innu interview", that has given the Committee greatest cause for concern. This stemmed not only from the nature

of the report—what it said and what it left unsaid, as well as the research techniques that appear to have been used—but also what the report caused members of the Review Committee to say about the comments made by the Solicitor General when he released the report and about SIRC's relationship to Parliament.

In the Committee's view, the report does not complete what its terms of reference promised initially. As a result, the report leaves many questions unanswered. There may be extenuating circumstances for this. The out-going Chairman of SIRC may have required the report to be submitted to the Minister before his term of office expired and this may have pressured staff to report before they had completed all of the planned dimensions of the investigation. Certainly, the report does not possess the carefully measured prose that is characteristic of many SIRC reports.

More worrisome is the fact that it became clear to the Committee during SIRC's testimony before the Standing Committee on Justice and Solicitor General (regarding the Review Committee's Main Estimates) that SIRC was at odds with the interpretation put on the report by the Solicitor General. Because SIRC had not indicated publicly that it disagreed with the Solicitor General's characterization, a member of the Standing Committee claimed that it raised "serious questions of confidence" in SIRC. The Committee understands that the Review Committee will have more to say on this matter in its next annual report.

The Committee is of the view that two aspects of the current arrangement by which CSIS is accountable to Parliament need to be improved. One concerns SIRC's reporting relationship. The other concerns its relationship to Parliament. While the Committee agrees that the Solicitor General should be able to request SIRC to conduct certain reviews, and that reports subsequent to such reviews should be made public only at the discretion of the Minister, the Committee believes it is quite inappropriate for SIRC to submit either its annual reports or the special reports it initiates to the Solicitor General.

Section 54 gives SIRC discretion to furnish the Minister with a report at any time on any matter that relates to the performance of its duties and functions. Under this section, the Minister has no obligation to advise Parliament of the report's contents. Nor can SIRC speak openly about any public comments that the Solicitor General may make. The Committee believes this situation is in need of correction and that SIRC should have the same powers in reporting to Parliament as the Privacy Commissioner and the Information Commissioner have.

RECOMMENDATION 93

The Committee recommends that section 54 of the *CSIS Act* be amended so as to permit SIRC to submit special reports to the Speakers of both Houses at any time for tabling in Parliament.

The Committee is also of the view that SIRC's independence should be made clearer in another way. The Committee considers that the obligations placed on SIRC by section

55 of the *CSIS Act* are prudent ones. They require SIRC to consult with the Director of CSIS before releasing certain statements and reports to avoid SIRC releasing information that would pose a threat to national security. The Committee understands that SIRC and the Director have interpreted the meaning of section 55 differently. It is the Committee's view that the section was included to provide SIRC with a resource that could quickly identify whether particular information might be sensitive in terms of national security. The Committee believes that it was not Parliament's intention to imply that the Director should be allowed to determine what should or should not go into any report or statement issued by SIRC. The Committee believes that to be SIRC's right. Obviously, however, there is a fine line here. In the Committee's view, SIRC should pay careful attention to any recommendation coming from the Director concerning the need to delete sections of statements or reports on national security grounds. Nevertheless, the Committee is firm in the view that where there is a genuine difference of opinion, the Review Committee's determination should be conclusive.

RECOMMENDATION 94

The Committee recommends that section 55 of the *CSIS Act* be amended to provide that before determining the content of a statement or report described in that section, SIRC shall consult with the Director of CSIS to ensure compliance with section 37, and that the Review Committee's determination in this regard shall be conclusive.

NOTES

1. Canada, House of Commons, *Minutes of Proceedings and Evidence of the Standing Committee on Justice and Solicitor General*, Issue No. 29 (April 10, 1990), p. 5.

2. Security Intelligence Review Committee, "Section 54 Report to the Solicitor General of Canada on CSIS's Use of its Investigative Powers with Respect to the Labour Movement", 1988, p. 13.

CHAPTER TWELVE

The Complaints Process — The Security Intelligence Review Committee

12.1 Introduction

In this chapter, the Committee considers the role of the Security Intelligence Review Committee (SIRC) in the complaints process. In this regard, the statutory and procedural rules followed by the Review Committee are reviewed, as are some of the problems identified in the complaints process itself.

To undertake its study of the Security Intelligence Review Committee complaints process, the Committee reviewed the pertinent legal and social science literature and contacted a number of persons who had experience either working for or appearing before SIRC. In addition, the Committee sought the views of complainants and counsel by way of a questionnaire that was forwarded to them by the Review Committee. A number of those identified from the questionnaire were contacted and, in some cases, more in-depth case studies were undertaken where certain problem areas were identified. The Committee also heard testimony regarding the role of SIRC and the complaints process during its public hearings and received confidential briefs.

The initial recommendation for establishing an administrative tribunal with responsibility for hearing complaints against the security service was proposed by the McDonald Commission in 1981. The Commission recommended that a Security Appeals Tribunal hear security appeals in the areas of "Public Service employment, immigration, and citizenship." It also recommended that:

a) the Security Appeals Tribunal consist of five members appointed by the Governor in Council, any three of whom could compose a panel to hear security appeals;

b) the Chairman of the Tribunal be a Federal Court Judge;

c) the other members not be currently employed by a federal government department or agency.[1]

Many of the McDonald Commission recommendations appear to have guided Parliament in the establishment of Canada's first security appeals tribunal known as the Security Intelligence Review Committee.

12.2 The Review Committee's Functions

In addition to providing the external review function for the Canadian Security Intelligence Service (CSIS), the Review Committee also acts as a tribunal to consider various types of complaints and to provide reports on its findings to the Solicitor General. As a tribunal it investigates and makes recommendations about complaints made against the Service (section 41 complaints), as well as security clearance denials involving the federal government (section 42 complaints). SIRC is also required to conduct investigations in relation to reports made pursuant to section 19 of the *Citizenship Act* or sections 39 and 81 of the *Immigration Act* and matters referred to it pursuant to section 45 of the *Canadian Human Rights Act*.[2]

In its tribunal function, SIRC employs "Rules of Procedure" adopted in March 1985. These Rules were developed to provide more detailed procedural guidance in relation to the Review Committee's functions under section 38(*c*) of the *CSIS Act*.

12.3 Making a Complaint – Expanding SIRC's Jurisdiction

12.3.1 *Section 41 Complaints*

Section 41 of the *CSIS Act* reads:

> 41. (1) Any person may make a complaint to the Review Committee with respect to any act or thing done by the Service and the Committee shall, subject to subsection (2), investigate the complaint if:
>
> (*a*) the complainant has made a complaint to the Director with respect to that act or thing and the complainant has not received a response within such period of time as the Committee considers reasonable or is dissatisfied with the response given; and
>
> (*b*) the Committee is satisfied that the complaint is not trivial, frivolous, vexatious or made in bad faith.
>
> (2) The Review Committee shall not investigate a complaint in respect of which the complainant is entitled to seek redress by means of a grievance procedure established pursuant to this Act or the *Public Service Staff Relations Act* 1984, c.21, s.41.

Only regarding complaints against the Service is there an obligation on the complainant to direct his or her complaint to the Director of CSIS. The Review Committee cannot investigate such a complaint until a complainant has received a reply from the Director of the Service or until such time has passed that the Review Committee

considers it reasonable for the Director to have made a reply. Under the provisions of the *CSIS Act* addressing complaints relating to a denial of a security clearance or investigations under the *Immigration Act*, the *Citizenship Act* or the *Canadian Human Rights Act*, there is no requirement that the person concerned must first make a complaint to the Director of the Service.

The Committee believes that the requirement to notify the Director under section 41 of the Act is unnecessary. It believes that a person may feel intimidated or be deterred from making such a complaint if he or she is required to contact the Director of the Service. This would likely be the case for anyone who is making allegations of wrongdoing against the Service, especially persons employed by CSIS itself. The Committee is also concerned that the complaints process may be delayed because of this requirement. Indeed, the Committee has learned that on occasion complainants have had to wait several weeks after sending an initial letter of complaint before receiving a reply from the Director of the Service.

The current process serves no purpose other than to notify the Director of CSIS that a complaint has been made and to allow the Director to make the initial reply to a complainant. The Committee understands that the first Director of the Service believed the current requirement to notify the Director was "ill conceived from the start". The Committee also believes that complaints may not actually be seen or dealt with by the Director.

RECOMMENDATION 95

The Committee recommends that paragraph 41(1)(*a*) of the *CSIS Act* be amended to allow complainants to address their concerns directly to SIRC and to give SIRC discretion to advise the Director of CSIS that a complaint has been made.

Further, the Committee believes that SIRC, as an independent investigatory body, should be able to initiate complaints on its own. For example, if, during the course of a SIRC investigation of a complaint, cause for a further complaint arises (such as if CSIS is late in responding to a request for information or documents), the Review Committee should be able to initiate its own complaint against the Service. On this point, it is noteworthy that under the *Royal Canadian Mounted Police Act* the Chairman of the RCMP Public Complaints Commission can initiate complaints where he or she is satisfied that there are reasonable grounds to do so.[3]

RECOMMENDATION 96

The Committee recommends that the *CSIS Act* be amended to permit SIRC to initiate its own complaints against the Service.

12.3.2 *Section 42 Complaints—Undue Delay*

Section 42 complaints relate to the denial of a security clearance where an individual seeks or wishes to maintain employment with the federal government.

The Committee has learned that, in certain circumstances, the completion of a security assessment investigation by the Service has taken a long time. A person faced with a delay in having his or her security assessment completed by the Service is severely prejudiced by being unable to work with the government while the necessary inquiries are under way. Persons who find themselves in such a situation should be able to seek recourse through SIRC.

The Director of CSIS, during testimony before the Standing Committee on Justice and Solicitor General, indicated that security clearances for level one and level two assessments take approximately three months to complete, while anyone requiring a top-secret clearance must wait some six or seven months before the clearance is completed. It is the hope of the current Director of the Service that a thirty- day turn-around time for security assessments could be made a realistic goal for the future.[4]

The Committee recognizes that the Service is making significant headway in reducing the length of time required for security assessment investigations and that many of the causes of delay lie outside the Service's control. Nevertheless, the Committee believes that a person who is the subject of a security assessment investigation should be able to make a complaint to the Review Committee where there is undue delay. The Committee believes that a person who has not had his or her security assessment investigation completed by the Service within a reasonable period should, as of right, be able to make such a complaint to SIRC.

RECOMMENDATION 97

The Committee recommends that section 42 of the *CSIS Act* be amended to allow the Review Committee to receive and investigate a complaint from any individual who, by reason of failure of the Service to complete a security assessment within a reasonable period after a request is received by the Service, is denied employment or is dismissed, demoted, or transferred or denied promotion or transfer, or is denied a contract to provide goods or services to the Government of Canada.

RECOMMENDATION 98

The Committee recommends that if the delay by CSIS in providing a security assessment amounts to constructive denial of employment to the complainant, then SIRC may forward a recommendation to a deputy head under section 52 of the *CSIS Act* and that recommendation shall have binding effect upon the deputy head concerned.

12.3.3 *Section 42 Complaints—Who Has a Right to Make a Complaint*

As noted by the Review Committee in its brief to the Committee:

> There should not be categories of Canadians or landed immigrants who do not have the right to complain to SIRC when they are denied a security clearance, while others have the right to a full investigation by the Committee. It is a fact of life in the modern world that the denial of a security clearance usually has a long term effect on the individual's employment potential. In any event ... no Canadian or landed immigrant should be put in the position of having his or her loyalty questioned to such an extent that a security clearance is refused without having an automatic right to request an investigation by the Review Committee.[5]

The Review Committee has recommended that section 42(1) and (2) of the *CSIS Act* be repealed and replaced by the following provision:

> 42. (1) When a security clearance, required by the Government of Canada for an individual for any purpose, is denied or is granted at a lower level than that required or is downgraded to a lower level than that required, the deputy head or other person making that decision shall send, within ten days after the decision is made, a notice informing the individual of the denial of a security clearance at the required level, and of the individual's right under this section to complain to the Security Intelligence Review Committee.

The remainder of section 42 would require minor consequential amendments.[6]

The Committee supports the recommendation of the Review Committee regarding the right of any Canadian or landed immigrant to complain to SIRC when denied a security clearance. The Committee is aware that at times SIRC has been unable to deal with *bona fide* complaints as a result of the denial of a security clearance because it lacked jurisdiction. For example, the Review Committee is unable to hear a section 42 complaint unless the person concerned was the subject of a decision by a deputy head to "deny employment ... or to dismiss, demote or transfer an individual or to deny a promotion or transfer [or] to deny ... a contract to provide goods or services to the Government of Canada."

As SIRC has generally followed a narrow interpretation of this provision, many complainants have been left without a forum in which to bring a complaint regarding the denial of a security clearance. The limitation thus proves to be ultimately unfair to persons who may have enjoyed long service with the federal government, but because of a technical shortfall in the Act, SIRC finds itself without authority to address their complaints.

The Committee proposes that SIRC's recommendation on this issue be accepted in its entirety.

RECOMMENDATION 99

The Committee recommends that section 42(1) and (2) of the *CSIS Act* be repealed and replaced by:

42.(1) When a security clearance, required by the Government of Canada for an individual for any purpose, is denied or is granted at a lower level than that required or is downgraded to a lower level than that required, the deputy head or other person making that decision shall send, within ten days after the decision is made, a notice informing the individual of the denial of a security clearance at the required level, and of the individual's right under this section to complain to the Security Intelligence Review Committee.

12.3.4 *Investigations Concerning Immigration*

A matter that came to the attention of the Committee has to do with persons who may be subject to decisions by the Canada Employment and Immigration Commission (CEIC) for their removal from Canada, although they are not the subject of a report pursuant to sections 39 and 81 of the *Immigration Act*. The situation appears to arise in the following circumstances.

