Solicitor General Canada
Solliciteur général Canada

ON COURSE

NATIONAL SECURITY FOR THE 1990s

ON COURSE:

NATIONAL SECURITY FOR THE 1990s

The Government's Response

to the Report of the House of Commons
Special Committee
on
the Review of the Canadian Security Intelligence Service Act
and the Security Offences Act

February 1991

Solicitor General Canada | Solliciteur général Canada

Canada

Minister of Supply and Services Canada 1991
Cat. No. JS42-47/1991
ISBN 0-662-58112-1

ON COURSE:
NATIONAL SECURITY FOR THE 1990s

TABLE OF CONTENTS

FOREWORD

In 1984, the Canadian Security Intelligence Service (CSIS) Act and the Security Offences Act established a new legislative framework to govern Canada's national security system. The legislation stipulated that a parliamentary review of the new arrangements would be undertaken five years after their coming into force. In June 1989, that review was assigned to a Special Committee of the House of Commons, under the chairmanship of Mr. Blaine Thacker, M.P., and the Committee issued its report In Flux but not in Crisis on September 24, 1990. Under the rules of Parliament, the Government is required to respond to committee reports within 150 days. On Course constitutes the Government's response.

The Special Committee was presented with a challenging task. It was given a year to conduct "a comprehensive review of the provisions and operation" of complex legislation which had created a number of new institutions. Moreover, it was required to form judgments on difficult and sensitive issues without direct access to all the documents it felt it needed.

Successive governments have consistently recognized an obligation to adhere to certain principles with respect to the disclosure of information. These have included the right of individuals to privacy, the confidentiality of officials' advice to Ministers, and the protection of national security. Notwithstanding this obligation, the Government conveyed an unprecedented amount of security-related information to the Special Committee through both public and in camera testimony by government officials, and through extensive written responses to questions. On Course underscores the Government's commitment to openness by providing still more information on the national security system.

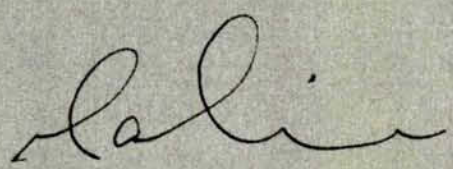
The Special Committee produced a report of considerable depth and sophistication. I am pleased to note that it concluded a separate civilian security service is in the best interests of Canadians, that it believes our new national security system to be essentially sound, and that it found no violations of the rights and freedoms of Canadians. The Committee, however, also identified a number of issues that deserve attention, and it offered some useful recommendations for addressing these. I take this opportunity to thank the Special Committee for its report.

On Course sets out, for the first time in a comprehensive manner, how the 1984 legislation has been implemented and how the national security system now functions. It also addresses the major issues raised by the Special Committee, and responds directly or indirectly to most of the recommendations made by the Special Committee. Its purpose is to explain how the control, accountability, and review arrangements work in practice, and thereby to assure Parliament and the public that a high degree of confidence in these arrangements is warranted.

There may be reasons to open the two Acts for amendment in the future, given evolving jurisprudence and the continuing development of the new system. But the Government does not believe legislative changes are required at present. In many cases where the Special Committee has recommended amendments to deal with issues, the Government believes further policy development would address the concerns raised. In other cases, further review of the functioning of the national security system is required before definitive judgments can be made. The Government does not favour altering the intricate system of checks and balances established by the Acts. So far, these have served Canadians well in ensuring effective national security with due regard for the fundamental rights of individuals. But confidence in the system can be improved by providing Parliament with more information on security issues.

A major theme of the report of the Special Committee was that there must be a continuing process of building confidence with Parliament and the public in the security sector. The Government agrees fully and is committed to working with the Standing Committee to achieve this end. The ways in which the Government intends to pursue this objective are outlined in Chapter X, entitled "Parliament and the Public".

In the years to come, the Government will be examining how the system put in place in 1984, with its careful balance of powers and controls, might be further developed in the direction Parliament intended. We are "on course", and the Government will arrange for another Parliamentary review of our progress in 1998.



Pierre H. Cadieux
Solicitor General of Canada

CHAPTER I: NATIONAL SECURITY FOR THE 1990s

Every nation, even one as privileged by geography and history as Canada, needs a system to protect its national security.

Canadians have not often thought of their country as exposed or vulnerable. Vast oceans, and the presence of a friendly military power next door, have provided Canadians with a large measure of immunity from the troubles which have afflicted other parts of the globe. Moreover, Canada is a relatively prosperous society with a tradition of promoting and protecting democratic rights and freedoms, and seeking peaceful resolution of conflicts.

But Canada's security has been more than just an outcome of geography and history. Collective security arrangements through NATO and NORAD, and an active diplomacy, have played important roles. So too have those agencies of government charged with internal security. Since the end of the World War II, Canada has been the target of a large number of foreign intelligence services, and more than 100 individuals from a dozen countries have been expelled for security-related activities since the early 1950s. During the same period, the incidence of terrorism involving Canada and Canadians has been on the rise, and a silent war has been waged against it.

The World of the 1990s

As Canadians look to the future, there is cause for hope but not complacency. The transformations underway provide reason to hope for reduced threats to national security. But uncertainty and volatility are characteristic of periods of international transition.

- Terrorism rooted in longstanding disputes, such as those to be found in the Gulf, in other parts of the Middle East, on the Indian sub-continent, and in Northern Ireland, will still be for export including to North America.

- Throughout the world, rising expectations, political vendettas, longstanding territorial disputes, and the acquisition of advanced weapons systems by despotic regimes offer little assurance that universal peace will prevail.

- International competition for scarce resources and advanced technology, including weapons development, will continue to lead some states to try to acquire what they want through espionage.

- In the Soviet Union, revolutionary change has yet to run its course. The USSR has few democratic traditions to fall back on, the country is in desperate economic straits, and reforms have unleashed discontent which could reverse the course of perestroika. Meanwhile, the USSR remains one of the world's foremost military powers and maintains a vast foreign intelligence service.

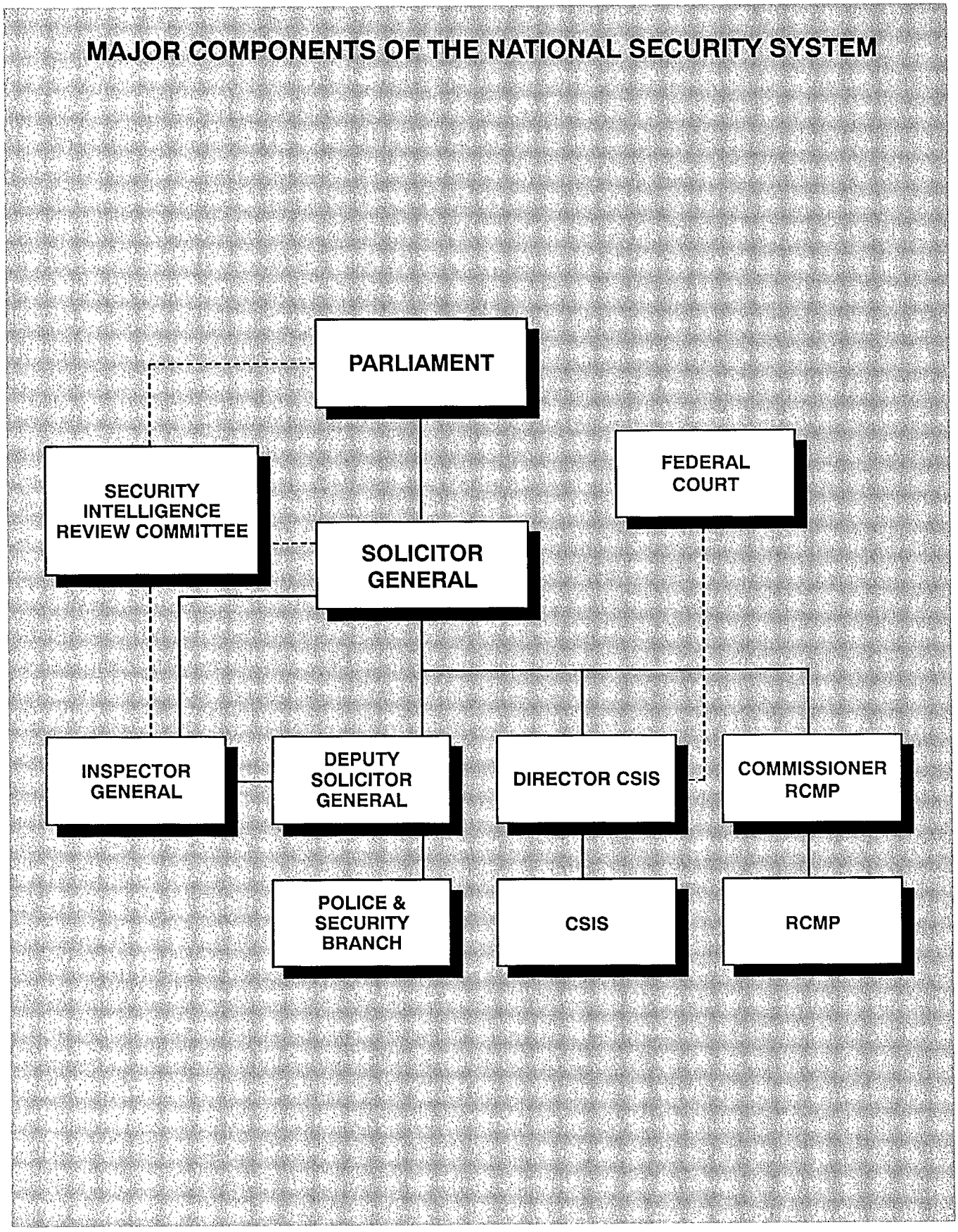
- In Eastern Europe, democratization has given expression to old antagonisms and national aspirations, generating the potential for instability of a kind not seen since the 1930s.

Meanwhile, domestic politically motivated violence is not unknown in Canada. In the past, hate groups and extremists of various persuasions have adopted violent means to vent their anger against minorities and government institutions. The events of the summer of 1990 suggest some groups are also prepared to use violence to achieve their political ends.

With the future an uncertain one, Canadians will continue to require a security system able to combat terrorism, defeat espionage activities, and preserve and protect their democratic way of life.

Canada's National Security System

In Canada, many departments and agencies have responsibilities for national security. Foremost among these is the Department of the Solicitor General and its agencies. Other departments of Government also have important responsibilities for national security not dealt with in this report. These include the Privy Council Office, and the Departments of External Affairs, National Defence, Transport and Employment and Immigration.


MAJOR COMPONENTS OF THE NATIONAL SECURITY SYSTEM
PARLIAMENT
SECURITY INTELLIGENCE REVIEW COMMITTEE
FEDERAL COURT
SOLICITOR GENERAL
INSPECTOR GENERAL
DEPUTY SOLICITOR GENERAL
DIRECTOR CSIS
COMMISSIONER RCMP
POLICE & SECURITY BRANCH
CSIS
RCMP

The national security system established by the CSIS Act and the Security Offences Act of 1984 sought to reflect the values and aspirations of Canadian society. Embodied in the legislation was a set of interlocking principles to shape and guide the operation of the system. Each principle can be associated with one of its major participants.

- A Minister of the Crown, the Solicitor General, is responsible for the effective operation of the national security system.

- The Deputy Solicitor General provides informed and impartial advice and assistance to the Minister.

- The Inspector General conducts independent internal reviews for the Minister.

- The Director of the Canadian Security Intelligence Service is responsible for the control and management of the Service.

- CSIS has a precise mandate which is defined in legislation.

- The RCMP is responsible for security enforcement and protective security.

- The Service's use of certain intrusive techniques is subject to a requirement for prior judicial authorization.

- The Security Intelligence Review Committee (SIRC) conducts independent external reviews for the Minister and for Parliament.

- Parliament is to conduct a comprehensive review of the provisions and operation of the two Acts after five years.

Security Intelligence and Law Enforcement

Canada's national security model is unique, though elements of it can be found in other democratic societies. Its design stemmed from dissatisfaction in the 1970s with the operations of the RCMP Security Service. In the early 1980s, the decision was taken to separate the security intelligence function from the RCMP and replace the RCMP Security Service with a civilian security intelligence agency. The new Canadian Security Intelligence Service (CSIS) would concentrate on collecting,

analyzing and reporting on security information and intelligence; the RCMP would concentrate on security enforcement and protective security.

The purpose of security intelligence is to provide timely advice on threats, so that action can be taken to deal with them before they harm national security - such as the murder of a visiting foreign leader, the bombing of an embassy, the hijacking of an airliner, the recruitment of a government official to supply classified documents, or the inappropriate influencing of the political process. To perform this function effectively, a security intelligence agency needs to be engaged early, in order to detect and monitor activity which could reasonably be suspected to constitute a threat to the security of Canada.

Separating the function of collecting intelligence on threats to security from the function of enforcing the law recognized the distinctive character of each function, and the distinctive controls appropriate to each. Effective security intelligence requires a security intelligence agency to work closely with the government, in order to receive direction and report findings. The enforcement of laws, on the other hand, requires a police agency to be independent from government interference in specific investigations. The two must work together, however, if the security system is to function effectively.

Balancing Security and Freedom

In adopting the new framework in 1984, Parliamentarians were conscious of the need both to protect Canadians from threats to their security and to preserve their fundamental freedoms. Accordingly, the legislation incorporated a clear mandate and strict controls on the activities of the new Service. The inclusion of Ministerial oversight and sophisticated review mechanisms ensured that the Service would be effective and that the rights of individuals would be respected. Balance was a distinguishing feature of the legislation.

- The need to protect national security was balanced by respect for individual rights and freedoms.

- The need to provide the Service with sufficient powers to produce effective security intelligence was balanced by statutory controls and policy direction.

- The need for CSIS to employ certain intrusive techniques was balanced by the requirement for prior authorization by a Minister of the Crown and the Federal Court.

- The need for secrecy was balanced by Ministerial accountability and informed independent review.

On Course

The new system has now been in place for over six years, long enough to determine whether it is essentially workable. What follows is a detailed presentation on how the system has been working - the most detailed presentation ever made public by the Government. It draws on the Government's own experience with the system, reports over several years by the Inspector General and the Security Intelligence Review Committee, the report of the Osbaldeston Independent Advisory Team, and most recently the analysis and insights of the Special Committee. The conclusion reached is that the system is sound, has served the nation well and should be preserved. Though some refinements can be contemplated and policy development continues, the framework created by the Acts has proven to be both durable and flexible in times of change.

CHAPTER II: THE SOLICITOR GENERAL AND MINISTERIAL RESPONSIBILITY

A Minister of the Crown, the Solicitor General, is responsible for the effective operation of the national security system.

The Solicitor General is responsible for the effective operation of the national security system established by the CSIS Act and Security Offences Act, and for certain aspects of Canada's criminal justice system. Five major corporate entities, each managed by an official of deputy rank, comprise the main agencies of the Ministry of the Solicitor General. Four of these have direct operational responsibilities:

- the Canadian Security Intelligence Service;
- the Royal Canadian Mounted Police;
- the Correctional Service of Canada; and
- the National Parole Board.

A fifth entity, the Ministry Secretariat, headed by the Deputy Solicitor General, provides advice and assistance to the Solicitor General in discharging the full range of his or her responsibilities.

The most important of the Minister's responsibilities are:

- providing direction to the agencies of the Ministry;
- exercising national leadership in security, policing, law enforcement, corrections and conditional release; and
- answering in Parliament.

The National Security System

The three elements of the national security system for which the Solicitor General is responsible are: security intelligence, security enforcement, and protective security. The first reflects the mandate of CSIS, the latter two the security mandate of the RCMP. As a consequence of the Minister's security responsibilities, the Solicitor General is also the lead Minister for counter-terrorism arrangements in Canada.

Since the passage of the CSIS Act and the Security Offences Act in 1984, the national security system put in place by that legislation has evolved to the point of maturity. CSIS has emerged as a responsible security intelligence agency, on a professional par with those of other Western democracies. Similarly, the RCMP has maintained its customary high standards in discharging its responsibilities for national security. The review mechanisms created by the Acts have developed and refined their ability to investigate and report.

Ministerial Control and Accountability

The principles of Ministerial control and accountability are central to Canadian parliamentary democracy. The CSIS Act ensured that the Minister would have full knowledge and power of direction over the policies, operations and management of CSIS. Subsection 6(1) of the CSIS Act is unequivocal in its message that the Minister provides direction to the Director of the Service. The CSIS Act also supplied the Minister with the means to control and guide the Service. The Minister's responsibility for the RCMP is set out in the RCMP Act, with the Security Offences Act confirming the security responsibilities of the RCMP.

Ministerial control is to be distinguished from Ministerial accountability. Though they are sometimes used interchangeably, the terms have distinct meanings. The Special Committee noted the importance of this distinction in the security intelligence context.

Control refers to the Minister's power of approval, the Minister's ability to set policy and give direction, and the means at the Minister's disposal to ensure decisions are implemented. Accountability refers to the Minister's obligation to answer before Parliament, and the duty of officials to answer to the Minister.

A principal means by which the Minister exercises control over CSIS is through the power of approval. By the normal rules of government, a Minister must be consulted on all important matters related to the Minister's portfolio. In addition, the CSIS Act and

Ministerial directions issued to the Service require the Minister personally to approve a wide variety of operational activities, particularly sensitive operations. The CSIS Act stipulates that the Minister must personally approve:

- all applications for judicial warrants;
- all CSIS arrangements with other federal agencies and departments, provincial authorities, and foreign governments; and
- the Service's assistance in the collection of foreign intelligence in Canada.

Ministerial Direction

The Minister also exercises control over the Service through statutory power to establish the policy guidelines for the Service. This is achieved through the issuance of Ministerial directions.