As noted by SIRC in its report of January 1988, entitled "Immigration Screening Activities of the Canadian Security Intelligence Service", which was prepared in response to recommendations concerning immigration screening activity in the Ninth Report of the House of Commons Standing Committee on Labour, Employment and Immigration,

> In cases where an applicant is not clearly within the security-related inadmissible classes of subsection 19(1) of the *Immigration Act*, but where a "suspicion" nonetheless exists, CSIS will prepare and forward to CEIC an "information brief", which simply advises the Canada Employment and Immigration Commission (CEIC) of its suspicions without making a recommendation for denial of the application. Where, however, CSIS considers an applicant to be within one or more of the security-related inadmissible classes of subsection 19(1), CSIS will prepare and forward a "rejection brief" which particularizes the evidence against the applicant and contains a recommendation for denial of his application to immigrate. As a general rule, CEIC has not admitted applicants who have been the subject of information or rejection briefs.[7]

It is of concern to the Committee that the use of the "information" and "rejection" briefs from the Service allows the CEIC to circumvent the investigation process contemplated under section 38(*c*) of the *CSIS Act*. In one case reviewed by Committee staff, a person who was in Canada on a Minister's Permit received notice from CEIC that

he had to leave Canada or face deportation. The letter from CEIC did not specify the reasons for this decision. It was only after the person made enquiries of SIRC, which in turn made enquiries of CSIS, that it was determined that the reason behind the CEIC decision was based on a CSIS report.

The Committee believes that this practice has the effect of frustrating the process established under the *Immigration Act* to allow individuals who are the subject of a security certificate to make representations before SIRC in support of their case.

The Committee considers that the *Immigration Act* should be amended to allow any person who is the subject of an adverse decision by the CEIC, that relates in whole or in part to a security report obtained from CSIS, to have his or her case referred to SIRC so that the Review Committee may pursue an investigation as contemplated under the current provisions of sections 39 and 81 of the *Immigration Act*. The Committee also believes that any person who is the subject of an adverse decision by the CEIC, relating in whole or in part to a security report obtained from CSIS, should be advised that he or she has a right to make a complaint to the Review Committee.

12.4 The Complaints Process – Procedural Matters

The Committee learned of a number of other matters regarding the complaints process: although they do not give rise to specific recommendations, they certainly warrant mention. The Committee believes that the Review Committee should consider the following issues at an early opportunity, with a view to revising its Rules of Procedure and complaints process.

12.4.1 *Hearing Complaints and Dissenting Opinions*

Under various provisions of the Review Committee's Rules of Procedure relating to complaints under sections 41 and 42 of the *CSIS Act* or reports under the related provisions of the *Immigration Act*, the *Citizenship Act* and the *Canadian Human Rights Act*, the Chairman of the Review Committee is to assign one or more members of SIRC to hear a complaint or to investigate a report. It is apparent that in many cases only two SIRC members have sat during the hearing of a matter.

The McDonald Commission recommended that its equivalent of SIRC consist of five members, "any three of whom could compose a panel to hear security appeals".[8] It is of concern to the Committee that with an even number of SIRC members sitting on a case, a situation may arise where a stalemate occurs and the panel may be unable to reach a conclusion. The Committee received evidence in the responses to its questionnaire that suggests that two-person panels may lead to a "lowest common denominator" type of thinking more often than if panels were composed of three members.

It was also suggested by a number of legal counsel contacted by Committee staff that in cases where one member has a dissenting opinion regarding a case, the dissent should

be published as part of the report of findings released to the complainant. There is no reason to presume that a situation might not present itself, if it has not already, where a SIRC member feels that his or her dissenting opinion should be made known to the person concerned. In this regard, although the Committee is unaware of such a situation having occurred to date, provision should be made to allow for dissenting opinions to be reported to a complainant or the person affected by the SIRC recommendation.

12.4.2 *Addressing Multiple Complaints*

It is the Committee's understanding that if SIRC is seized with an initial complaint by an individual, any subsequent conduct of CSIS that gives rise to a further complaint may be regarded as a "new complaint". This matter was brought to the Committee's attention by an individual who had made a number of complaints to the Review Committee. For example, a person who has made an initial complaint under section 41 of the *CSIS Act* and subsequently wishes to make a second complaint arising out of the same set of circumstances may be obliged, under the current regime, to repeat the process of contacting the Director of the Service, awaiting a reply, then contacting the Review Committee. This discussion will be moot, of course, if Recommendation 95, made earlier in this chapter, is implemented.

The Committee believes that the most efficient way to conduct a review of more than one complaint is to consider related complaints *in toto* rather than as separate and distinct entities. SIRC should "join" multiple complaints arising out of the same set of circumstances. This would expedite the complaints process and facilitate the work of SIRC in addressing related complaints as part of one investigation or hearing.

12.4.3 *Informing Complainants of the Progress of their Complaints*

SIRC makes its best efforts to keep individuals advised of the status of their complaints or related investigations. For persons not represented by legal counsel, however, there is an added burden on the Review Committee, or its counsel, to keep them apprised of the status of their cases. Despite the best intentions of the Review Committee, there have been instances where complainants were not kept adequately advised of the progress of their cases. It cannot be said that SIRC was solely at fault for these occurrences, as any number of factors could explain why a complaint was delayed and why a complainant was not advised of its progress.

Nonetheless, SIRC should attempt to clarify to complainants the various stages through which a complaint must pass, and thereafter to inform complainants as to the stage their complaint has reached.

12.4.4 *A Complainant's Right to Make Representations*

The Committee is aware that some complaints heard by SIRC have been dealt with in the absence of a full opportunity for the person concerned to make representations to

the Review Committee. There is some concern that this practice may result in SIRC making decisions without having heard the full views and evidence of the person involved.

Since SIRC attempts to act as a quasi-judicial body, due attention should be paid to allowing complainants to make full representations before it. Indeed, to limit complainants' representations before the Review Committee may offend natural justice or *Charter* rights.

12.4.5 *Providing Reasons for Objections or a Refusal to Exercise Certain Powers*

Section 50 of the *CSIS Act* provides SIRC with the following powers in relation to the investigation of any complaint:

> 50. The Review Committee has, in relation to the investigation of any complaint under this Part, power
>
> (*a*) to summon and enforce the appearance of persons before the Committee and to compel them to give oral or written evidence on oath and to produce such documents and things as the Committee deems requisite to the full investigation and consideration of the complaint in the same manner and to the same extent as a superior court of record;
>
> (*b*) to administer oaths; and
>
> (*c*) to receive and accept such evidence and other information, whether on oath or by affidavit or otherwise, as the Committee sees fit, whether or not that evidence or information is or would be admissible in court of law.

This provision would appear to give a person subject to a hearing before SIRC, or SIRC itself, the ability to bring a witness before the Review Committee. It is somewhat surprising, then, that the summons provisions in the *CSIS Act* have been used on only one occasion.[9] Although a summons was issued by the Review Committee, it appears that it was not served on the witness. One reason for the apparent lack of use of these summons powers was that most witnesses appeared before the Review Committee of their own volition.

On some occasions, counsel for complainants have requested that a witness be summoned by the Review Committee, but SIRC has refused to exercise its powers in this regard. What is of concern here is that SIRC has not provided reasons for its refusal to issue a summons. The Committee believes SIRC should accept submissions from counsel when considering a request and provide reasons for any refusal to issue a summons.

Legal counsel contacted by Committee staff raised a similar concern with respect to upholding objections. For example, if counsel for CSIS objects to a witness answering certain questions, it appears that the presiding members of SIRC uphold the objection without hearing submissions from counsel or providing reasons for the decision. There is a concern that such a practice may offend a person's natural justice or *Charter* rights. An appropriate procedural remedy for this issue would be to allow counsel to make submissions regarding an objection and, if warranted, SIRC should provide written reasons on any matter of procedural import dealt with in its decision. Of course, this suggestion would also apply to the upholding by SIRC of a complainant's objection.

12.4.6 *Reporting SIRC Decisions*

The Committee believes the case summaries provided in SIRC's annual reports can be improved. The current summaries provide only the most cursory review of a complaint. There is no description of the type of evidence heard, the issues raised or the various legal authorities, if any, that were relied upon by SIRC members in reaching their decisions. Most important, because the summaries do not provide the "reasons" for the decision in each case, their precedent value is negligible.

As more cases are heard by SIRC, there will be a greater need to develop a body of jurisprudence that can be relied upon by complainants or counsel participating in hearings. Maintaining the privacy of an individual who has had a case decided by the Review Committee is of paramount importance. Nevertheless, there are examples of case reports being made public that provide adequate protection to the person concerned. Comprehensive and useful jurisprudence has developed, for example, in cases involving young offenders under the *Young Offenders Act* and injured workers before various provincial bodies. This case law has developed without compromising the identity of the persons concerned. The Committee believes that similar developments could, and should, take place in regard to matters heard before SIRC.

The Committee suggests that SIRC consider developing a form of jurisprudence to be reported in its annual reports, or in some other appropriate format, and that it include the following information:

- type of matter heard;
- panel members hearing matter;
- numbers of witnesses and exhibits;
- types of evidence heard;
- procedural rulings;
- statutes, regulations, policies cited;
- case law cited;
- terms interpreted.

12.5 The Role of Legal Counsel

The role of legal counsel during the complaints process is of great importance to a complainant or a person who is the subject of an adverse security report. SIRC maintains a list of twenty-four male and three female lawyers from across the country to act as "Committee counsel"; all of these counsel have obtained a Level III (Top Secret) security clearance. It has been the practice of the Review Committee to engage security-cleared counsel when required during the investigatory and hearings processes. These counsel take on the role of devil's advocate during *in camera* proceedings. This process has been established to allow security-sensitive evidence to be brought before the Review Committee in the absence of the complainant and his or her counsel.

Committee counsel may cross-examine witnesses on behalf of an absent complainant. SIRC is also empowered to provide summaries of the evidence heard *in camera* and Committee counsel play an important role in the negotiating process prior to the disclosure of this information to a complainant.

Legal counsel who have represented individuals before the Review Committee have expressed concerns about the role of "Committee counsel". In brief, they are unable to determine whether Committee counsel represent their clients' interests adequately during *in camera* proceedings. In addition, many counsel have indicated to Committee staff that they were not satisfied with the overall disclosure of information provided during SIRC hearings, in some cases to the point that they were significantly handicapped in preparing for the case. It appears that SIRC counsel is unable to disclose to a complainant and counsel what kind of questions were asked or the issues and evidence discussed in the absence of the parties. What can be disclosed to a complainant and counsel is a summary of the evidence, subject to an agreement as to its contents negotiated between SIRC counsel and CSIS.

Despite the best efforts of the Review Committee and SIRC counsel, this process is flawed. Not only do complainants have to trust a total stranger to represent their interests, but several legal counsel have indicated to the Committee that the disclosure provided in the summaries of evidence is often inadequate for the purposes of understanding or preparing for the case being presented.

12.5.1 *The Impact of the Chiarelli Decision*

Before setting out the Committee's suggestions, it is important to look at the Federal Court of Appeal case of *Chiarelli v. Minister of Employment and Immigration*.[10] Mr. Chiarelli was alleged to have been involved in organized crime in Canada. In February 1987 the Solicitor General and the Minister of Employment and Immigration made a joint report to SIRC under former sections 82.1 and 83 of the *Immigration Act* (now sections 81 and 82), stating that there were reasonable grounds to believe that Mr. Chiarelli was a person who would engage in organized crime.

Under the provisions of the *Immigration Act*, Mr. Chiarelli was entitled to an investigation conducted by SIRC and to make representations to it. SIRC undertook its investigation during the summer of 1987 and held a hearing in September of that year. During a subsequent hearing before the Review Committee, Mr. Chiarelli and his counsel were not allowed to attend while the RCMP presented its evidence. Mr. Chiarelli was provided with summaries of the evidence heard *in camera*, although the attending SIRC member indicated that he was unhappy with the procedures imposed upon the Review Committee by the Act.

In October 1987, SIRC told Mr. Chiarelli it had sent the Governor in Council a report supporting the original report by the Solicitor General and the Minister of Employment and Immigration. The report recommended that a certificate be issued under section 83 of the *Immigration Act*. When a certificate is filed under section 83, the Immigration Appeal Board is required to dismiss an appeal that is based on humanitarian and compassionate grounds. Mr. Chiarelli's counsel gave notice, however, that he intended to raise constitutional questions about the procedure. The Immigration Appeal Board, in turn, referred a number of constitutional questions to the Federal Court of Appeal for its consideration.

All three members of the Federal Court of Appeal panel concluded that the process for issuing the section 83 certificate had infringed Mr. Chiarelli's *Charter* rights "because the procedure followed by the Security Intelligence Review Committee did not meet the requirements of that section."[11] Where the judges differed, however, was with respect to whether the infringement could be upheld as a reasonable limit under section 1 of the *Charter*.

Mr. Justice Stone, for the majority, stated that the hearings process before SIRC failed to balance the state's interest in protecting police sources with the individual's right to fundamental justice. On the contrary, Mr. Justice Stone noted that the offending provision:

> ... opts for a complete obliteration of the individual's rights in favour of the State's interest. The provision could have achieved its objectives while infringing the appellant's rights far less severely than it has done by providing a balancing mechanism rather than a total denial of the appellant's rights. Accordingly, the provision does not "impair as little as possible" the rights of the appellant.[12]

Mr. Justice Stone also recognized that:

> there may well be circumstances where disclosure of information is unavoidably necessary to establish the innocence of the person against whom the allegations have been made, and in such circumstances the infringement of the right in question, in my view, would be out of proportion to the objective sought to be achieved.[13]

Mr. Justice Stone concluded that section 82.2(3) of the *Immigration Act*, prescribing the limit under section 48(2) of the *CSIS Act*, was not justified under section 1 of the *Charter*.[14]

12.5.2 *A Difficult Problem*

The Committee recognizes that the difficulties posed by the *Chiarelli* decision apply not only to hearings before SIRC, but potentially to other administrative tribunals that hear evidence in private or allow for the limited disclosure of confidential information and the sources of that information. For example, section 48(2) of the *CSIS Act* is incorporated not only in various parts of the Immigration Act, but also in the provisions of the *Citizenship Act* and the *Canadian Human Rights Act*. Provisions similar to that of section 48(2) can also be found in other federal legislation, including the *Privacy Act*, the *Access to Information Act*, and the *Canada Evidence Act*.