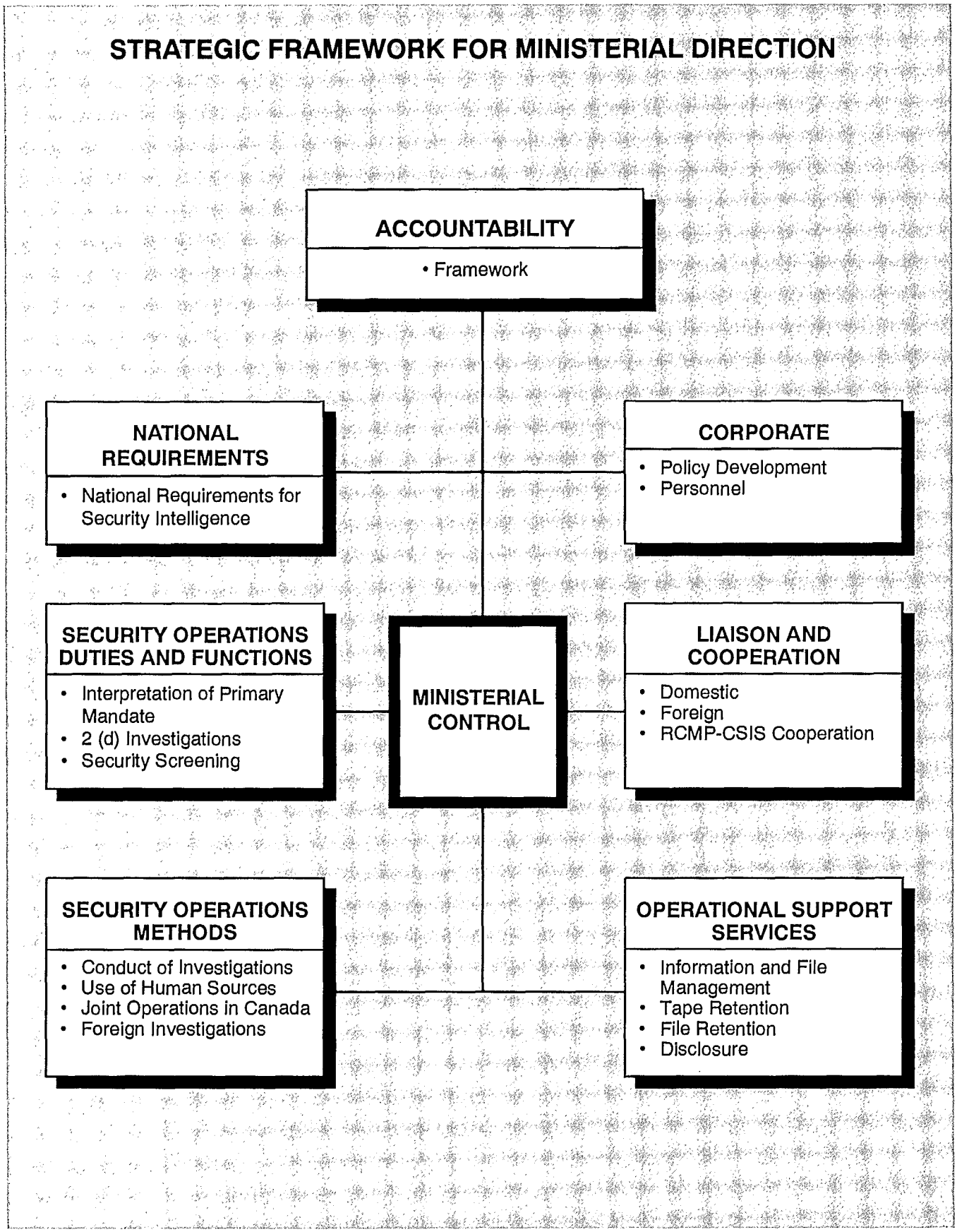
An act of Parliament can construct a legislative framework, but legislation alone cannot provide detailed guidance covering every aspect of operational activity. For this, there needs to be a policy framework to assist interpretation and implementation. Legislation governing the creation of a security intelligence agency has a special need for such a policy framework, if there is to be public confidence in how the agency operates.

Policy frameworks in support of legislation are normally achieved in two ways: through the promulgation of regulations and/or the development of operational guidelines. Neither mechanism, however, is entirely satisfactory in the security intelligence context. Regulations are public instruments and obviously unsuited for conveying detailed instructions on how secret operations are to be conducted. Internal agency rules, on the other hand, would not provide a sufficient level of confidence.

A third device was therefore embodied in the legislation, in the form of Ministerial direction issued pursuant to subsection 6(2) of the Act. Ministerial direction helps to ensure that the Solicitor General is the linchpin in the legal and policy framework.

In practice, the Minister issues all instructions of consequence in written form regardless of subject. Through the experience of working with the CSIS Act, the Government now defines direction pursuant to subsection 6(2) as "written instructions of a continuing nature, issued at the prerogative of the Minister, that relate to policies, standards or procedures".

STRATEGIC FRAMEWORK FOR MINISTERIAL DIRECTION



Strategic Framework for Ministerial Direction

Over the last six and a half years, a set of Ministerial directions has been developed setting out the Solicitor General's governing principles for the Service and its activities.

The directions may be grouped into seven major categories relating to:

- arrangements to assist the Director's accountability to the Minister.
- the Government's annual priorities for intelligence on threats to Canada's security, known as the "national requirements";
- guidance on the Service's statutory duties and functions;
- guidance on investigative methods and techniques;
- instructions dealing with the Service's corporate management practices;
- standards for negotiating cooperative arrangements with domestic and foreign organizations; and
- policy on file management issues, particularly the Service's retention of files inherited from the RCMP Security Service.

Key direction within each category is outlined in the sections below.

There are currently some 50 Ministerial directions in effect. These are being consolidated into fewer directions having a strategic, as distinct from case-originated, focus. New directions are also being developed to complete the framework. Directions are converted by the Service into operational procedures for use directly by CSIS staff. This logical progression from statute to Ministerial direction to operational procedure provides a managed and auditable means of ensuring that the Service is fulfilling its duties and functions in an appropriate manner.

Accountability

A general direction exists to ensure the Director's accountability to the Minister. It describes the roles and responsibilities of the Solicitor General, the Deputy Solicitor

General and the Director, and outlines formal reporting requirements, such as the Director's obligation to prepare an Annual Report. The Minister has also established guidelines for the scope and content of the Director's Annual Report.

National Requirements for Security Intelligence

In light of the constantly changing security environment, the Government must regularly provide the Service with guidance on its requirements for security intelligence. Accordingly, a national threat assessment is prepared annually, identifying emerging issues and trends, on the basis of which national security requirements are determined for the year ahead. Currently, five areas of particular national interest have been identified as priorities for CSIS.

- **Public Safety:** the ability of Canadians to engage in ordinary social activity without fear of harm, including the safety of air transportation.

- **The Integrity of Canada's Democratic Process:** the functioning of those institutions, rights and freedoms fundamental to the well-being of Canada's democratic society.

- **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.

- **Economic Security:** the conditions necessary to sustain a competitive international position for Canada, to provide productive employment, and to contain inflation.

- **International Peace and Security:** the ability of the international system to evolve peacefully and assure Canada's continued security.

In view of events in Europe and the Middle East, and growing international economic competition, CSIS will have a special responsibility over the next few years to assess how external events might affect national security. The increased difficulty in future of identifying threats to the security of Canada in an accurate and timely manner will demand effective and responsive security intelligence collection.

Security Operations

Direction on Service operational policy in respect of the Service's security intelligence mandate is particularly important to Ministerial control. It ensures that the Service's collection, analysis and reporting activities respond to the Government's annual national requirements for security intelligence, and provides practical guidance in interpreting important terminology of the CSIS Act. These issues are discussed further in Chapter V.

The Minister has also provided specific direction relative to the threat of "subversion". As a rule, CSIS must rely on open published information in investigating any such threat, and must seek Ministerial approval before it may use intrusive collection techniques when the severity of the threat in this area dictates their use.

Directions on security screening outline special procedures for conducting citizenship, immigration and government employment security assessments. These require that the Solicitor General be consulted on all negative recommendations regarding citizenship and immigration, and that the Director personally approve any negative recommendation concerning security assessments relative to Government employment.

Operational Methods

A general direction on the conduct of investigations serves as an "umbrella" for other more specific directions providing guidance on operational methods. It explicitly endorses the five "fundamental principles" for controlling investigations espoused by the McDonald Commission.

- The rule of law must be observed.

- The investigative means used must be proportionate to the gravity of the threat posed and the probability of its occurrence.

- The need to use various investigative techniques must be weighed against possible damage to civil liberties or to valuable social institutions.

- The more intrusive the technique, the higher the authority required to approve its use.

- Except in emergency circumstances, the least intrusive techniques of information collection must be used before more intrusive techniques.

In addition to the principles governing the conduct of investigations, a direction on the use of human sources in investigations enjoins the Service to use human sources in accordance with the following criteria.

- Human sources are to be used only when and to the extent it is reasonable and necessary to do so in meeting the Service's statutory responsibilities.

- The need to use a source must be carefully weighed against possible damage to civil liberties.

- Given the intrusiveness of this investigative technique, the use of sources must be centrally controlled.

- Sources are to carry out their tasks without engaging in illegal activities. They should conduct themselves in such a manner as not to discredit the Service or the Government of Canada.

- Sources are to be managed so as to protect both the security of the Service's operations and the personal safety of sources.

- Sources should be treated ethically and fairly in their handling and compensation.

A direction on joint operations recognizes that, in certain circumstances, Canadian security interests may demand the active presence in Canada of investigators from foreign security and intelligence organizations. The principles that are to guide the Service's activities in this field are that:

- Canadian sovereignty and law are to be fully respected and protected;

- the objective and potential product of the cooperation must be of benefit to Canada and serve Canadian national interests; and

- CSIS must exercise effective control of the cooperative activity.

A direction on foreign investigations provides guidelines governing the Service's foreign investigative activity in relation to threats to the security of Canada. It stipulates that the approval of the Solicitor General is required before CSIS may undertake

operational activity abroad. The direction applies to human source travel, foreign security intelligence investigations by CSIS officials, and Service operational assistance abroad to foreign security and intelligence organizations.

Liaison and Cooperation

A direction on domestic liaison provides guidance on the establishment of arrangements between the Service and other federal or provincial institutions. A primary example is the Ministerial direction on RCMP-CSIS cooperation. The principles governing domestic liaison ensure that arrangements are consistent with the Service's mandate, and that they are in place when there is a requirement for access to information, operational support, information exchange or organizational consultation.

Similarly, a direction on foreign liaison sets out principles to guide CSIS in the establishment and conduct of liaison with foreign security and intelligence organizations.

Operational Support Services

Direction on file management covers a wide range of issues. It is designed to ensure that CSIS retains only information and intelligence that is consistent with its legislated duties and functions. Direction exists on the handling, segregation and disposal of the files CSIS inherited from the RCMP Security Service; on the disposal of categories of files for which the National Archives has approved schedules; and on the retention of files of historical value.

Completing the Framework

The Special Committee noted 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 the use of human sources; and to reconfirm the roles and responsibilities of the major office holders in the national security framework." Since the tabling of the Special Committee's Report, as recommended by the Committee, additional direction has been issued on the primary mandate of the Service.