The issues raised in the *Chiarelli* decision are related to the crucial balancing of interests that must be specified in the above statutes. In the Memorandum of Argument filed with the Supreme Court of Canada in its application for leave to appeal, the Crown noted that:

> The proposed appeal raises squarely the significant question of what balancing must be specified in statutes which allow for limited disclosure of confidential information and the sources of that information, and whether and to what degree the criteria for such balancing can be developed by the courts and by tribunal rules. Subsection 48(2) of the *CSIS Act* and similar provisions stand at the centre of numerous statutory schemes which may be rendered inoperable if information and sources cannot be maintained in confidence. These statutory schemes seek to protect the public interest in national security and other matters. The validity of these schemes is a question of public importance which merits the attention of [the Supreme Court of Canada].[15]

The Committee agrees that the issues in *Chiarelli* raise important concerns about the "balancing" of the state's interests in safeguarding national security information and its sources against the rights of an individual to know the allegations against him or her so as to be able to make a full and fair defence. The Committee believes that SIRC should try to develop criteria which would take these competing interests into account.

The Committee accepts the decision of the Federal Court of Appeal in *Chiarelli*. Without second-guessing the Supreme Court of Canada, the Committee believes that section 48(2) of the *CSIS Act* needs to be re-drafted. The Committee reviewed draft statutory amendments provided to SIRC in an opinion prepared for it by legal counsel. The considerable number of interests that were raised in the draft amendments underline the difficulty of attempting to balance the interests of CSIS, the Government, SIRC, the complainant and the public at large.

The Committee believes that SIRC, as a first arbiter, must fine-tune the balancing requirements applied during its hearings process. The Committee further urges SIRC to look afield for advice to resolve this problem.

Finally, SIRC may consider allowing a complainant's own counsel to be security-cleared and to attend before the entire proceeding before it. The Committee

believes it is ultimately preferable to have a person's own counsel play the role of advocate, rather than to assign that role to an individual unknown to the complainant. The Committee believes that a system could reasonably be designed to allow complainants' counsel to be security cleared. Although there may be some concern that this would create a "security-cleared Bar", it would surely give complainants some assurance that their own counsel was vigorously advocating their cause. The Committee is aware of a number of situations where confidential information is disclosed to counsel on the condition that it not be disclosed to the client. Cases involving commercial law, mental health issues and applications under the *Access to Information Act* have approved this in order to allow counsel to prepare their cases.[16] Indeed, the Committee believes that the proposed system of allowing counsel to be security-cleared and to attend before SIRC would address the problems related to the inadequate disclosure of information.

The Committee also suggests that SIRC continue to use its roster of security-cleared counsel, as such counsel play an important role, especially for those individuals who wish to represent themselves during a SIRC hearing.

12.5.3 *The Right to Representation by Counsel*

The Committee heard evidence indicating that persons who are required to attend before SIRC as witnesses have done so without the assistance of legal counsel. This concern was expressed by the President of the CSIS Employees' Association when he testified before the Committee and urged that CSIS investigators have the right to legal counsel when they appear as witnesses before SIRC.

SIRC has also noted on a number of occasions that, especially for complaints brought to it when security clearances are denied to DND personnel, the individual appears before the Review Committee unrepresented. As noted in the 1988-89 Annual Report: "It is dismaying to see a young member of the Forces at one of our hearings, unable to afford counsel, matching his wits with the best that the Forces' legal and security machine can muster."[17]

The Committee believes that every individual who is required to attend before the Review Committee should have the opportunity to be represented by legal counsel. It may not always be adequate to rely on counsel for the Service to represent the interests of a CSIS employee. The interests of the Service and the employee may at times be at odds with one another. The Committee notes that under section 70(5) of the *Australian Security Intelligence Organization Act* "A person summoned to appear before [the Security Appeals Tribunal] may request that he be represented by a barrister or solicitor...". The Committee has concluded that a similar provision should be incorporated in the *CSIS Act*.

The Committee suggests that SIRC review its Rules of Procedure to determine whether an amendment could be made to address this issue.

12.6 Augmenting the Powers of SIRC

In this section, a number of issues relating to the powers of SIRC in the complaints process are addressed. As a specialized tribunal with responsibility for the review, investigation and adjudication of security-related matters, SIRC has developed significant experience and expertise in performing its various functions. It is a unique tribunal that, despite some of the concerns expressed in this chapter, should be given increased powers.

12.6.1 *The Binding Nature of SIRC Recommendations*

Subsection 52(2) of the *CSIS Act* provides that:

> 52. (2) On completion of an investigation in relation to a complaint under section 42, the Review Committee shall provide the Minister, the Director, the deputy head concerned and the complainant with a report containing any recommendations that the Committee considers appropriate, and those findings of the investigation that the Committee considers it fit to report to the complainant.

The question of whether SIRC recommendations are binding on deputy heads has been the subject of protracted litigation. SIRC recommended in its brief to the Committee that subsection 52(2) of the *CSIS Act* be amended to provide that its rulings in respect of security clearances be final and binding on a deputy head. This issue has been the subject of substantial litigation before the Federal Court, most notably in *Thomson*.[18]

During various court proceedings, it was submitted that SIRC is an independent, quasi-judicial body that has developed expertise in hearing matters regarding issues related to national security. If deputy heads can continue to disregard SIRC recommendations, this would have the effect of undermining SIRC's independence. Moreover, as the members of the Review Committee are Privy Councillors, it is suggested that the *CSIS Act* has displaced the Crown's former prerogative with respect to matters of national security and security clearances and has delegated its exercise to SIRC. For this reason, and because of the way its process is set out in the Act, the recommendations of SIRC should have binding effect.

In addition, the legislative history of the consideration given to the nature of SIRC's recommendations suggests that the intention was to vest such recommendations with binding authority. The former Solicitor General of Canada, the Honourable Robert Kaplan, in response to a question in the House of Commons in 1983 concerning the role of SIRC, noted:

> An individual denied employment or promotion in the government on the grounds of national security will have a right of review if this Bill is passed. Not only that, in response to the Honourable Member's question, there is already a

> complaints procedure provided in the Bill which has no counterpart today, where anyone in the country who feels he or she has been victimized by the Security Service has a right to a hearing if that is what the Review Committee decides, and it is up to them to decide. Such a person will have the opportunity to get the records corrected and have justice done with respect to his or her case.[19]

As noted by the Federal Court of Appeal in the first *Thomson* decision, the elaborate scheme for reviewing a Minister's decision under the *CSIS Act* tends to confirm that it was Parliament's intention to provide a complainant with a binding remedy rather than simply an opportunity to state a case and learn the basis for the denial.[20] Indeed, the Committee believes that Parliament could only have expressed its intention more clearly if it had used the word "decision", instead of "recommendation", in the provisions of the *CSIS Act*.

The Committee is concerned that this issue is still being litigated. Indeed, at the time of drafting this Report there is an indication that the Minister of Justice will seek leave to appeal the *Thomson* decision to the Supreme Court of Canada. The Committee is also aware of a case involving the Director of CSIS where an individual who had applied for employment with the Service was denied a security clearance. This person made a complaint to SIRC, which in turn recommended that CSIS grant a security clearance to the complainant. The Director of CSIS refused to follow SIRC's recommendation; as a result, the complainant has commenced a civil action against the Service.

The Committee believes that subsection 52(2) of the *CSIS Act* should be amended to vest SIRC decisions with binding authority. The Committee believes that it is financially wasteful for all parties involved to litigate this issue any further.

RECOMMENDATION 100

The Committee recommends that subsection 52(2) of the *CSIS Act* be amended to provide that SIRC rulings in respect of security clearances are final and binding upon a deputy head.

At this juncture, the Committee's only reservation on this issue is whether the findings of the Review Committee should have binding effect in relation to investigations under the *Citizenship Act*, the *Immigration Act* and the *Canadian Human Rights Act*. The Committee is aware of one case under the *Immigration Act* that gives rise to some concern. This case, referred to earlier in this chapter, involved an individual who made an application from within Canada for permanent resident status. About four years ago, he received a notice from Employment and Immigration Canada that he had to leave the country. The individual made a complaint to SIRC and, although given a positive recommendation by SIRC, waited more than a year before receiving a decision from the Minister indicating that he had to start the landing process anew (although he was allowed to make his application from within the country).

12.6.2 *Committee Reports and Statements Under Section 55*

Section 55 of the *CSIS Act* provides that:

> 55. The Review Committee shall consult with the Director in order to ensure compliance with section 37 in preparing:
>
> (*a*) a statement under section 46 of this Act, subsection 45(6) of the *Canadian Human Rights Act*, subsection 19(5) of the *Citizenship Act* or subsection 39(6) or 81(5) of the *Immigration Act*; or
>
> (*b*) a report under paragraph 52(1)(*b*), subsection 52(2) or section 53 of this Act, subsection 19(6) of the *Citizenship Act* or subsection 39(1) or 81(8) of the *Immigration Act*.

Section 55 thus provides that prior to releasing any statement or report, SIRC must consult with the Director of the Service to ensure that what it wishes to release is devoid of information or sources of information that would be detrimental to the security of Canada if disclosed. The legislative history of this provision appears to confirm, however, that the Review Committee can disregard the advice of the Director and report what it believes is appropriate. When the former Solicitor General, the Honourable Robert Kaplan appeared before the Standing Committee on Justice and Legal Affairs in 1984, he opined that SIRC could ignore the advice of the Director if it chose.[21]

Despite the apparent intention of Parliament, there have been differences of view between SIRC and the Service with respect to the disclosure of information to complainants. In SIRC's written replies to questions posed by the Committee, the Review Committee noted that "there have been instances where SIRC's decision to release information to a complainant (under section 55) has resulted in the Service withdrawing from the case so as to avoid the information being released."[22]

Cases that result in this outcome are unsatisfactory. The Committee believes that the Review Committee, as an independent and expert tribunal made up of Privy Councillors, should have the final say in what may or may not be included in its statements and reports. The current practice of consulting with the Director of the Service serves a useful purpose, however, and should be maintained. The Committee made a recommendation on this issue in Chapter 11 of this Report (Recommendation 94).

12.6.3 *Providing Legal or Financial Assistance*

There may be circumstances where a complainant is unable to secure legal assistance through a provincial legal aid plan and must therefore appear before SIRC without legal representation. Of course, part of the role of Committee counsel is to represent the views of a complainant. Because of the reservations expressed elsewhere in

this chapter about the potentially conflicting roles of SIRC counsel, the Committee believes that a different model is required to provide independent legal advice to complainants. The Committee proposes, therefore, that the Review Committee be allowed to provide legal or financial assistance independently or through a provincial legal aid plan. The test for providing such assistance should relate to the individual having a *bona fide* case before the Review Committee as well as to economic need.

Under the provisions of the *Australian Security Intelligence Organization Act*, the Attorney-General "may, if he is satisfied that it would involve hardship to that person to refuse the application ... authorize the provision by the Commonwealth to that person, either unconditionally or subject to such conditions as the Attorney-General determines, of such legal or financial assistance in relation to the proceedings as the Attorney-General determines."[23]

This provision allows the Attorney-General of Australia to provide legal or financial assistance in connection with Security Appeals Tribunal hearings. The British Columbia Law Union has indicated its support for the inclusion of a similar provision in the *CSIS Act*.

RECOMMENDATION 101

The Committee recommends that the Government study the feasibility of authorizing the Review Committee to provide legal or financial assistance to any person who, it is felt, requires such assistance to present his or her case before the Review Committee.

12.6.4 *Awarding Costs*

The Australian Royal Commission on Intelligence and Security, which reported in 1978, recommended that the government compensate a person who had been the subject of a wrongful denial of a security clearance.[24] The Committee believes that similar provisions should be made to award costs to a complainant who has been successful before SIRC.

As a final recommendation in this part of the chapter, the Committee proposes that SIRC be able to award costs to a complainant who, in its opinion, was successful in a matter before it. This recommendation found favour with Professor Murray Rankin and with the British Columbia Law Union in their testimony before the Committee, as well as with every complainant and legal counsel contacted by Committee staff. It is contemplated that such compensation should be paid by the Solicitor General, but that costs not be awarded in favour of CSIS or the government department involved. To do so would have the effect of penalizing complainants who are exercising their rights before SIRC.

RECOMMENDATION 102

The Committee recommends that the *CSIS Act* be amended so that SIRC may award costs to a complainant who was successful in his or her application before the Review Committee.

12.7 Judicial Review of SIRC Decisions

Under the current provisions of the *Federal Court Act*, applications for judicial review can come before the Federal Court under either section 18 or section 28 of the Act. The Federal Court system has been criticized because of the confusion that arises with respect to the division of responsibility between the Trial Division and the Federal Court of Appeal. The Committee learned of a number of cases involving issues under the *CSIS Act* that have required an applicant to bring more than one application before the Federal Court because of jurisdictional difficulties. As a result of this split jurisdiction, commencing proceedings at the Federal Court is all too often plagued by uncertainty.