The Solicitor General will issue new directions as necessary to ensure that Canada has a responsive and responsible security intelligence agency. In the meantime, there will be ongoing work to consolidate, update and complete the policy framework.

CHAPTER III: THE DEPUTY SOLICITOR GENERAL AND THE INSPECTOR GENERAL

In exercising Ministerial responsibility for the effective operation of the national security system, the Solicitor General draws on the executive support of a number of senior officials and their staffs. Each provides support of a unique and distinctive character.

- The Deputy Solicitor General provides informed and impartial advice and assistance on the entire range of national security issues.

- The Inspector General provides independent internal review of the Service's compliance with legislation, Ministerial direction, and operational policy.

- The Director of CSIS controls and manages the Service.

- The Commissioner of the RCMP controls and manages the Force.

THE ROLE OF THE DEPUTY SOLICITOR GENERAL

The Deputy Solicitor General provides informed and impartial advice and assistance to the Minister.

The Deputy Solicitor General is the deputy head of the Department of the Solicitor General. The principal function of the Deputy Solicitor General is to advise and assist the Minister in the discharge of his or her responsibilities for exercising national leadership in security, law enforcement, corrections and parole. In the security area, this includes:

- providing objective and timely advice on national security issues;

- coordinating the policies and programs of the security agencies reporting to the Solicitor General;

- initiating policies and programs in support of the Solicitor General's national leadership role;

- promoting communications with organizations and individuals publicly active in the national security policy area, and

- undertaking research on security policy issues.

The Deputy's Responsibilities with Respect to CSIS

The CSIS Act assigns a number of specific functions to the Deputy Solicitor General in assisting the Minister on national security issues. These are identified in section 7 of the Act.

One of the Deputy's most important functions is to advise the Minister on policy directions to be issued to the Service. This function is critical to the Minister's ability to provide effective leadership and to ensure the Service exercises its powers in accordance with law and policy. In practice, this means that the Deputy and his staff (the Ministry Secretariat) play a lead role in developing the written directions which the Minister issues periodically to guide the Service in particular policy sectors.

A second function assigned the Deputy under the CSIS Act is to be consulted on the "general operational policies" of the Service. In practice, this has meant that the Deputy and the Director discuss all matters affecting the Service which might require the Minister's attention or approval. It also entails frequent and extensive consultation between the Secretariat and the Service.

Thirdly, the CSIS Act specifies that the Deputy is to be consulted before the Service applies to the Federal Court for a warrant, or the renewal of a warrant, seeking authorization for the use of certain intrusive investigative powers. This vital function is further considered in Chapter VIII.

In addition, the CSIS Act stipulates that the Deputy is the individual to whom the Inspector General is responsible. The functions of the Inspector General are discussed below.

The Ministry Secretariat

The Deputy is supported by the staff of the Ministry Secretariat. One of the Secretariat's three branches, the Police and Security Branch, assists in respect of the Deputy's responsibilities for the national security system, policing, contingency planning, and coordinating the Federal Government's counter-terrorism program.

Within the Branch, the Security Policy and Operations Directorate assists in the coordination and development of sectoral and agency policy in two main areas: CSIS security intelligence operations, and RCMP security enforcement and protective security programs. The Directorate, which comprises approximately 20 people, reviews all Service requests for authority to use special investigative techniques and to undertake sensitive operations.

The Police and Security Branch also contains the National Security Coordination Centre (NSCC). The NSCC was created in response to the 1987 Report of the Special Senate Committee on Terrorism and Public Safety. It manages the national counter-terrorism plan, serves as a secretariat for the interdepartmental Security Advisory Committee, and provides operational support to the Solicitor General as lead Minister for counter-terrorism arrangements in Canada.

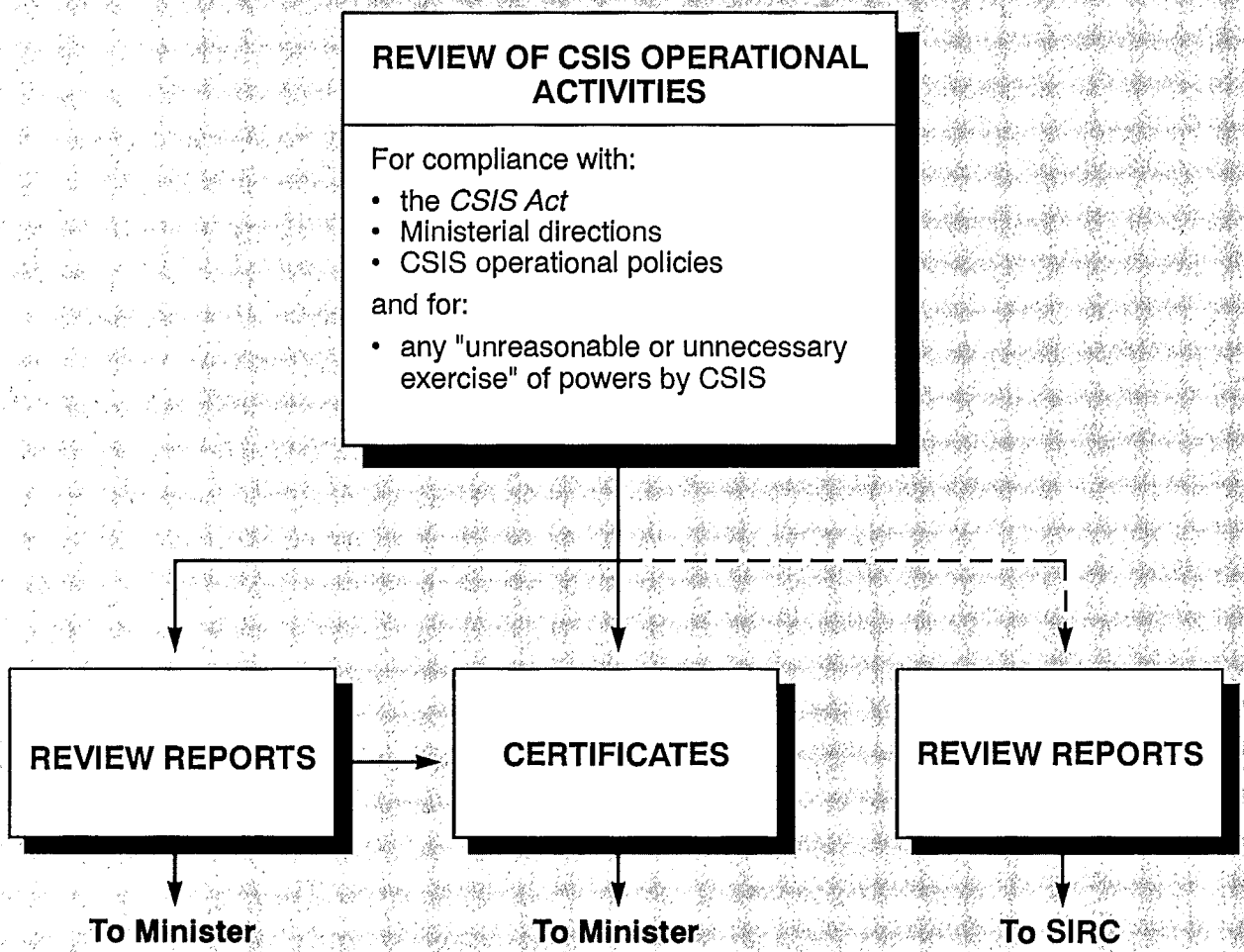
The Deputy and the Director

The Deputy Solicitor General has no line management responsibilities for CSIS or the RCMP. The Director of CSIS reports directly to the Solicitor General. So does the Commissioner of the RCMP.

This situation is not unique within the Government. There are other cases where more than one official of deputy rank reports to a Minister. But in view of the breadth, complexity and sensitivity of the portfolio, the Special Committee wondered whether the agency heads should report through the Deputy Solicitor General to the Minister. The Special Committee believed that the creation of a "senior deputy" position might improve coordination among the agencies and ease the management responsibilities of the Solicitor General.

Practice has shown that the current arrangements work well. The Deputy has a variety of means to remain informed and able to provide the advice and assistance the Minister needs. On the other hand, there might be something lost by the Deputy

THE FUNCTIONS OF THE INSPECTOR GENERAL



coming "on line". The Deputy would have to assume a large measure of responsibility for the management and operation of the agencies, and would not be as free to provide independent advice to the Minister. Ministerial control might thereby be diminished.

THE ROLE OF THE INSPECTOR GENERAL

The Inspector General conducts independent internal reviews for the Minister.

In view of the heavy burden placed on the Solicitor General to ensure CSIS exercises its powers lawfully and responsibly, the post of Inspector General was created to provide the Minister with an independent window on the operational activities of the Service. In effect, the Inspector General serves as the Minister's internal auditor for CSIS, supplementing the advice the Minister receives from the Deputy with an independent means of assurance that the Service is complying with the law, Ministerial direction, and its own policies.

The post of Inspector General is unique. It has evolved over time in response to practical experience and Ministerial expectations. Today, it is functioning to the full satisfaction of the Minister.

The Special Committee's commentary on the office of the Inspector General reflected a misunderstanding of the purpose and functions of the office, and the confidential nature of the Inspector General's work. Notwithstanding the testimony of the Solicitor General, the Deputy Solicitor General, the current Inspector General and other knowledgeable witnesses, the Special Committee relied on information and opinion which did not accurately reflect the role and operation of the office. In consequence, the Special Committee expressed concerns which are without foundation.

The Functions of the Inspector General

Under section 30 of the CSIS Act, the "Governor in Council shall appoint an officer to be known as the Inspector General, who is responsible to the Deputy Minister". The Act identifies three interlocking functions for the Inspector General:

- to review the operational activities of the Service;
- to monitor the Service's compliance with its operational policies; and
- to submit certificates to the Minister.

To ensure the Inspector General is able to exercise these functions effectively, the Act stipulates that the Inspector General is entitled to have access to "any information under the control of the Service" that relates to the performance of the functions of the office, and to receive from the Service "such information, reports and explanations" as the Inspector General deems necessary. Under section 31, no information other than Cabinet confidences may be withheld on any grounds.

The Inspector General's staff consists of approximately a dozen individuals, with considerable depth and breadth of experience in a variety of disciplines.

The Review Program

The CSIS Act assigns review and monitoring functions to the Inspector General which are continuous and, in practice, closely related. The Inspector General has combined these functions in a review program that is selective and consistent with the resources available. In addition, the Inspector General will occasionally be tasked by the Minister to undertake special reviews, and may be directed by the Security Intelligence Review Committee (SIRC) to examine a specific activity of the Service. (The functions of the SIRC are discussed in Chapter IX).

The Inspector General's review program is designed, through a series of review projects, to result in a systematic and thorough review of major aspects of the Service's operational activities. Within a 4-5 year cycle, review priorities are updated annually, taking into account progress on previously scheduled work as well as new priorities.

The review program focusses on the operational activities that are unique to CSIS as a security intelligence agency, and about which the Minister should be well informed. Accordingly, the primary focus is on program areas where the Minister needs regular, independent assurance that all is in order -- and, if it is not, information on the problems that exist. These are the areas where the Service's failure to comply with the relevant authorities would present the greatest risk of its operations compromising the individual rights and freedoms of Canadians.

Review projects in recent years have focussed on:

- CSIS targeting policies, decisions and practices;
- CSIS applications for Federal Court warrants, and how the Service has exercised the powers authorized by such warrants;
- the Service's recruitment and handling of human sources of information;
- the Service's control and use of information collected; and
- CSIS security screening programs.

In undertaking review projects, the Inspector General's investigators will examine files, conduct interviews at CSIS Headquarters and in the field, and double-check facts and findings with senior Service personnel before submitting written reports to the Minister. The Minister meets regularly with the Inspector General to discuss specific reports and the status of the review program. Reports requiring follow-up action are reviewed by the Minister, and remedial action taken as necessary.

The reviews carried out by the Inspector General assess compliance with:

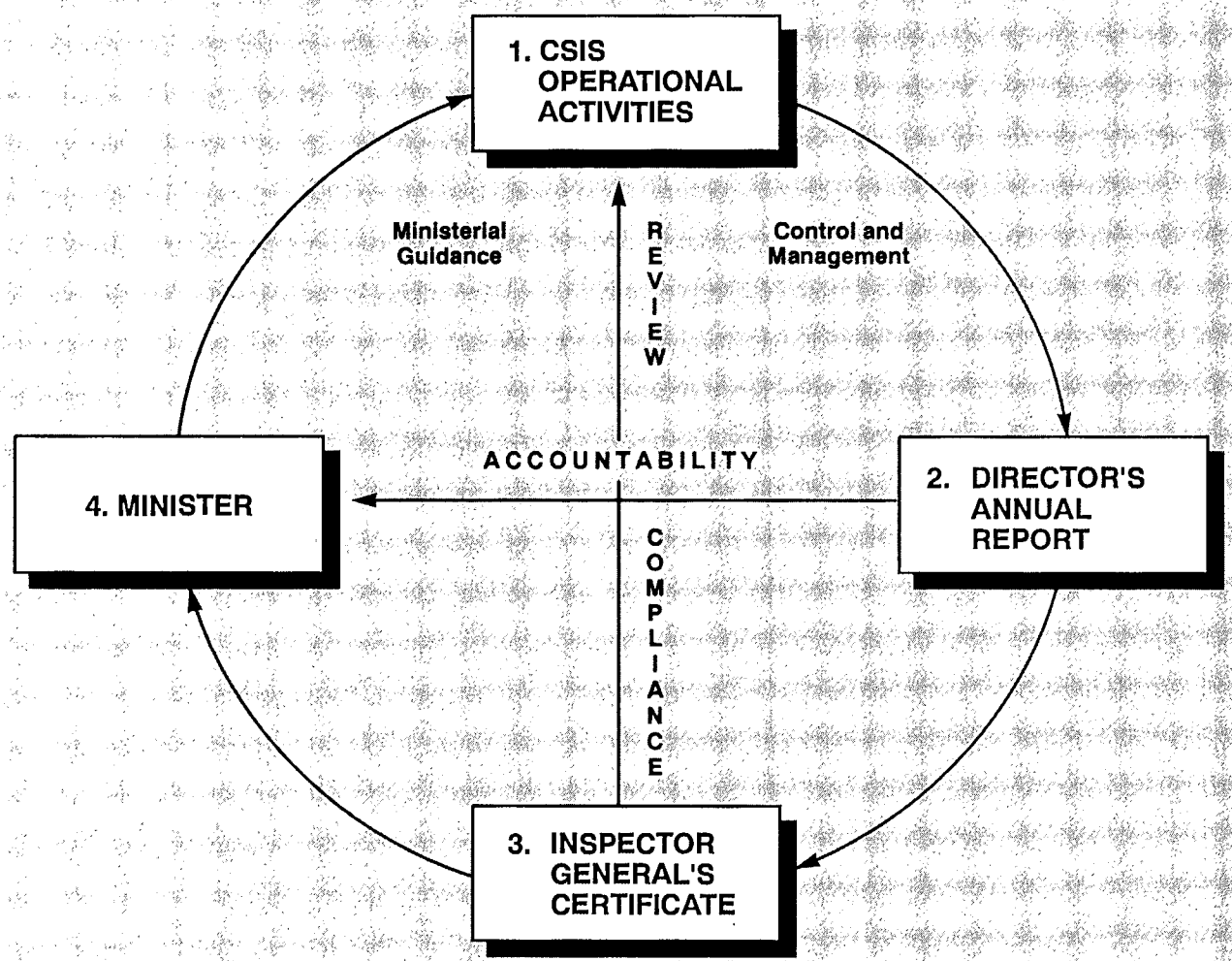
- the CSIS Act;
- Ministerial directions;
- the Service's operational policies; and
- conditions imposed by the Federal Court in authorizing warrants.

In addition, reviews assess whether operational activities by the Service involved any unreasonable or unnecessary exercise of the Service's powers.

The Certificates of the Inspector General

The CSIS Act requires the Inspector General to submit certificates to the Minister. The on-going review program assists the Inspector General to prepare each certificate on a well-informed basis.

INTERNAL REVIEW CYCLE



Under section 33 of the CSIS Act, the Director of CSIS must submit a report to the Minister at least every 12 months "with respect to the operational activities of the Service". A copy of that report is then conveyed to the Inspector General, who, in turn, is required to submit a certificate to the Minister stating the extent to which the Inspector General is "satisfied" with the report. The Minister looks to the certificate for assurance that the Director's report provides a reasonable and balanced account of the Service's operational activities over the year.

In addition, section 33 specifically requires the Inspector General to notify the Minister in the certificate "whether any act or thing done by the Service":

- was not authorized by the CSIS Act;
- contravened any directions issued by the Minister; or
- involved any unreasonable or unnecessary exercise of the Service's powers.

Once submitted to the Minister, the Director's Annual Report and the Inspector General's certificate serve as important documents in the annual accountability cycle.

The Independence of the Inspector General

Under the terms of the CSIS Act, the Inspector General reports to the Minister and is responsible to the Deputy Minister. The Inspector General may be directed by SIRC to conduct reviews, and copies of certificates along with other reports are made available to SIRC. The question has arisen, therefore, whether the Inspector General retains sufficient freedom to provide independent reports and assessments on the Service's activities.

The record indicates that the Inspector General's authority and independence are firmly grounded in law and practice.

- the Inspector General has final authority over the office's review program and priorities, notwithstanding the fact that the program is prepared with the benefit of the views of others and that additional reviews can be requested by the Minister or SIRC;
- the CSIS Act states that the Inspector General is entitled to have access to any information under the control of the Service that relates to, or which the

Inspector General deems necessary for, the performance of the duties and functions of the office. Lack of access to Cabinet confidences has not hindered the Inspector General's ability to review critical information;

- by serving the Minister directly, the Inspector General maintains a measure of distance from the Minister's policy and operational advisors in the Ministry Secretariat;

- while SIRC may direct the Inspector General to conduct specific reviews on its behalf, the Inspector General functions independently from SIRC; and

- because SIRC has right of access to all of the Inspector General's work, it is in a position to provide Parliament with external assurance that the functions of the Inspector General are being discharged independently.

As the current Inspector General has pointed out, the fact that all the parties to the review function "share a common goal of helping ensure an effective security intelligence service that respects the fundamental rights of Canadians means that reason and common sense prevail".

CHAPTER IV: THE DIRECTOR AND CSIS

The Director of CSIS is responsible for the control and management of the Service.

THE ROLE OF THE DIRECTOR

The Director's authority to manage and control the Service is found in section 6 the CSIS Act. In addition, section 8 of the CSIS Act gives the Director exclusive authority to appoint employees and, subject to Governor in Council regulations, to exercise the powers and perform the duties and functions of the Treasury Board relating to personnel management, and of the Public Service Commission pursuant to the Public Service Employment Act.

The Director manages the Service in keeping with the CSIS Act, other legislation such as the Official Languages Act, the Canadian Multiculturalism Act, the Access to Information and Privacy Acts, and Ministerial direction.