SIRC recommended in this brief to the Committee that in the case of one of its decisions being challenged before the Federal Court, the Federal Court of Appeal should be granted exclusive jurisdiction under section 28 of the *Federal Court Act*. It recommended further that the Federal Court of Appeal be empowered to review all documents and files under the control of SIRC and that procedures be authorized to enable SIRC files and documents to be transferred to the Federal Court of Appeal without the nature of those documents being made public and, where necessary, without even the existence or absence of these documents being acknowledged. SIRC proposed these amendments to make judicial review of its decisions fairer and more efficient. The Committee accepts SIRC's proposals and accordingly makes the following recommendations.

RECOMMENDATION 103

The Committee recommends that the *Federal Court Act* be amended to provide that, in the event of judicial review, the Federal Court of Appeal have exclusive jurisdiction under section 28 of the *Federal Court Act*, and that it be entitled to review any SIRC report rendered pursuant to section 42 or any report affecting the rights of an individual rendered pursuant to section 41, together with all relevant documents.

RECOMMENDATION 104

The Committee recommends that special procedures be established under the *CSIS Act* and the *Federal Court Act* to enable SIRC files and documents to be transferred to the Federal Court of Appeal without the nature of these documents being made public and, where necessary, without even the existence or absence of such files being acknowledged.

NOTES

1. Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (McDonald Commission, 1981), Second Report, Volume 2, p. 812.

2. *Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C– 23, as amended, section 38.

3. *Royal Canadian Mounted Police Act*, section 45.37.

4. Canada, House of Commons, *Minutes of Proceedings and Evidence of the Standing Committee on Justice and Solicitor General*, Issue No. 30 (April 24, 1990), pp. 16 and 18.

5. Security Intelligence Review Committee, *Amending the CSIS Act: Proposals for the Special Committee of the House of Commons 1989*, p. 11.

6. *Ibid.*, pp. 11–12.

7. Security Intelligence Review Committee, "Immigration Screening Activities of the Canadian Security Intelligence Service", January 18, 1988, released under the *Access to Information Act*, pp. 7–8.

8. McDonald Commission, Second Report, Volume 2, *op. cit.*

9. Conversation with Senior Complaints Officer of SIRC, May 22, 1990.

10. *Chiarelli* v. *Minister of Employment and Immigration*, unreported, February 23, 1990, File #A–219–89, (Federal Court of Appeal).

11. *Chiarelli* v. *M.E.I.*, pp. 1 and 2 of Stone J.A.'s judgment.

12. *Chiarelli* v. *M.E.I.*, p. 4 of Stone J.A.'s judgment.

13. *Ibid.*

14. Section 48(2) of the *CSIS Act* states:

    48.(2) In the course of an investigation of a complaint under this Part by the Review Committee, the complainant, deputy head concerned 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.

15. *The Minister of Employment and Immigration and Joseph Chiarelli*, Applicant's Memorandum of Argument, Supreme Court of Canada, paragraph 43.

16. See (Commercial law interests) *Magnasonic Canada Ltd.* v. *Anti– Dumping Tribunal*, (1972) F.C. 1239, 30 D.L.R. (3d) 118 (C.A.), per Jackett C.J. and the *Canadian International Trade Tribunal Act*, S.C. 1988, c.56, sections 43–49.

(Mental Health law) *Re Egglestone & Mousseau and Advisory Review Board* (1983) 150 D.L.R. (3d) 86 (Ont. HC Div. Ct.).

(*Access to Information Act*) *Hunter and Consumer and Corporate Affairs*, unreported, March 1, 1990, File #T–1998–87, (Federal Court Trial Division).

17. SIRC *Annual Report*, 1988–1989, p. 47.

18. *Thomson* v. *The Queen* (1988), 3 F.C. 108 (C.A.);
Thomson v. *The Queen* (1989), 1 F.C. 86 (T.D.);
Thomson v. *The Queen*, unreported, May 17, 1990, File #A–748– 88, Federal Court of Appeal.

19. Canada, House of Commons, *Debates*, June 6, 1984.

20. *Thomson* v. *The Queen* (1988), 3 F.C. 108 (C.A.), at pp. 136– 138.

21. Canada, House of Commons, *Minutes of Proceedings and Evidence of the Standing Committee on Justice and Legal Affairs*, Issue No. 9 (April 2, 1984), p. 14.

22. Written Response of the Security Intelligence Review Committee to the Special Committee's Questions, reply dated January 11, 1990, p. 16.

23. *ASIO Act*, subsection 72(2).

24. Royal Commission on Intelligence and Security (The Hope Commission), Second Report, 1978, p. 95.

CHAPTER THIRTEEN

The Complaints Process — The RCMP Public Complaints Commission

13.1 Background

In 1974 the federal government established a Commission under Mr. Justice René Marin to inquire into RCMP procedures for dealing with discipline, grievances and the handling of complaints by members of the public against the Force. When the Commission reported in 1976, it recommended that the RCMP should continue to investigate complaints, but that a Federal Police Ombudsman be appointed with powers to make inquiries and to appoint tribunals for holding public hearings concerning the merits of complaints.

Following public revelations of extensive alleged wrongdoing, the federal government established a further commission of inquiry in 1977 to inquire into certain activities of the RCMP. Although the McDonald Commission focused on the work of the Security Service, its final reports of 1981 concluded that the police should have the authority to investigate complaints and that an Office of the Inspector of Police Practices should be established within the Solicitor General's department to conduct investigations and to report regularly to the Minister.

In 1986, SIRC concluded that the RCMP possessed security intelligence capabilities "which might operate in parallel with CSIS, duplicating or even conflicting with the Service's primary role mandated by Parliament", and observed that there was

> comparatively little independent oversight of the RCMP – no Inspector General, no Review Committee, no annual report tabled in Parliament, no independent adjudication for members of the public and less stringent requirements for obtaining warrants authorizing interception of communications.[1]

13.2 Establishment of the RCMP Public Complaints Commission

Despite the introduction of a number of legislative proposals, Parliament did not amend the *RCMP Act* until March 1986. This amendment provided for mechanisms by which the Force could be held publicly accountable for the conduct of its almost 18,000 members. Part VI of the amended legislation established the RCMP Public Complaints

Commission in December 1986. This Commission is an independent administrative body, external to the RCMP, that is mandated to receive, review and inquire into complaints against members of the RCMP, regardless of whether they work for the Force as federal officers or under provincial or municipal contracts.

Any member of the public may make a complaint to the RCMP, the provincial authority of the province in which the subject matter of the complaint arises, or directly to the Commission about the conduct of any member of the Force in the performance of his or her duties under the Act. There is no requirement that the complainant be involved in the subject matter of the complaint. In addition, the Chairman has the authority to initiate complaints. This may arise, for example, where a person in an official capacity makes a complaint or where a complainant wishes to preserve anonymity. A recent case heard in the Federal Court Trial Division affirmed the right of the Commission to investigate complaints even if their subject matter occurred prior to the amendment of the Act.

Significantly, section 45.43 of the *RCMP Act* also gives the Commission the authority to investigate a complaint or to instigate a hearing into a complaint where the Chairman considers it advisable in the public interest. The Commission has drafted rules governing procedures to be followed at such hearings.

The Chairman of the Commission is designated as a deputy head under the *Public Service Employment Act*. Among the responsibilities of Dr. Richard Gosse, the current Chairman, is an obligation to submit an annual report to the Solicitor General of Canada for tabling before both Houses of Parliament.

13.3 Committee's Interest in the RCMP Public Complaints Commission

The Committee was interested in the Commission's work because neither SIRC nor the Inspector General of CSIS has any authority to review the activities of those elements of the RCMP that fulfil the Force's national security responsibilities.

The Committee wrote three letters to Dr. Gosse. Two concerned specific cases. The other related to the role of the Commission and inquired about investigations he might have undertaken into the conduct of RCMP officers arising out of the performance of their duties relating to the *Security Offences Act*. Until the formation of the National Security Investigations Directorate (NSID) and its regional sections (NSIS) in 1988, such officers were employed in the National Crime Intelligence Branch (NCIB), its regional sections (NCIS), or other elements having responsibility for protective policing.

The first case about which the Committee wrote to Dr. Gosse concerned the interrogation of Gordon Thomas, (a correspondent for the London Sunday Express and author of *Journey into Madness*, a study of CIA brainwashing programs), at Mirabel International Airport. In this case, Charles Dale, President of the Newspaper Guild of

America, made a complaint on the journalist's behalf. He claimed that Mr. Thomas had been improperly detained for between one and two hours and questioned about his sources of information. This, Mr. Dale argued, constituted unwarranted harassment. He also opined that the case raised *Charter* issues and matters specifically concerning freedom of the press. While the Chairman has appointed a panel to hear this complaint, Mr. Thomas has indicated a reluctance to return to Canada to appear before it. The Committee believes that in matters of considerable public interest, panels appointed by the Chairman of the RCMP Public Complaints Commission should be able to travel abroad to hear testimony. SIRC has already acknowledged that it has adopted this practice.

The second case about which the Committee wrote to Dr. Gosse concerned matters arising out of inquiries made in May 1989 by NSIS officers at the El Salvador Information Office in Vancouver. According to newspaper reports, officers of the unit asked questions about fund-raising, contacts with the Faribundo Marti National Liberation Army (FMLNA) and the Information Office's speaking tours.[2] The Committee's letter indicated that it wanted to know 1) whether the Commission had received a complaint concerning this matter; 2) whether members of the Information Office knew about the Public Complaints Commission; and 3) whether the Commission had considered undertaking an investigation in the public interest. Underpinning the Committee's questions was a wish to establish whether any security offence had been committed and if so, what; whether the inquiries had had a "chilling" effect on the rights of Canadians to lawful advocacy, protest, and dissent; and whether there had been any impropriety in the RCMP's investigations.

When Dr. Gosse testified, he did not fully address the issues raised by the Committee. While he did indicate that no complaint had been received by the Commission and that, from conversations with the British Columbia Civil Liberties Association, he understood that the Information Office did know about the complaints process, he went no further than to state:

> In this particular instance I thought about initiating a complaint. In the end I guess it is fair to say that I concluded that if neither the El Salvador Information Office people nor the B.C. Civil Liberties Association wished to initiate a complaint, we had lots of other matters to deal with, and I did not do so. I thought about it, and it was a judgment call on my part not to do that.[3]

The Committee wishes to make two observations regarding this case. First, it has reason to suspect that the interview may have had a "chilling" effect on the activities of the El Salvador Information Office. Second, the Committee wishes to commend the RCMP for distributing, in December 1989, a new General Policy Statement regarding the Force's National Security Investigations Program. The Committee believes that the guidelines provided in this document should go a long way to prevent unwarranted questioning by members of National Security Investigations Sections.

The Committee also made enquiries into a third case. This related to the arrest of a twenty-year veteran of the RCMP attached to the regional NSIS in Montreal. The officer

arrested was charged with two counts of corruption, nine counts of breach of trust, and one of trafficking in cocaine. According to media reports, the charges related to accepting money for information and providing tip-offs concerning confidential RCMP investigations. One television broadcast claimed that "the criminal charges laid today have nothing to do directly with the corporal's job in national security"[4] (emphasis added).

The Committee approached the Commissioner of the RCMP directly on this matter with a view to establishing (i) whether the charges laid in any way related to the officer's work for NSIS; and (ii) whether the passing of confidential information regarding RCMP investigations posed a threat to the security of Canada. The Commissioner confirmed to the Committee by letter that the criminal charges "did not in any way relate to [the officer's] work as a member of NSIS." In addition, he stated that:

> it is our assessment, which is shared by CSIS and by other agencies with whom we have contact, that [the officer's] actions have not resulted in a threat to the national security of Canada.

The Commissioner also informed the Committee that he had canvassed all divisions within the Force with a view to establishing whether any other officer involved in national security-related duties had been charged or disciplined since July 16, 1984. He indicated that the divisions were not aware of any charges or disciplinary action.

The Committee acknowledges that the Chairman of the RCMP Public Complaints Commission and some of his staff have very substantial experience in performing reviews of this sort. Nevertheless, it believes that their primary function is to review public complaints, a function that is already substantial and is likely to expand as the Commission becomes better known. It therefore does not recommend that the Commission be given any additional responsibilities in this area. The Committee recommended in Chapter 11 that RCMP security- related duties be subject to review by SIRC (Recommendation 88).

RECOMMENDATION 105

The Committee recommends that SIRC be authorized to receive complaints about the conduct of members of the RCMP employed by the Force in national security-related matters but be required to forward such complaints to the RCMP Public Complaints Commission.

RECOMMENDATION 106

The Committee recommends that SIRC be empowered to request the RCMP Public Complaints Commission to conduct an investigation into a complaint concerning a national security-related matter.

NOTES

1. Security Intelligence Review Committee, *Annual Report 1985– 86*, p. 7.

2. See, for example, Richard Cleroux, "RCMP Security Team Could Rival CSIS", *The Globe and Mail* (July 4, 1989), pp. A1–A2.

3. Canada, House of Commons, *Minutes of Proceedings and Evidence of the Special Committee on the Review of the CSIS Act and the Security Offences Act*, Issue 17 (February 22, 1990) pp. 7–8.

4. Dennis Trudeau and Ray Fichaud, "RCMP Officer Suspected of Tipping off Drug Investigations," *Newswatch*, CBMT, April 5, 1990.

CHAPTER FOURTEEN

The Role of Parliament

14.1 Background

Parliament has played a minor role in monitoring and reviewing the activities of Canada's security and intelligence community. Even in what is arguably its most traditional of functions—the scrutiny of departmental estimates and the voting of funds—Parliament's involvement has been minimal in the area of security and intelligence. It has not been made privy to information on CSIS beyond the one-line entry in the Main Estimates.