The Director's key responsibilities include:

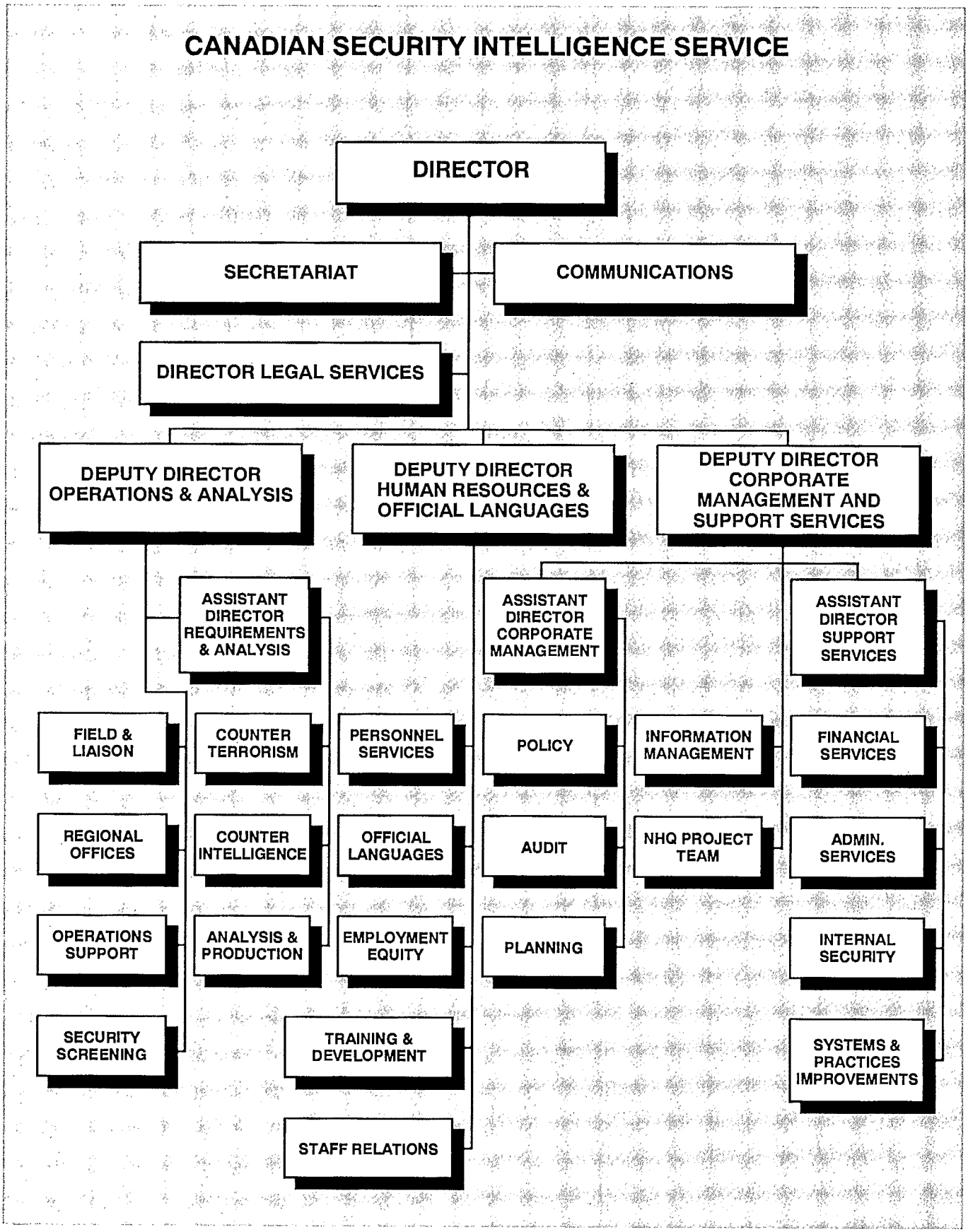
- providing direction to the Service in discharging its responsibilities under the CSIS Act relative to threats to the security of Canada;

- managing the Service to deliver its programs (counter intelligence, counter terrorism, security assessments);

- building the management and corporate structure and function of the Service, by providing direction and supervision to ensure the Service's discharge of its responsibilities within the law, Ministerial direction and policy, and by chairing the key senior management committees;

- managing the statutory and other external relationships of the Service;

CANADIAN SECURITY INTELLIGENCE SERVICE



- discharging the personnel management responsibilities granted to the Service as a separate employer;

- approving the Service's internal policy and ensuring its proper implementation;

- widening and enhancing public knowledge of the Service's role and mandate through active public and media relations;

- consulting the Deputy Solicitor General on the general operational policies of the Service and any matter with respect to which consultation is required by directions issued under section 6; and

- reporting to the Solicitor General on all matters within the Director's purview.

In discharging these responsibilities, the Director is aided by three Deputy Directors (Operations and Analysis, Human Resources and Official Languages, Corporate Management and Support Services), and two Directors General (Secretariat and Communications).

Control and Management of the Service

In recognition of the unique role played by a security intelligence agency, the Act assigns to the Director special authority and responsibility for the control, organization and management of the Service.

In 1984, CSIS faced the challenge of establishing an entirely new infrastructure to support the work of a new civilian workforce. Separation from the RCMP had entailed the loss of the basic building blocks of a personnel management system. It was necessary to establish a system whose goals and objectives would reflect the desired corporate culture of a modern security intelligence service.

In 1987, the Government recognized that CSIS had experienced serious resource problems and that it had been established without a full appreciation of the real costs of separation from the RCMP. A review of the funding requirements of the Service was thereupon undertaken by a team including representatives from the Treasury Board Secretariat, the Privy Council Office and the Ministry Secretariat. The result of the review was that the resource levels of the Service were raised. They have since been augmented annually to reflect the need for Headquarters accommodation in the National Capital Region and the need to keep pace with technological advances in tradecraft.

Also in 1987, the initial hierarchical decision-making structure that tended to isolate the Director from the day-to-day operations of the Service was abandoned, in favour of one which provided for a more direct involvement on the Director's part in the internal accountability framework of the Service and its day-to-day operations. The Director augmented direct control over the Service's activities through personal chairmanship of key Service committees responsible for:

- senior management issues;
- the determination of the strategic direction of the Service;
- the approval of operational proposals and policies; and
- the review and approval of targets and warrants.

Additional organizational changes have since been undertaken to encourage the development of a corporate level perspective on program planning and priorities.

In late 1987, the Deputy Director (Human Resources and Official Languages) was named to be responsible for all matters relating to personnel, official languages, employment equity, training and development and staff relations. A Secretariat was also formed to assist the Director in managing the Service's relations with the various review bodies, the Minister and the Ministry, access to information and privacy requests, the internal committee system, the public complaints process, and to act as a gate for material destined for the Director's review.

In 1990, the position of Deputy Director, Administration and Services, was retitled Deputy Director, Corporate Management and Support Services. Reporting to this position are the Assistant Director, Corporate Management (formerly a deputy directorship) with responsibility for audit, policy and planning, and the Assistant Director, Support Services, responsible for financial and administrative services, internal security and systems and practices improvements. At the same time, the operational structure was strengthened by the creation of the position of Assistant Director Requirements, reporting directly to the Deputy Director, Operations and Analysis.

Personnel Management

The vitality, strength and morale of an organization are directly related to the integrity of its human resource policies and the degree of mutual trust and respect which exists between management and employees. In a short period of time, the

Service has built a human resource management structure that incorporates the important elements of Public Service initiatives, and visibly demonstrates that CSIS is a career-oriented employer.

Since inception, the Service has made marked progress in putting in place human resource and labour-management programs that demonstrate management's commitment to creating a quality working environment in step with the challenges of the 1990s, and in keeping with the Government's policies on employment equity, multiculturalism and official languages.

Within the constraints of a set human resource base, and in light of the need to hire specific professional skills and abilities, the Service has now established realistic strategic and numerical objectives to reflect the government's employment equity objectives.

The employment equity goals of the Service are to ensure equal access to employment and development, and to reflect the Canadian mosaic. CSIS has implemented an employment equity plan for all target groups for the period 1989-1994 that sets out both numerical and systemic objectives and includes a communications plan. The program actively seeks candidates from all groups across Canada through contact with various communities, and stresses the Service's commitment to employment equity in all public advertising. Since the fall of 1988, the Service has hired equal numbers of male and female candidates at the intelligence officer entry level. While the merit principle is the basis for hiring and promotion within the Service, an effort has been made to ensure that members of target employment equity groups are able to compete effectively for jobs.

In 1990, the Service's multiculturalism program was incorporated into the Service's overall strategy, in keeping with the Canadian Multiculturalism Act. This program should enable the Service to continue to attract recruits who have a mother tongue other than English or French.

Official Languages

CSIS is implementing the Government's official languages program, whose three objectives are: service to the public, language of work, and equitable participation. Equitable participation means providing equal opportunities for employment and career advancement to both anglophones and francophones. The anglophone/francophone participation rate in CSIS compares favourably with that of the federal Public Service generally and the Service is pursuing its efforts to increase its bilingual capacity.

ANGLOPHONE/FRANCOPHONE PARTICIPATION RATE

	Overall	Management Category	Officer Category
CSIS	68%/32%	72%/28%	77%/23%
Federal Public Service	72%/28%	78%/22%	73%/27%

At present, approximately 10 percent of CSIS employees are pursuing part-time or full-time second language training. In 1988, revised federal language training policies made training accessible to Federal Government employees for career planning purposes and in support of human resource management planning objectives, in addition to existing statutory reasons. While statutory reasons will continue to constitute the priority for second language training in CSIS, full-time training for unilingual persons in unilingual positions throughout the Service will be expanded in accordance with Government policies. An employee's potential to succeed, established through aptitude testing, must generally be demonstrated prior to access to language training. In addition, there must be a reasonable expectation that persons will use and maintain their acquired language skills by movement to a bilingual position or region.