This lack of involvement has developed for a variety of reasons. Perhaps of greatest importance has been the perception that matters of national security are by convention the prerogative of the Crown, not Parliament. This perspective has been enhanced by the view that intelligence agencies need a high level of secrecy to be effective and that making Parliament knowledgeable about such matters may not only politicize affairs, but may actually endanger the state by weakening the effectiveness of its defences.

The extended period of public scrutiny encompassed by the Keable and McDonald Commissions stimulated parliamentary activity in the area. After the adoption of the *CSIS Act* in 1984, the House of Commons Standing Committee on Justice and Solicitor General heard testimony on a fairly regular basis from the Solicitor General, the Director of the Service, SIRC, and the Inspector General. Between 1986 and 1989, the Senate conducted two important inquiries into terrorism and public safety. Parliament also replaced the *War Measures Act* by adopting the *Emergencies Act*.

14.2 Current Obligations

Parliament placed a number of statutory obligations on itself when it passed the *CSIS Act* and the *Security Offences Act*. The Solicitor General must now lay SIRC's annual report before each House of Parliament within fifteen sitting days of receiving it. This has drawn parliamentary and public attention to the security intelligence function.

Finally, section 56 of the *CSIS Act* and section 7 of the *Security Offences Act* required Parliament to establish a committee for the specific purpose of conducting "a comprehensive review of the provisions and operation" of the two Acts and to submit a report on that review to Parliament.

14.3 The Comprehensiveness of the Committee's Review

The Committee believes it is part of its statutory obligation to assess how comprehensive its review has been. The Committee undertook a number of research initiatives to supplement and complement its public hearings. Some of these initiatives were more successful than others. Research interviews provided useful background information concerning the role and function of members of Canada's security and intelligence community, as did many of the *in camera* briefing sessions provided by witnesses representing various government departments and agencies. The public hearings were useful in so far as they gave Committee members a sense of what was of current concern to Canadians. The Committee received numerous thoughtful and well-argued briefs from individual Canadians and from organizations. In this regard, the Committee was particularly well served by SIRC. The Committee believes it has been able to do the best job possible in conducting a comprehensive review of the provisions of the two Acts, given the various constraints it faced.

The Committee is less confident that it has been able to assess how the *CSIS Act* is operating. Important documents that would have allowed the Committee to reach some fairly firm conclusions were not made available to it. The Committee was unable to examine the Minister's written directions, the Director's annual reports, the Inspector General's certificates or any other reports produced by his office, or the special reports of SIRC, especially those concerning how the various branches of the Service function. With the exception of a special *in camera* briefing provided by the RCMP on its security-related responsibilities, the Committee's staff was prevented from attending briefings on secure premises. Consequently, the Committee believes it has been unable to review adequately the roles of key government participants in the security and intelligence process.

14.4 Future Needs

As a result of its experience and because it has been unable to fulfil its obligations to Parliament regarding this review of the operation of the *CSIS Act*, the Committee believes that steps should now be taken to ensure that Parliament has a greater continuing review and oversight capacity in this area. Parliament requires the wherewithal to understand and review the actions of the Service and to obtain such information from the review agencies as it believes is necessary to make the Service properly accountable.

Recommendations have already been made in this Report that, if acted upon, would make the Inspector General of CSIS somewhat more independent and give SIRC wider access to information and a broader review mandate. The Committee believes that it was Parliament's intention that SIRC's reports be fully intelligible to Parliament. Clearly, this is not the case at the moment; nor can SIRC report in a timely fashion under the current restrictions imposed on the Review Committee by the *CSIS Act*.

To rectify this situation, the Committee has already recommended that SIRC be able to submit special reports to Parliament when it deems it appropriate. But this is only part

of the answer. Parliament needs to be able to go behind SIRC's reports to ensure that the Review Committee is actually posing the questions Parliament would want to ask and investigating matters on which it would want to have reports. To make this possible, the Committee puts forward the following scheme for consideration.

14.5 A Scheme for the Next Five Years

The Committee believes Parliament should have a continuing role in the review of security and intelligence agencies other than CSIS. Many of them have extensive powers to infringe on the rights and freedoms of Canadians and, as such, must be scrutinized more closely by Parliament. Many Canadians rightfully expect their representatives to protect their interests and to be fully informed about the activities of agencies like CSIS. A committee of Privy Councillors can be no substitute for democratically elected parliamentarians.

The Committee acknowledges there will be resistance in some quarters to establishing a parliamentary committee on security and intelligence. The Committee understands this reluctance. It believes, however, that recent events in Eastern Europe have tipped the balance in favour of greater openness. It is now time for Parliament to play a larger role and to be fully informed.

The Committee examined a number of options available to Parliament. After careful consideration, the Committee is hesitant to make a comprehensive recommendation about how Parliament should review Canada's security and intelligence matters over the long term. As a result, the recommendations that follow are intended as an interim step to cover the next five years and to make the best use of the experience that has been gained to date.

RECOMMENDATION 107

The Committee recommends that the House of Commons Standing Committee on Justice and Solicitor General establish a permanent sub-committee to deal exclusively with security and intelligence matters.

The Committee is cognizant of the need to keep certain information secret. To restrict the flow of classified information within Parliament, the Committee believes that the membership of the proposed sub-committee should be kept as small as possible.

The Committee is also cognizant of the fact that the review process places burdens on organizations that are subject to review. It therefore wishes to be particularly careful not to impose on agencies such as CSIS an additional level of review. The Committee has already recommended that SIRC should normally request the Inspector General of CSIS to conduct compliance reviews. The Committee is not recommending that the sub-committee's research staff have a function similar to those of SIRC or the Inspector

General. Nor does it believe that the sub-committee would ask CSIS for information frequently. Such matters would be addressed through SIRC. Rather the Committee believes that the sub-committee's role would be primarily three-fold. First, it would review budgets and make recommendations concerning the Main Estimates to the Standing Committee on Justice and Solicitor General or to such other committees as the House of Commons may consider necessary. Second, it would oversee the activities of SIRC and the Inspector General by reviewing their work plans and reports. Third, it would undertake reviews of a general nature regarding security and intelligence matters that would be of interest to Parliament.

RECOMMENDATION 108

The Committee recommends that the functions of the sub- committee be (1) to review the budgets of security and intelligence organizations with a view to providing reports to such committees as the House of Commons may determine; (2) to review the work undertaken by SIRC and the Inspector General; and (3) to undertake reviews of a general nature regarding security and intelligence matters.

RECOMMENDATION 109

The Committee recommends that the sub-committee be composed of five members.

The Committee believes further that the sub-committee will require its own full-time research and support staff to provide it with the advice it will need and to make its work effective. U.S. Congressional committees charged with reviewing the activities of the American security intelligence community have found this essential.

RECOMMENDATION 110

The Committee recommends that a small, expert, full-time research staff with its own administrative support staff be specially hired to conduct research and to analyze material under the direction of the sub-committee.

To ensure that proper security procedures are followed and to permit members of the sub-committee and staff to have access to all necessary documents and information, the Committee believes that staff of the sub-committee should be security cleared and placed under an appropriate oath.

RECOMMENDATION 111

The Committee recommends that all research and support staff of the sub-committee undergo security assessments and that all senior staff be cleared to the Top Secret Special Activity level and be placed under an appropriate oath.

RECOMMENDATION 112

The Committee recommends that the sub-committee meet *in camera* in a secure environment and that all notes and documents relating to its work be retained in a secure environment.

The Committee considers that it would be inappropriate for Members of Parliament to be vetted by the Service. It believes, however, that Members of Parliament who serve on special committees of either the House of Commons or the Senate who see classified material should be placed under an appropriate oath.

The Committee recognizes that continuity of membership on the sub-committee and in staffing is important for a variety of reasons. Continuity of membership and staff will build expertise and experience, as well as confidence in the Committee by both the public and the security and intelligence community. Too much turnover among membership and staff may increase the possibility of leaks and make it more difficult to identify the source of such leaks should they occur. In addition, security assessments of staff to the Top Secret Special Activity level are the most time-consuming and costly to perform.

RECOMMENDATION 113

The Committee recommends that the Party leaders attempt to ensure continuity, security and integrity in membership on the sub-committee for the duration of a Parliament.

The Committee has already set out a number of safeguards that should be incorporated into this scheme. It believes one further safeguard is in order.

RECOMMENDATION 114

The Committee recommends that, before submitting any report to any other committee of the House of Commons or to the House of Commons as a whole, the sub-committee develop procedures to establish whether the release of any information in such reports could pose a threat to the security of Canada.

In the event that the House of Commons Standing Committee on Justice and Solicitor General decides not to establish a sub-committee on security and intelligence, the Committee believes that the *CSIS Act* and the *Security Offences Act* should be amended to provide for another parliamentary review five years after the tabling of this Report.

The Committee believes that the work it accomplished has been productive, despite the difficulties it has encountered. The recommendations in this Report are testimony to that fact. The usefulness of Parliament reviewing the provisions and operations of the *CSIS Act* and the *Security Offences Act* should not be disregarded in the future. Nor should its right to do so be discounted. The Committee nevertheless believes that the five-year review, although better than nothing, does not have the same advantages as a continuing review by Parliament.

RECOMMENDATION 115

The Committee recommends that, in the event that the Standing Committee on Justice and Solicitor General decides not to establish a sub-committee on security and intelligence, section 56 of the *CSIS Act* and section 7 of the *Security Offences Act* be re-enacted to provide for another parliamentary review five years after the tabling of this Report.

In the course of its work, the Committee encountered a number of difficulties. It did not have full access to the materials and officials it required to conduct the comprehensive review required by the law. The one-year time limit imposed on the Committee to complete its work, provided for in the *CSIS Act* and the *Security Offences Act*, also proved to be an impediment. The Committee believes that Parliament should take note of these difficulties if it decides in favour of another five-year review.

RECOMMENDATION 116

The Committee recommends that, in the event Parliament opts for another five-year review, the *CSIS Act* and *Security Offences Act* be amended to provide that the Committee established for the purposes of conducting such a review:

1) **have access to any information under the control of the Service that relates to the performance of the duties and functions of the Committee and be entitled to receive from the Director and employees such information, reports and explanations as the Committee deems necessary for the performance of those duties and functions;**

2) **have the obligation to submit its final report to Parliament, not within a predetermined time limit, but only at such a time as the Committee considers appropriate; and**

3) **have its staff security cleared before the start of the review.**

CHAPTER FIFTEEN

Conclusion – Setting the Agenda

The security and intelligence community plays an important role in Canada. It must perform its functions effectively with the resources at its disposal, but it must do so without infringing rights and freedoms and while being accountable for its actions. In 1984, Parliament made important changes to the security and intelligence community by adopting the *CSIS Act* and the *Security Offences Act*, whose provisions and operation were the object of this comprehensive review.

When the House of Commons established this Committee on June 27, 1989, the members knew that the task they had been assigned was a sensitive, complex one that had to be completed within a tight timeframe. They were also fully aware of the difficulty and importance of their assignment. With these factors in mind, the Committee undertook, as described throughout this Report, a number of inter-related activities, both traditional and innovative in the parliamentary context, to complete its workplan.

The Committee's comprehensive review was carried out during a time of uncertainty and dynamic change. Recently, there have been unexpected developments in the international political realm whose outcomes do not easily lend themselves to prediction. Basic political changes have occurred in many parts of the world, with consequential impacts on alliances, institutions and ideologies. The Post-World War II era, with all it implies, appears to be coming to an end, and a new historical epoch seems to be beginning. Resulting from this era of international political dynamism will be new challenges for Canada's security and intelligence community. These challenges will be fuelled by changing alliances, governments and ideologies.

The security and intelligence community itself has experienced change and uncertainty in recent years. After a painful beginning when CSIS was fashioned out of the RCMP Security Service, the Service was subjected to a mid-course correction in 1987. As a result of the implementation of many of the recommendations of the Independent Advisory Team, the Service is much changed from its beginning. Many of the changes in the Service are still in the process of being implemented. Thus the Service itself is still in flux and adapting to changing internal and external realities.

As a result of its comprehensive review of the provisions and operation of the *CSIS Act* and the *Security Offences Act*, the Committee did not find any egregious improprieties, although it came across a number of issues it believes have to be addressed. The Committee believes that the uniquely Canadian security and intelligence model reflected in the *CSIS Act* and the *Security Offences Act* has worked well and should be preserved. Based on this fundamental conclusion, the Committee's recommendations, if

implemented, will build upon and improve security and intelligence institutions already in place.

The Committee's recommendations will have the effect of clarifying the mandates of the security and intelligence community without impairing its ability to function effectively and efficiently. The proposals for direction and judicial control contained in this Report, if adopted, will ensure that the security and intelligence community performs its functions within the limits of its mandates. Adoption of the Committee's recommendations for augmenting the independence and broadening the jurisdiction of the review mechanisms in the security and intelligence community will strengthen the accountability structures already in place and consequently make them both more comprehensive and more effective. Because the Committee believes the complaints process to be essential in providing redress to those who may have been aggrieved, it believes that the changes it urges will make a unique and largely effective system function at an even higher level. Parliamentary review of the security and intelligence community is important for assuring Canadians that the system is effective and not functioning to restrain rights and freedoms. The Committee believes its recommendations in this area will ensure efficiency and effectiveness while not disrupting the institutions already in place.

As indicated in various parts of this Report, the Committee had considerable difficulty in getting full access to the documents and information required to conduct its review. The Committee understands why this was so. Security and intelligence work is both important and sensitive and thus best carried out beyond the glare of direct public scrutiny. Major adjustments in attitude were therefore required in the security and intelligence community for it to accept and accommodate a comprehensive review by Parliament. Some progress was made in this area. Still more remains to be achieved. There must be such progress if the review role the Committee recommends for Parliament with respect to security and intelligence matters is to be performed effectively.

There are a number of issues the Committee was unable to explore thoroughly in conducting this review and that require close examination. These unfinished parts of the security and intelligence review agenda should be taken up by the sub-committee that the Committee has recommended be established by the Standing Committee on Justice and Solicitor General. Among the issues that should be considered by the proposed sub-committee are the following:

1) a review of the *Official Secrets Act* and related provisions of the *Criminal Code*;

2) a review of Emergency Preparedness Canada and the *Emergencies Act*;

3) a review of the role and functions of such other members of the security and intelligence community as can be found in the

Department of External Affairs, the Department of National Defence, the Department of Employment and Immigration, the Department of Transport and Revenue Canada;

4) a study of the invocation of sections 37–39 of the *Canada Evidence Act*;

5) an examination of archives policy as it relates to historical research in the security and intelligence area;

6) monitoring of exempt banks under the *Privacy Act*;

7) a study of the feasibility of establishing an institute of security intelligence studies at a Canadian university;

8) an examination of the Report of the External Review of the Canadian Forces Special Investigation Unit conducted by the Honourable René J. Marin;

9) an examination of public awareness of security and intelligence issues and of the complaints process;

10) a review of the Independent Advisory Team reports recommended in this Report;

11) a review of SIRC's March 1989 decision to suspend its proposed inquiry into CSIS policies, procedures and practices related to the Narita bombing and the loss of Air India Flight 182 in June 1985;

12) a review of the reports, documents, transcripts and other evidence accumulated by the McDonald Commission to determine whether they have all been made accessible to the public;

13) a review of the *CSIS Act* warrant provisions in light of the *Atwal* decision; and

14) an evaluation after five years of its own experience with parliamentary review.

Some of the recommendations made by the Committee go beyond the confines of the *CSIS Act* and the *Security Offences Act*. This is particularly so in reference to the Committee's recommendations dealing with the expansion of SIRC; the independence of the Inspector General of CSIS; a legislated mandate for Communications Security Establishment and the RCMP's National Security Investigations Directorate; the adoption of the Government Security Policy in the form of regulations; co-ordination,

assessment and dissemination of intelligence; and labour relations and human resource management issues. Consequently, the legislative base set out in the two Acts will be inadequate if the Committee's recommendations are implemented. It will therefore be necessary for Parliament to adopt a *National Security Act*. Such an Act would incorporate the *CSIS Act* and the *Security Offences Act*, as well as whatever other legislative changes may be required by the implementation of the Committee's recommendations. The adoption of such legislation would codify the rules establishing the mandates, control, accountability, and redress mechanisms to which the security and intelligence community would be subject.

RECOMMENDATION 117

The Committee recommends that Parliament adopt a *National Security Act*, which would incorporate the *CSIS Act*, the *Security Offences Act* and any other legislation necessitated by the implementation of the recommendations set out in this Report.

The proposals contained in this Report build upon existing institutions and indicate how they can be made to function more effectively. Their implementation will enable the security and intelligence community to adapt to a rapidly changing reality. They will take the security and intelligence community through the 1990s and beyond.

RECOMMENDATIONS

1) **The Committee recommends that the Canadian Security Intelligence Service, the Inspector General and the Security Intelligence Review Committee be continued, and that the provisions of the *Canadian Security Intelligence Service Act* and the *Security Offences Act* be retained and amended by adoption of the recommendations contained in this Report.**

2) **The Committee recommends that section 3 of the *CSIS Act* be amended to set out the objectives to be pursued by the Service, and to ensure that these objectives and the primary and secondary mandates of CSIS are not pursued to the detriment of lawful advocacy, protest or dissent.**

3) **The Committee recommends that the terms "espionage" and "sabotage" be defined in the *CSIS Act* and that modern definitions of these terms be inserted into the *Criminal Code*, the *Official Secrets Act*, and related legislation.**

4) **The Committee recommends that the phrase "detrimental to the interests of Canada", used in paragraphs (*a*) and (*b*) of the definition of threats to the security of Canada, contained in section 2 of the *CSIS Act*, be itself defined.**

5) **The Committee recommends that paragraph (*a*) of the definition of 'threats to the security of Canada' contained in section 2 of the *CSIS Act* be amended by removing the words "directed toward or".**

6) **The Committee recommends that paragraph (*b*) of the definition of threats to the security of Canada contained in section 2 of the *CSIS Act* be amended so that the words "foreign–influenced" are replaced by "foreign–directed".**

7) **The Committee recommends that paragraph (*b*) of the definition of threats to the security of Canada contained in section 2 of the *CSIS Act* be amended by inserting the word "directly" before the phrase "relating to Canada".**

8) **The Committee recommends that paragraph (*b*) of the definition of threats to the security of Canada contained in section 2 of the *CSIS Act* be amended by inserting the word "serious" before the phrase "threat to any person".**

9) **The Committee recommends that paragraph (*c*) of the definition of threats to the security of Canada contained in section 2 of the *CSIS Act* be amended by inserting the word "directly" before the phrase "relating to Canada" and by deleting the words "directed toward".**

10) **The Committee recommends that paragraph (*d*) of the definition of 'threats to the security of Canada' contained in section 2 of the *CSIS Act* be repealed.**

11) **The Committee recommends that section 21(5)(*a*) of the *CSIS Act* be repealed.**

12) **The Committee recommends that the Solicitor General issue to the Director of the Canadian Security Intelligence Service a comprehensive direction dealing with CSIS's primary mandate.**

13) **The Committee recommends that the *CSIS Act* be amended to define "security assessment" under section 2 of the Act to coincide with the 'threats to the security of Canada' provisions under the Act.**

14) **The Committee recommends that the *CSIS Act* and the Government Security Policy be amended to provide that a person who is subject to a security assessment interview be allowed to be accompanied by legal counsel or an agent and to have the interview tape-recorded after advising the Service of his or her intention to do so.**

15) **The Committee recommends that the "Security Exclusion" provisions of the *Immigration Act* be amended to correspond with the "threats to the security of Canada" definition contained in section 2 of the *CSIS Act*.**

16) **The Committee recommends that Treasury Board study the possibility of revising the Government Security Policy so as to reduce the number of categories for the classification of government information.**

17) **The Committee recommends that the Government Security Policy be adopted as regulations by the Governor in Council.**

18) **The Committee recommends that the Government ensure that guidelines are in place both within CSIS and in government departments to ensure that security assessment reports are treated as confidential and are communicated only to persons who have authority to have access to them.**

19) **The Committee recommends that an Independent Advisory Team be created with a mandate to examine Canada's foreign intelligence capacity.**

20) The Committee recommends that the Independent Advisory Team study the implications of enlarging the foreign intelligence mandate of CSIS by repealing the words "within Canada" from section 16 of the *CSIS Act*.

21) The Committee recommends that the Independent Advisory Team ascertain, among other things, 1) whether the Service has the necessary resources and appropriate skills mix to enable it to conduct foreign intelligence operations outside Canada, and 2) whether it is appropriate for a single agency to conduct both security intelligence and foreign intelligence operations, either in Canada or abroad.

22) The Committee recommends that the Independent Advisory Team prepare a public version of its findings to be tabled in Parliament.

23) The Committee recommends that section 16 of the *CSIS Act* be amended by adding the term "foreign intelligence" in such a way as to show that the collection and investigation activities mandated under that section constitute foreign intelligence.

24) The Committee recommends that the term "foreign intelligence" be added to the interpretation section of the *CSIS Act*.

25) The Committee recommends that the Independent Advisory Team examine the co-ordination, assessment and dissemination of intelligence in the Government of Canada.

26) The Committee recommends that the Independent Advisory Team examine the security and intelligence function in PCO with a view to determining whether it is accomplishing its work in this area efficiently and effectively.

27) The Committee recommends that the Independent Advisory Team examine the feasibility of establishing in Canada an independent Bureau of National Assessments.

28) The Committee recommends that SIRC undertake a follow-up review of, and prepare a report on, language issues within the Service. SIRC's review should address 1) the possibility of representational imbalances with respect to Francophones; 2) the adequacy of services in both official languages within CSIS; 3) the accuracy of CSIS reports regarding official languages; and 4) the possibility of harassment by CSIS management of employees who make language-related complaints. A public version of SIRC's final report on official languages within the Service should be tabled in Parliament within a reasonable period.

29) The Committee recommends that the Service complete the development and implementation of its employment equity program by December 31, 1991. The program should aim to increase the representation of women, visible minorities, Aboriginal people, and disabled persons.

30) The Committee recommends that the CSIS employment equity program be based on an active, rather than a reactive strategy, in that the Service should actively seek out women and candidates from minority groups.

31) The Committee recommends that the Service continue to recruit individuals with knowledge of languages other than English and French.

32) The Committee recommends that the Service review the psychological assessment program it administers for employee selection purposes with a view to determining whether it is still current and appropriate for its needs and report to the Solicitor General on this issue within a reasonable period.

33) The Committee recommends that the polygraph not be used by the Service for employment screening purposes.

34) The Committee recommends that the Service establish full-time second language training programs in all regions of the country. In particular, the Committee recommends that immediate action be taken by the Service to provide full- time French language instruction to its employees in Toronto and areas west of Toronto.

35) The Committee recommends that the Service make available to its intelligence officers postings in areas of the country where the language of the majority is different than their own language.

36) The Committee recommends that the employees of the Service be given access to all public service competitions and an opportunity to participate in secondment and temporary assignments in the public service.

37) The Committee recommends that the Service recruit from the widest possible population base — that is both within and outside government — for all middle and senior management positions with the Service, while making every effort to identify qualified candidates already inside CSIS who may possess the required qualifications.

38) The Committee recommends that the Solicitor General's Department study the feasibility of extending the RCMP Employee Assistance Program to members of the Service.

39) **The Committee recommends that all persons employed by the Service should have the right to unionize under the *Public Service Staff Relations Act*.**

40) **The Committee recommends that the determination of who in the Service should have the right to strike should be left to the Public Service Staff Relations Board.**

41) **The Committee recommends that the *CSIS Act* or the *Public Service Staff Relations Act* be clarified to confirm that employees of the Service are not to be excluded from collective bargaining under section 2 of the *Public Service Staff Relations Act* as "managerial or confidential" employees only because the employees have access to confidential matters concerning national security.**

42) **The Committee recommends that, to ensure that employees of the Service have the same collective bargaining rights as workers in the rest of the public service, section 9(1) of the *CSIS Act* be repealed.**

43) **The Committee recommends that section 2(*f*) of the *Public Service Staff Relations Act* be repealed, thus recognizing the same collective bargaining, grievance and adjudication rights for all employees of the Service as are granted to workers in the rest of the public service.**

44) **The Committee recommends that section 66(2) of the *CSIS Act* be amended to provide that the benefits accruing to former members of the RCMP be modified or removed only after management has obtained the prior consent of the individual employees concerned.**

45) **The Committee recommends that the *Department of the Solicitor General Act* be amended to give the Solicitor General of Canada a mandate for the direction, control and management of Canada's counter-terrorism program; and that the amendment indicate the lead ministry responsibilities of the Department and, more particularly, those of the National Security Co-ordination Centre and the National Policy Centre.**

46) **The Committee recommends that consideration be given by the Solicitor General to conducting a review within his ministry to establish whether agency heads should report to the minister through a senior deputy minister.**

47) **The Committee recommends that the Solicitor General require the Director of CSIS to provide the Minister with an additional annual report that can be tabled in Parliament.**

48) **The Committee recommends that Section 6(2) of the *CSIS Act* be amended to require the Minister to issue all instructions to the Service in writing. Provision**

should, however, be made for emergency oral instructions. In such circumstances there should be an obligation on the Minister to confirm the instructions so given in writing within 48 hours. The amendment should also require that all instructions be termed 'directions' and be forwarded to SIRC.

49) The Committee recommends that the *CSIS Act* be amended to require the Minister to table a report in Parliament at least once each fiscal year concerning the status of written directions provided to the Service and that the Standing Committee to which it is referred consider the report in an *in camera* session.

50) The Committee recommends that the limits prescribed by section 19 of the *CSIS Act* apply equally to the Solicitor General and to all officials and exempt staff in the Ministry of the Solicitor General having access to information obtained by CSIS in the performance of its duties and functions.

51) The Committee recommends that section 19(2)(*d*) of the *CSIS Act* be amended to permit disclosures to members of the Senate and the House of Commons on the same basis as to ministers of the Crown and to a "person in the public service of Canada".

52) The Committee recommends that section 38(*a*)(ii) of the *CSIS Act* be amended to require SIRC to review ministerial directions, not only with a view to confirming compliance, but also to establish whether the directions provide adequate and appropriate instructions to the Service.

53) The Committee recommends that the *Security Offences Act* not be incorporated into the *Criminal Code*.

54) The Committee recommends that section 5 of the *Security Offences Act* be amended so that a copy of each *fiat* issued is referred to SIRC.

55) The Committee recommends that the federal government continue to pursue, as a matter of urgency, a policing agreement with the Province of Quebec, along the lines of that with the Province of Ontario.

56) The Committee recommends that Section 6(2) of the *Security Offences Act* be amended to require the Solicitor General of Canada 1) to lay before Parliament a copy of every arrangement made under this subsection and 2) to provide the Security Intelligence Review Committee with a copy of each such arrangement.

57) The Committee recommends that the *Security Offences Act* be amended to include a section that permits the Government of Canada to establish a Special Emergency Response Team (SERT).