Whenever possible, employees are encouraged to use and maintain their acquired language skills. Subject to operational requirements, postings to bilingual positions or career assignments to a bilingual region are encouraged. Intelligence officers can apply through existing rotational development or normal transfer programs to move to areas of the country where the language of the majority is different from their own.

The Service is negotiating a Letter of Understanding (LOU) on Official Languages with the Treasury Board which will deal with the government's three program objectives. This Letter, which will be a public document, will cover all aspects of the present situation and will include a three-year action plan to build on

progress already achieved. There will also be provisions in the LOU for an internal audit of the program within the next three years.

Recruitment and Development

CSIS is a separate employer committed to the concepts and practices of career employment. These are an integral part of the orientation and operation of its resourcing activities. Outside recruitment occurs periodically when specific skills are not available, or when lengthy development programs are not feasible. The Service's first choice is to develop its own employees for advancement.

CSIS policies clearly outline the Service's approach for attracting and hiring people, developing their skills and helping them pursue rewarding careers. Internal CSIS publications defining managers' responsibilities emphasize the importance of ensuring that employees must be developed, challenged and prepared for the future.

In 1985, CSIS introduced a pilot project requiring candidates for employment with the Service to take a polygraph test. The test originally covered matters of loyalty to Canada and lifestyle but, in early 1988, lifestyle questions were dropped. Since then, polygraph tests have focussed exclusively on loyalty to Canada. The Service has since been examining its use of the polygraph as a condition of employment, and will shortly be submitting a report to the Government on the question.

In response to the Special Committee's recommendation, the Service is also reviewing the psychological assessment component of the employee selection process.

Labour-Management Relations

As a separate employer, the Service has kept in step with the programs and policies of the Public Service. As a general principle, CSIS employees have the same level of benefits as members of the Public Service. The benefits of those employees who enjoy "grandfathered rights", in consequence of their transfer from the RCMP, exceed those of public servants generally. The Service has no intention of changing entitlements without full consultation.

The Service has made a dedicated effort to building a sound employee assistance program. Assured of confidentiality, employees can avail themselves of either professional in-house assistance or external support. The Service's program

is modelled on similar programs in the public and private sector, including that of the RCMP.

The employee/employer committees CSIS has introduced meet to discuss all major issues affecting employees, apart from collective agreements on terms and conditions of employment. Discussion can range from employees' views on office environment to work scheduling. The committees also provide managers and employees an opportunity to correct situations in their own work areas, thus reducing the need to resort to grievance procedures.

CSIS has gone to considerable lengths to put in place suitable mechanisms for labour-management relations in the Service. For example, ad hoc adjudication arrangements have been concluded with the Public Service Staff Relations Board to provide an avenue for CSIS employees to seek redress in grievance cases. CSIS management has no basic objection to extending collective bargaining rights to the majority of its employees, provided that certain employees may be designated to perform duties necessary for the safety or security of the public.

CHAPTER V: CSIS MANDATE

The national security system created in 1984 assigned specific and distinct mandates to CSIS and the RCMP. The CSIS Act described the several mandates assigned to CSIS, and the Security Offences Act confirmed the RCMP's responsibility for security enforcement and protective security.

CSIS has a precise mandate which is defined in legislation.

Under the CSIS Act, Parliament has assigned CSIS a clearly defined set of objectives. These are:

- to collect, analyze and retain information and intelligence on activities that may on reasonable grounds be suspected of constituting threats to the security of Canada, and in relation thereto, to report to and advise the Government of Canada (section 12);

- to provide security assessments in support of the government's security clearance program (section 13);

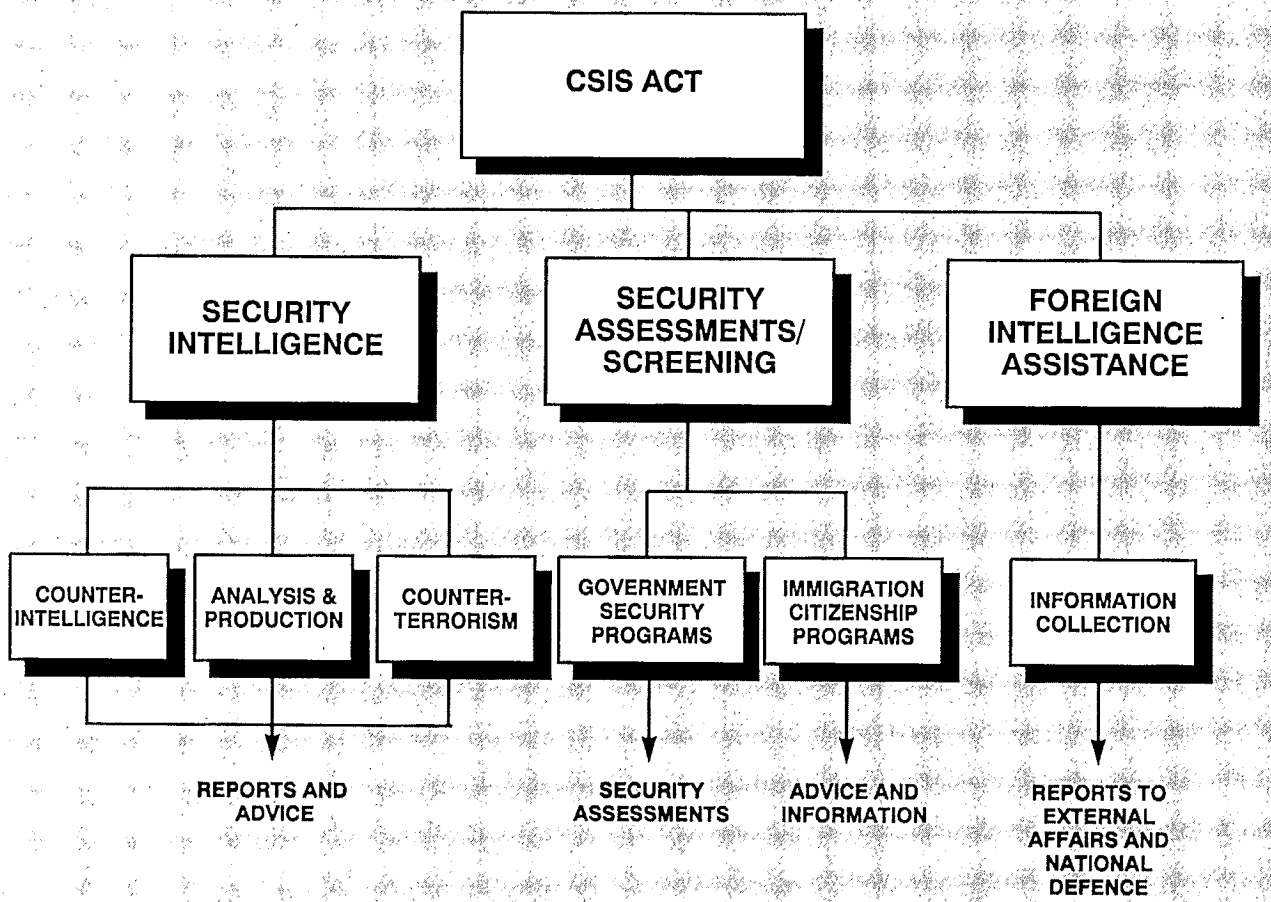
- to provide information and advice in support of government citizenship and immigration programs (section 14); and

- to assist in the collection of foreign intelligence in Canada (section 16).

This chapter deals with the first three of these objectives. Chapter VII discusses the Service's role in the collection of foreign intelligence.

Like other Government departments and agencies, CSIS is required to pursue its objectives with full respect for the law including the Canadian Charter of Rights and Freedoms.

CSIS MANDATE



THREATS TO THE SECURITY OF CANADA

The Service's primary mandate, relating to its core security intelligence role, is to be found in two provisions of the CSIS Act: the definitions of "threats to the security of Canada" outlined in paragraphs 2(a),(b),(c) and (d); and the description of the Service's duty to collect, analyze and retain information and intelligence on "threats to the security of Canada" outlined in section 12.

The exercise of this mandate is conditioned by the limits and controls specified in sections 2 and 12 themselves, by Ministerial directions, and by the Service's own operational policies and procedures. In addition, certain powers employed by the Service are subject to the requirement to obtain a judicial warrant.

In Canada, the search for an acceptable definition of "threats to the security of Canada" dates back at least to the 1946 Kellock and Taschereau Royal Commission. Parliament worked long and hard before settling on the language contained in section 2 of the CSIS Act, and it is understandable that the issue continues to be debated. It touches fundamental political and philosophical questions on which there is never likely to be consensus. The Special Committee struggled as well to find ideal language, its Report arguing that the current language is too broad and potentially vulnerable to a Charter challenge. Accordingly, it recommended the adoption of more restrictive definitions for terms in the Act such as "espionage," "sabotage", and "detrimental to the interests of Canada".

The Special Committee provided a useful analysis of the issues and made several suggestions for refining the definitions contained in section 2. But history suggests amending the CSIS Act in this area would not be a very productive exercise. The current definitions are indeed broadly conceived. But in the Government's view, the present definitions, combined with existing statutory limitations and Ministerial directions, ensure suitably rigorous policy standards and operational interpretations to provide a balance between the Service's needs for discretion in investigating threats to the security of Canada, and Canadians' expectations that their rights will be protected.

To underscore its determination to place limits on the scope of the definitions, Parliament included in the definitions a proviso that excluded from the body of the definitions "lawful advocacy, protest or dissent", unless such activities were carried on in conjunction with any of the activities referred to in the specific categories defined.

SECTION 2 - THREAT DEFINITION

2. In this Act,

"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;

(b) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person;

(c) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political objective within Canada or a foreign state, and

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

but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (a) to (d).

SECTION 12 - SECURITY INTELLIGENCE

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.