58) **The Committee recommends that the government give priority to the establishment of a secure courtroom environment for the hearing of warrant applications under the *CSIS Act* or any other matters that involve national security issues.**

59) **The Committee recommends that the inter-departmental technical group established under the direction of the Department of Justice be mandated to review 1) the constitutionality of the warrant provisions of the *CSIS Act* and 2) the applicability of criminal law standards to the adjudication of matters involving the *CSIS Act*.**

60) **The Committee recommends that section 21(4) of the *CSIS Act* be amended to provide statutory protection to solicitor – client communications unless the solicitor is the target of a judicial warrant.**

61) **The Committee recommends that section 21(4) of the *CSIS Act* be amended to provide statutory protection to communications involving innocent third parties.**

62) **The Committee recommends that section 21(4) of the *CSIS Act* be amended to add to the list of warrant limitations those now applied routinely by Federal Court judges.**

63) **The Committee recommends that the length of time for which warrants can be issued and renewed under the *CSIS Act* be reviewed by SIRC and by the Government.**

64) **The Committee recommends that the Governor in Council develop regulations in respect of warrants as provided for under section 28 of the *CSIS Act*.**

65) **The Committee recommends that the *CSIS Act* be amended to provide that security cleared counsel attend before the Federal Court as *amicus curiae* during each warrant application under Part II of the Act.**

66) **The Committee recommends that the Federal Court, in consultation with the Canadian Bar Association, prepare a list of appropriate counsel to take the role of *amicus curiae* during the warrant application process before the Federal Court.**

67) **The Committee recommends that SIRC regularly monitor and report on the use of human sources by CSIS.**

68) **The Committee recommends that the *CSIS Act* be amended to provide that the use of "participant surveillance" may be carried out only under the authority of a judicial warrant as described under Part II of the Act.**

69) **The Committee recommends that the Department of the Solicitor General study the matter of CSIS and the CSE obtaining judicial authorization before using electromagnetic eavesdropping technology for investigative purposes.**

70) **The Committee recommends that the *Canada Post Corporation Act* be amended to provide that the acquisition of information by CSIS, obtained by tracing the names and addresses of persons with whom targets correspond, require judicial authorization.**

71) **The Committee recommends that the *CSIS Act* be amended to provide that SIRC be authorized specifically to compile and analyze warrant statistics and that SIRC be required to publish annually statistics containing the number of Canadian citizens or landed immigrants who have been affected by surveillance powers granted to CSIS under judicial warrants.**

72) **The Committee recommends that the Solicitor General, after consultation with the Inspector General, the Deputy Solicitor General and SIRC, provide a direction detailing what matters are to be included in the Director's Annual Report.**

73) **The Committee recommends that 1) the Inspector General be obliged to consult with the Minister and the Deputy Minister of the Department of the Solicitor General and with SIRC concerning the review priorities of the office; and 2) the Inspector General make all decisions regarding the order of review priorities, which decisions shall be conclusive.**

74) **The Committee recommends that section 30 of the *CSIS Act* be amended so as to make it clear 1) that the primary function of the Inspector General is to establish that the activities of the Service are in compliance with the laws of Canada, ministerial directions, regulations, and operational policies and procedures; 2) that the purpose of the certificate is to indicate compliance or non- compliance by the Service; and 3) that any review conducted under this section be for the purpose of establishing compliance or non-compliance by the Service.**

75) **The Committee recommends that the *CSIS Act* be amended so as to make it obligatory 1) on the part of the Inspector General to forward all reports to the Minister; and 2) for the Solicitor General to forward *all* reports provided by the Inspector General to SIRC.**

76) **The Committee recommends that section 31(2) of the *CSIS Act* be repealed so that the Inspector General has a right of access to all Cabinet documents under the control of the Service.**

77) **The Committee recommends that a copy of all recommendations made by the Inspector General to the Solicitor General be forwarded to SIRC.**

78) **The Committee recommends that section 34 of the *CSIS Act* be amended so as to rename SIRC the "Security *and* Intelligence Review Committee".**

79) **The Committee recommends that section 34 of the *CSIS Act* be amended to set the membership of SIRC at no fewer than five persons.**

80) **The Committee recommends that section 34 of the *CSIS Act* be amended to require the Prime Minister 1) to notify in writing the leaders of each of the parties with more than twelve seats in the House of Commons that an appointment to SIRC is to be made; 2) to request the leaders of each party so notified to put forward a short list of names of persons they believe to be qualified to be a member of SIRC; and 3) to communicate and discuss with the party leaders in the House so as to be apprised of their views on who should be appointed.**

81) **The Committee recommends that the current practice of calling newly appointed SIRC members before the Standing Committee on Justice and Solicitor General be continued.**

82) **The Committee recommends that section 34(3) of the *CSIS Act* be amended to provide that the Chairperson and members of SIRC be eligible to be re-appointed for one term not to exceed five years.**

83) **The Committee recommends that the staggering of appointments to SIRC be continued.**

84) **The Committee recommends that section 38 of the *CSIS Act* be amended so as to make it clear that SIRC has the mandate to monitor and review the effectiveness and efficiency of the Service.**

85) **The Committee recommends that the *CSIS Act* be amended to authorize SIRC to undertake financial reviews of the Service in conjunction with the Auditor General.**

86) **The Committee recommends that section 40 be amended to encompass reviews for compliance by the Service with the *Canadian Charter of Rights and Freedoms* and with the laws of Canada, including provincial laws.**

87) **The Committee recommends that Parliament 1) formally establish the CSE by statute and 2) establish SIRC as the body responsible for monitoring, reviewing**

and reporting to Parliament on the activities of the CSE concerning its compliance with the laws of Canada.

88) **The Committee recommends that Parliament establish SIRC as the body responsible for monitoring, reviewing and reporting to Parliament on the activities of those elements of the RCMP that fulfil the Force's security-related responsibilities concerning their compliance with the laws of Canada.**

89) **The Committee recommends that the Government Security Policy be replaced by regulations to be adopted by the Governor in Council and to be administered by the Treasury Board.**

90) **The Committee recommends 1) that regulations concerning the Government Security Policy (GSP) require the Treasury Board to submit a copy of its reports concerning matters currently identified in the GSP to SIRC at the same time as such reports are submitted to the Cabinet Committee on Security and Intelligence and 2) that SIRC be empowered to request Treasury Board and other departments to supply the Review Committee with such statistical reports as SIRC may consider necessary.**

91) **The Committee recommends that section 39(3) of the *CSIS Act* be repealed so that SIRC has a right of access to all Cabinet documents under the control of the Service.**

92) **The Committee recommends that section 53 of the *CSIS Act* be amended so as to require 1) SIRC to submit its annual report direct to the Speaker of each House of Parliament by September 30th of each year and 2) the Speaker of each House to table the annual report in Parliament within 15 sitting days after having received it.**

93) **The Committee recommends that section 54 of the *CSIS Act* be amended so as to permit SIRC to submit special reports to the Speakers of both Houses at any time for tabling in Parliament.**

94) **The Committee recommends that section 55 of the *CSIS Act* be amended to provide that before determining the content of a statement or report described in that section, SIRC shall consult with the Director of CSIS to ensure compliance with section 37, and that the Review Committee's determination in this regard shall be conclusive.**

95) **The Committee recommends that paragraph 41(1)(a) of the *CSIS Act* be amended to allow complainants to address their concerns directly to SIRC and to give SIRC discretion to advise the Director of CSIS that a complaint has been made.**

96) The Committee recommends that the *CSIS Act* be amended to permit SIRC to initiate its own complaints against the Service.

97) The Committee recommends that section 42 of the *CSIS Act* be amended to allow the Review Committee to receive and investigate a complaint from any individual who, by reason of failure of the Service to complete a security assessment within a reasonable period after a request is received by the Service, is denied employment or is dismissed, demoted, or transferred or denied promotion or transfer, or is denied a contract to provide goods or services to the Government of Canada.

98) The Committee recommends that if the delay by CSIS in providing a security assessment amounts to constructive denial of employment to the complainant, then SIRC may forward a recommendation to a deputy head under section 52 of the *CSIS Act* and that recommendation shall have binding effect upon the deputy head concerned.

99) The Committee recommends that section 42(1) and (2) of the *CSIS Act* be repealed and replaced by:

> **42.(1) When a security clearance, required by the Government of Canada for an individual for any purpose, is denied or is granted at a lower level than that required or is downgraded to a lower level than that required, the deputy head or other person making that decision shall send, within ten days after the decision is made, a notice informing the individual of the denial of a security clearance at the required level, and of the individual's right under this section to complain to the Security Intelligence Review Committee.**

100) The Committee recommends that subsection 52(2) of the *CSIS Act* be amended to provide that SIRC rulings in respect of security clearances are final and binding upon a deputy head.

101) The Committee recommends that the Government study the feasibility of authorizing the Review Committee to provide legal or financial assistance to any person who, it is felt, requires such assistance to present his or her case before the Review Committee.

102) The Committee recommends that the *CSIS Act* be amended so that SIRC may award costs to a complainant who was successful in his or her application before the Review Committee.

103) The Committee recommends that the *Federal Court Act* be amended to provide that, in the event of judicial review, the Federal Court of Appeal have exclusive

jurisdiction under section 28 of the *Federal Court Act*, and that it be entitled to review any SIRC report rendered pursuant to section 42 or any report affecting the rights of an individual rendered pursuant to section 41, together with all relevant documents.

104) The Committee recommends that special procedures be established under the *CSIS Act* and the *Federal Court Act* to enable SIRC files and documents to be transferred to the Federal Court of Appeal without the nature of these documents being made public and, where necessary, without even the existence or absence of such files being acknowledged.

105) The Committee recommends that SIRC be authorized to receive complaints about the conduct of members of the RCMP employed by the Force in national security-related matters but be required to forward such complaints to the RCMP Public Complaints Commission.

106) The Committee recommends that SIRC be empowered to request the RCMP Public Complaints Commission to conduct an investigation into a complaint concerning a national security-related matter.

107) The Committee recommends that the House of Commons Standing Committee on Justice and Solicitor General establish a permanent sub-committee to deal exclusively with security and intelligence matters.

108) The Committee recommends that the functions of the sub-committee be 1) to review the budgets of security and intelligence organizations with a view to providing reports to such committees as the House of Commons may determine; 2) to review the work undertaken by SIRC and the Inspector General; and 3) to undertake reviews of a general nature regarding security and intelligence matters.

109) The Committee recommends that the sub-committee be composed of five members.

110) The Committee recommends that a small, expert, full-time research staff with its own administrative support staff be specially hired to conduct research and to analyze material under the direction of the sub-committee.

111) The Committee recommends that all research and support staff of the sub-committee undergo security assessments and that all senior staff be cleared to the Top Secret Special Activity level and be placed under an appropriate oath.

112) The Committee recommends that the sub-committee meet *in camera* in a secure environment and that all notes and documents relating to its work be retained in a secure environment.

113) The Committee recommends that the Party leaders attempt to ensure continuity, security and integrity in membership on the sub-committee for the duration of a Parliament.

114) The Committee recommends that, before submitting any report to any other committee of the House of Commons or to the House of Commons as a whole, the sub-committee develop procedures to establish whether the release of any information in such reports could pose a threat to the security of Canada.

115) The Committee recommends that, in the event that the Standing Committee on Justice and Solicitor General decides not to establish a sub-committee on security and intelligence, section 56 of the *CSIS Act* and section 7 of the *Security Offences Act* be re-enacted to provide for another parliamentary review five years after the tabling of this Report.

116) The Committee recommends that, in the event Parliament opts for another five-year review, the *CSIS Act* and *Security Offences Act* be amended to provide that the Committee established for the purposes of conducting such a review

1) have access to any information under the control of the Service that relates to the performance of the duties and functions of the Committee and be entitled to receive from the Director and employees such information, reports and explanations as the Committee deems necessary for the performance of those duties and functions;

2) have the obligation to submit its final report to Parliament, not within a predetermined time limit, but only at such a time as the Committee considers appropriate; and

3) have its staff security cleared before the start of the review.

117) The Committee recommends that Parliament adopt a *National Security Act*, which would incorporate the *CSIS Act*, the *Security Offences Act* and any other legislation necessitated by the implementation of the recommendations set out in this Report.

APPENDIX A

Witnesses

Assembly of First Nations
- Georges Erasmus, National Chief (Issue 13)

British Columbia Civil Liberties Association
- Philip Bryden, Vice-President
- Patrick Smith, Member (Issue 22)

British Columbia Law Union
- Brenda Gaertner, Member
- Craig Paterson, Member
- Don Stewart, Member (Issue 23)

Brodeur, Jean-Paul
- University of Montreal (Issue 10)

Canada Employment and Immigration Commision
- Charles Belford, Director Control and Enforcement Policy, Immigration Policy (Issue 35)

Canadian Association of University Teachers
- Pamela Smith, President
- Donald Savage, Executive Director
- Alan Andrews, Person Chairing Academic Freedom and Tenure Committee (Issue 10)

Canadian Civil Liberties Federation
- Bill Rafoss, Board Member (Issue 9)

Canadian Civil Liberties Association
- A. Alan Borovoy, General Counsel
- Keneth P. Swan, Vice President and Chairman of the Board (Issue 8)

Canadian Jewish Congress
- Dr. Eli Rabin, Ottawa Jewish Community Council Representative on the National Officers Body
- Manuel Prutschi, National Director of the Joint Community Relations Committee
- Eric Vernon, Director of the Law and Social Action Committee (Issue 18)

Canadian Physicians for the Prevention of Nuclear War
Dr. Mary-Wynne Ashford, President (Issue 23)

Canadian Security Intelligence Service
Reid Morden, Director (Issue 2) (Issue 3) (Issue 34) (Issue 35)
Eric Brick, Director General Security Screening (Issue 35)

Canadian Security Intelligence Service Employees' Association
Paul Gibson, President (Issue 21)

Canadian Security Intelligence Service Employees' Association (Quebec Region)
Bernard Marentette, Representative (Issue 36)

Canadian Bar Association
John R. R. Jennings, President
Terence Wade, Director Legislation and Law Reform
Albert Strauss, Chairman C.B.A. Special Committee on CSIS
Donald Bishop, Member C.B.A. Special Committee on CSIS (Issue 15)

Charters, David, Director,
Centre for Conflict Studies,
University of New Brunswick (Issue 12)

Crelinsten, Ronald
Department of Criminology
University of Ottawa (Issue 12)

Czechoslovak Association of Canada
George Corn, Honorary and Past President
Victor M. Fic, Vice-President (Issue 18)

Kealey, Greg
Department of History
Memorial University (Issue 29)

Department of the Solicitor General
The Honourable Pierre Blais
Ian Glen, Assistant Deputy Solicitor General
James Lahey, Director General (Issue 2)
Richard Thompson, Inspector General (Issue 5)
Joseph Stanford, Deputy Solicitor General (Issue 6)

Fletcher, Joseph (Issue 8)

Griffiths, Franklyn
Department of Political Science
University of Toronto (Issue 33)

Public Service Alliance of Canada
Daryl T. Bean, National President
Lynn Ray, National President
Union of Solicitor General Employees (Issue 21)

Rankin, Murray
Faculty of Law
University of Victoria (Issue 24)

Royal Canadian Mounted Police
Norman D. Inkster, Commissioner
P.M. Cummings, Chief Superintendent (Issue 7)

Royal Canadian Mounted Police Public Complaints Commission
Dr. Richard Gosse, Chairman and Former Inspector General of CSIS (Issue 17)

Russell, Peter
Director of Graduate Studies
Department of Political Science
University of Toronto (Issue 32)

Seaborn, Blair
Former Intelligence and Security Co-ordinator, Privy Council Office (Issue 16)

Security Collective of the Law Union of Ontario
Paul D. Copeland (Issue 31)

Security Intelligence Review Committee
Maurice Archdeacon, Executive Secretary (Issue 2)
The Honourable Ron Atkey, Chairman
The Honourable Jean-Jacques Blais, Member
The Honourable Saul Cherniack, Member
The Honourable Frank McGee, Member
The Honourable Paule Gauthier, Member (Issue 4)

Shore, Jacques (Issue 31)

Sikh Professional Association of Canada
Suresh Singh Bhalla
Executive Director and Secretary (Issue 20)

Starnes, John, Former Director General
RCMP Security Service (Issue 14)

Stevens, Dr. Harry
Director, Psychology and Law Institute
Simon Fraser University (Issue 22)

Treasury Board of Canada
Gerald Bethell, Director of Information Management Practices,
Administrative Policy Branch (Issue 35)

Victoria Civil Liberties Association
Dr. Tom Gore, President (Issue 24)

Whitaker, Reg
Department of Political Science
York University (Issue 29)

World Sikh Organization
Karnail Singh Gill, Director of Administration
Attar Singh Chawla, Director of Finance (Issue 10)

Yuille, Dr. John C.
Department of Psychology
University of British Columbia (Issue 23)

APPENDIX B

Submissions Received

The Committee received briefs from the following groups and individuals.

Armenian, Dr. Atken
Toronto, Ontario

Armenian Catholic Community of Toronto
Toronto, Ontario

Assembly of First Nations
Ottawa, Ontario

Barr, Archie
Ottawa, Ontario

British Columbia Civil Liberties Association
Vancouver, British Columbia

British Columbia Law Union
Vancouver, British Columbia

Brodeur, Jean-Paul
Montreal, Quebec

Cain, Dr. Frank
Campbell, Australia

Callwood, June
Toronto, Ontario

Canadian Association of University Teachers
Ottawa, Ontario

Canadian Bar Association
Toronto, Ontario

Canadian Civil Liberties Association
Toronto, Ontario

Canadian Council for Peace in Freedom
Ottawa, Ontario

Canadian Defence Preparedness Association
Ottawa, Ontario

Canadian Human Rights Commission
Ottawa, Ontario

Canadian Jewish Congress
Montreal, Quebec

Canadian Physicians for the Prevention of Nuclear War
Victoria, British Columbia

Canadian Rights and Liberties Federation
Ottawa, Ontario

Canadian Security Intelligence Service Employees' Association
Ottawa, Ontario

Canadian Security Intelligence Service Employees' Association, Quebec Region
Ottawa, Ontario

Case "A" SIRC complainant

Case "B" SIRC complainant

Case "C" SIRC complainant

Case "D" SIRC complainant

Case "E" SIRC complainant

Case "F" SIRC complainant

Charters, Dr. David
Fredericton, New Brunswick

Civil Liberties Commission of the Ukranian Canadian Congress
Winnipeg, Manitoba

Cline, Ray S.
Washington, D.C.

Crelinston, Ronald D.
Ottawa, Ontario

Cummings, Richard
Ottawa, Ontario

Czechoslovak Association of Canada
Toronto, Ontario

Doidge, Terence R.
Don Mills, Ontario

Fleming, Wayne
Toronto, Ontario

Fletcher, Professor Joseph
Toronto, Ontario

Fraser, Eon
Ottawa, Ontario

Gill, Peter
Liverpool, England

Groebel, Jo
Rhineland–Pfalz, FRG

Hoffman, Bruce
Santa Monica, California

Information Commissioner of Canada
Ottawa, Ontario

Islamic Propagation Centre
Toronto, Ontario

Kavchak, Andrew
Ottawa, Ontario

Law Reform Commission of Canada
Ottawa, Ontario

Law Union of Ontario
Toronto, Ontario

Mackenzie Institute
Toronto, Ontario

Macklon, William
Lethbridge, Alberta

Morcos, Lore
Ottawa, Ontario

Moschanski, B. Dan
Montreal, Quebec

National Association of Canadians of Origins in India
Ottawa, Ontario

Privacy Commissioner of Canada
Ottawa, Ontario

Public Service Alliance of Canada
Ottawa, Ontario

Rankin, Murray
Victoria, British Columbia

Registrar of Canadian Citizenship
Ottawa, Ontario

Saltstone, Scot Paul
Sudbury, Ontario

Schulman, Perry
Winnipeg, Manitoba

Security Intelligence Review Committee
Ottawa, Ontario

Shore, Jacques
Montréal, Quebec

Sikh Professional Association of Canada (Brian McAndrew and Zuhair Kashmeri)
Toronto, Ontario

Strategic Studies Program, University of Manitoba
Winnipeg, Manitoba

Sylvain, Gaston
Quebec, Quebec

Ukrainian Canadian Committee National
Winnipeg, Manitoba

Victoria Civil Liberties Association
Victoria, British Columbia

Weller, Geoffrey P.
Thunder Bay, Ontario

Whitaker, Professor Reg
Toronto, Ontario

World Sikh Organization
Ottawa, Ontario

REQUEST FOR GOVERNMENT RESPONSE

In accordance with Standing Order 109, the Committee requests that the government provide a comprehensive response to this Report within one hundred fifty (150) days.

A copy of the relevant Minutes of Proceedings and Evidence of the Special Committee on the Review of the *Canadian Security Intelligence Service Act* and the *Security Offences Act*, (Issue Nos. 1 to 36 and 37 which includes this Report), is tabled.

Respectfully submitted

Blaine Thacker
Chairman

MINUTES OF PROCEEDINGS

TUESDAY, JUNE 12, 1990
(59)

The Special Committee on the Review of the Canadian Security Intelligence Service Act and the Security Offences Act met *in camera* at 9:52 o'clock a.m. this day, in Room 308 West Block, the Chairman, Blaine Thacker, presiding.

Members of the Committee present: Ken Atkinson, John Brewin, Derek Lee, Wilton Littlechild, George Rideout, Jacques Tétreault and Blaine Thacker.

In attendance: *From the Research Branch of the Library of Parliament*: Philip Rosen, Senior Analyst. *From the Committee Research Staff*: Stuart Farson, Research Consultant.

The Committee resumed consideration of its Order of Reference dated Tuesday, June 27, 1989. (*See Minutes of Proceedings and Evidence of Tuesday, September 26, 1989, Issue No. 1*).

The Committee resumed consideration of its draft Report.

At 1:12 o'clock p.m., the Committee adjourned to the call of the Chair.

WEDNESDAY, JUNE 13, 1990
(60)

The Special Committee on the Review of the Canadian Security Intelligence Service Act and the Security Offences Act met *in camera* at 4:00 o'clock p.m. this day, in Room 307 West Block, the Chairman, Blaine Thacker, presiding.

Members of the Committee present: Ken Atkinson, John Brewin, Derek Lee, George Rideout and Blaine Thacker.

In attendance: *From the Research Branch of the Library of Parliament*: Philip Rosen, Senior Analyst. *From the Committee Research Staff*: Stuart Farson, Research Consultant; Brian Gorlick and François Cadieux, Research Associates.

The Committee resumed consideration of its Order of Reference dated Tuesday, June 27, 1989. (*See Minutes of Proceedings and Evidence of Tuesday, September 26, 1989, Issue No. 1*).

The Committee resumed consideration of its draft Report.

At 6:05 o'clock p.m., the sitting was suspended.

At 7:16 o'clock p.m., the sitting resumed.

At 10:38 o'clock p.m., the Committee adjourned to the call of the Chair.

TUESDAY, JUNE 26, 1990
(61)

The Special Committee on the Review of the Canadian Security Intelligence Service Act and the Security Offences Act met *in camera* at 4:18 o'clock p.m. this day, in Room 536 of the Wellington Building, the Chairman, Blaine Thacker, presiding.

Members of the Committee present: Ken Atkinson, John Brewin, Derek Lee, Wilton Littlechild, George Rideout, Blaine Thacker and Maurice Tremblay.

In attendance: *From the Research Branch of the Library of Parliament*: Philip Rosen, Senior Analyst. *From the Committee Research Staff*: Stuart Farson, Research Consultant; Brian Gorlick and François Cadieux, Research Associates.

The Committee resumed consideration of its Order of Reference dated Tuesday, June 27, 1989. (*See Minutes of Proceedings and Evidence of Tuesday, September 26, 1989, Issue No. 1*).

The Committee resumed consideration of its draft Report.

At 4:30 o'clock p.m., the sitting was suspended.

At 4:42 o'clock p.m., the sitting resumed.

At 6:00 o'clock p.m., the sitting was suspended.

At 8:00 o'clock p.m., the sitting resumed.

At 10:10 o'clock p.m., the Committee adjourned to the call of the Chair.

WEDNESDAY, JUNE 27, 1990
(62)

The Special Committee on the Review of the Canadian Security Intelligence Service Act and the Security Offences Act met *in camera* at 10:31 o'clock a.m. this day, in Room 701 of the Promenade Building, the Chairman, Blaine Thacker, presiding.

Members of the Committee present: Ken Atkinson, John Brewin, Derek Lee, George Rideout, Blaine Thacker and Maurice Tremblay.

In attendance: *From the Research Branch of the Library of Parliament*: Philip Rosen, Senior Analyst. *From the Committee Research Staff*: Stuart Farson, Research Consultant; Brian Gorlick and François Cadieux, Research Associates.

The Committee resumed consideration of its Order of Reference dated Tuesday, June 27, 1989. (*See Minutes of Proceedings and Evidence of Tuesday, September 26, 1989, Issue No. 1*).

The Committee resumed consideration of its draft Report.

At 12:37 o'clock p.m., the sitting was suspended.

At 12:51 o'clock p.m., the sitting resumed.

It was agreed, — That the Committee engage the services of an English text reviser/editor to prepare the finished English text of the Committee's report at an amount not to exceed $4,000.

It was agreed, — That the Chairman be authorized to extend, on behalf of the Committee, the contracts with Stuart Farson, Senior Research Consultant and with Brian Gorlick and François Cadieux, Research Associates to July 13, 1990.

At 2:02 o'clock p.m., the sitting was suspended.

At 3:47 o'clock p.m., the sitting resumed.

At 7:40 o'clock p.m., the Committee adjourned to the call of the Chair.

WEDNESDAY, JULY 11, 1990
(63)

The Special Committee on the Review of the Canadian Security Intelligence Service Act and the Security Offences Act met *in camera* at 9:55 o'clock a.m. this day, in Room 536 of the Wellington Building, the Chairman, Blaine Thacker, presiding.

Members of the Committee present: Ken Atkinson, John Brewin, Wilton Littlechild, George Rideout and Blaine Thacker.

In attendance: *From the Research Branch of the Library of Parliament*: Philip Rosen, Senior Analyst. *From the Committee Research Staff*: Stuart Farson, Research Consultant; Brian Gorlick and François Cadieux, Research Associates.

The Committee resumed consideration of its Order of Reference dated Tuesday, June 27, 1989. (*See Minutes of Proceedings and Evidence of Tuesday, September 26, 1989, Issue No. 1*).

The Committee resumed consideration of its draft Report.

It was agreed, — That the draft Report, entitled *In Flux, But Not in Crisis*, be adopted and that the Chairman be authorized to make such editorial changes as may be necessary without changing the substance of the draft Report.

It was agreed, — That pursuant to Standing Order 109, the Committee request the Government to table a comprehensive response to the Report.

It was agreed, — That the Chairman present the Committee's Report to the House.

It was agreed, — That the confidential case materials, *in camera* transcripts, research staff interview notes and other like material received or prepared by the Committee be destroyed.

It was agreed, — That the Chairman, at his discretion, be authorized to pay reasonable travelling expenses to bring the contract researchers (in Canada) to Ottawa during the time when the Report is presented to the House of Commons.

At 4:30 o'clock p.m., the Committee adjourned to the call of the Chair.

Charles Robert
Clerk of the Committee