In the Government's view, the definitions established by Parliament set outer limits for the Service's investigative authority which have proven both durable and acceptable. They are "activity-based", not ideological in conception, and framed in such a way that they can continue to identify injury to Canada's security interests regardless of changes to the domestic or international threat.

The security intelligence collection activities of CSIS are also subject to limitations beyond the definitions contained in section 2. Two of these appear in section 12 and have a major impact on the Service's investigative activities.

- CSIS must have "reasonable grounds to suspect" that activities constitute a threat before the Service may commence an investigation.

- CSIS may only collect information or intelligence "to the extent that it is strictly necessary."

Ministerial Direction on Sections 2 and 12

Ministerial direction is an essential mechanism of control, and Ministers have used it with particular effect to ensure that the appropriate focus is placed upon the interpretation and application of statutory terms, particularly the threat definitions.

The Special Committee expressed concern that there was no comprehensive Ministerial direction dealing with the primary mandate of the Service as specified under sections 2 and 12. The Minister has now issued such direction. Some of its principal elements include:

- CSIS must ensure that an appropriate balance is maintained among its collection, analysis, retention and reporting functions;

- CSIS' primary mandate is to provide information and advice on the range of activities described in section 2. The Service's mandate derives from the fact that these activities may harm Canada's security and is not a function of the lawfulness or unlawfulness of the particular activity;

- The Service is to accord priority to the collection of information on those activities directly "against Canada" or "within Canada".

- The terms in section 2 (i.e. "espionage" and "sabotage", "detrimental to the interests of Canada", "directed toward", and "relating to Canada") and in section 12 (i.e. "strictly necessary," "reasonable grounds to suspect") are to be interpreted in accordance with Ministerial direction;

- The privacy of individuals must not be interfered with, unless there are valid reasons to do so;

- The nature and extent of collection must be governed by the "strictly necessary" test. The Service must ensure that the scope and intrusiveness of its collection activities are proportionate to the seriousness of the threat being investigated;

- Lawful advocacy, protest or dissent may not be investigated unless such activities are carried on in conjunction with threats referred to in section 2; and

- CSIS is to continue to subscribe to the most rigorous standards of analysis and advice.

Ministerial direction also requires the Director to keep the Minister fully informed of all significant developments, problems or matters of potential controversy that may arise from the operation of the Service's security intelligence mandate.

Direction on paragraph 2(d)

In late 1987, the Government took the decision to disband the Counter-Subversion Branch of the Service; and in February 1988 the Solicitor General announced that Ministerial authorization would henceforth be required before the Service undertook investigations, beyond open published information, of "subversion" activities defined in paragraph 2(d). It is the Government's view that the early controversy over the "subversion" issue was not due to the definition contained in paragraph 2(d), but to the way in which the definition had been implemented during the transition period. Ministerial direction has since significantly limited the scope and intensity of the Service's activities under paragraph 2(d).

The Government believes its approach is consistent with the intent and purpose of the CSIS Act. While a particular threat may not be considered especially serious at a given time, this would not, in the Government's view, justify removing it altogether from the mandate of the Service, thereby precluding the Government from ever receiving advice on the issue in the future.

The Government is not insensitive to the concerns regarding paragraph 2(d) which were raised by some of those appearing before the Special Committee. It believes, however, that much of the criticism reflected unnecessary apprehension rather than evidence of an actual problem. The Special Committee itself was not unanimous in recommending that paragraph 2(d) be repealed, and a number of witnesses actively supported its retention.

Directions issued to CSIS on national requirements, the conduct of investigations and the use of human sources provide guidance on Service investigations and the means utilized to pursue these. In the Government's view, these directions provide effective control over the Service's investigative activities.

The essential elements of the Service's security intelligence mandate and related Ministerial direction are incorporated into the policy and procedures of CSIS. The policies of the Service are contained in the CSIS Operational Manual, which translates the CSIS Act and Ministerial direction into practical guidelines for CSIS employees in conducting their operational activities. The manual is the Service's most detailed source of guidance, and it is reviewed and modified by CSIS management to ensure Service activities are conducted in an approved manner.

SECURITY ASSESSMENTS

The Service's mandate for providing personnel security assessments to other Federal Government departments and agencies is set out in section 13 of the CSIS Act. Subject to the approval of appropriate Ministers, CSIS may also enter into arrangements authorizing the provision of security assessments for:

- provincial governments or departments;
- provincial police forces; and
- foreign governments, institutions, or international organizations.

A very demanding mandate of the Service is the provision of security assessments for a large number of Federal Government employees and contractors. Assessments entail forming a fair and accurate judgment of a person's loyalty to Canada, and of that person's reliability as it relates to loyalty.

SECTION 13 - SECURITY ASSESSMENTS

"13. (1) The Service may provide security assessments to departments of the Government of Canada.

(2) The Service may, with the approval of the Minister, enter into an arrangement with

(a) the government of a province or any department thereof, or

(b) any police force in a province, with the approval of the Minister responsible for policing in the province,

authorizing the Service to provide security assessments.

(3) The Service may, with the approval of the Minister after consultation by the Minister with the Secretary of State for External Affairs, enter into an arrangement with the government of a foreign state or an institution thereof or an international organization of states or institution thereof authorizing the Service to provide the government, institution or organization with security assessments."

CSIS must comply with legislation and policy that specifies what a security assessment must address. First, section 2 of the CSIS Act defines a "security assessment" as an "appraisal of the loyalty to Canada and, so far as it relates thereto, the reliability of an individual". Second, the Government Security Policy (GSP), a public document, sets out criteria to be taken into account in making security assessments. This policy integrates "threats to the security of Canada" with loyalty and related reliability criteria, to effectively protect sensitive government information and assets. The GSP also provides criteria and procedures for the classification and protection of government information and assets. As a relatively new government-wide policy issued under the authority of the Financial Administration Act, the GSP is under continuous review and is revised and updated for purposes of clarity and compatibility with legislative change and jurisprudence.

As with all aspects of the activities of the Service, the Government is sensitive to the need to ensure that the rights and freedoms of individuals subject to assessment are respected at all times, and that this respect is visible in the process. Should the subject of an assessment request that he or she be accompanied by legal counsel during a security assessment interview, or ask that such an interview be tape-recorded, the request would be honoured. CSIS and other government departments and agencies handle and protect personal information collected as a result of the security assessment process with due regard for the right to privacy of each individual and respect for the provisions of the Privacy Act. As is described in Chapter IX, the CSIS Act provides means of redress for an individual who feels that he or she may have been denied a security clearance unfairly.

CITIZENSHIP AND IMMIGRATION SCREENING

The Service may also perform personnel screening services for Ministers of the Crown who have responsibilities for the Federal Government's citizenship and immigration programs.

SECTION 14 - SECURITY SCREENING

"14. The Service may

(a) advise any Minister of the Crown on matters relating to the security of Canada, or

(b) provide any Minister of the Crown with information relating to security matters or criminal activities

that is relevant to the exercise of any power or the performance of any duty or function by that Minister under the Citizenship Act or the Immigration Act."

Under section 14 of the CSIS Act, the Service provides advice and information to support programs that are governed by the Citizenship Act and the Immigration Act. The criteria and standards that are demanded of CSIS in providing this advice and information are found in these Acts, rather than in the CSIS Act.

The criteria identified in the Citizenship Act and the Immigration Act reflect concerns relevant to the granting or denying of citizenship and to admissibility to Canada. The Citizenship Act includes in its criteria the definition of "threats to the security of Canada" appearing in section 2 of the CSIS Act. But the Citizenship Act goes on to list additional criteria that Parliament has determined are relevant to a decision to grant or deny citizenship. The Immigration Act sets forth a series of criteria relevant to a determination of admissibility. Much of the language of this section is compatible with the language describing "threats" in section 2 of the CSIS Act. The Immigration Act, at the same time, recognizes that the criteria to be considered when making an assessment of admissibility are not limited solely to activities that are threats to security, but include other types of behaviour such as criminal conduct.

Both the Citizenship Act and the Immigration Act authorize the SIRC to investigate matters related to the denial of citizenship or immigration on security grounds.

CHAPTER VI: THE NATIONAL SECURITY MANDATE OF THE RCMP

The RCMP is responsible for security enforcement and protective security.

The Royal Canadian Mounted Police form an integral part of Canada's national security system. First organized in 1873, the RCMP derives its present-day authority and responsibility from the RCMP Act. This Act establishes the RCMP as the federal police force, provides the legislative basis for its operations, and authorizes the Solicitor General to enter into policing agreements with provincial, territorial and municipal governments.

Under the direction of the Solicitor General, the Commissioner of the RCMP is responsible for controlling and managing the Force and all related matters. The Commissioner is assisted by four Deputy Commissioners responsible respectively for operations, law enforcement and protective services, corporate management, and administration. The Commissioner is also supported by 13 Divisional Commanding Officers, one for each province and territory and for the National Capital Region. The RCMP currently provides policing services under contract to all provinces except Ontario and Quebec, to the two territories, and to 191 municipalities.

The mandate of the RCMP is "to enforce laws, prevent crime, maintain peace, order and security". This mandate includes responsibility for:

- preventing, detecting and investigating offences defined by federal statutes;
- maintaining law and order, and preventing, detecting and investigating crimes in the provinces, territories and municipalities with which the Force has a policing contract;
- protective security measures to safeguard VIPs, certain federal properties, airports and vital points from security offences or threats;
- the provision of advice to departments and agencies of the Government respecting protective security measures; and

- providing all Canadian law enforcement agencies with specialized police training and research, forensic laboratory services, identification services and informatics technology.

Security Offences Act

The RCMP's responsibility for the enforcement of criminal law relating to security offences, and for protective security, has been continuous. But the legislative changes which occurred in 1984 did have an impact on the Force's security mandate. First, responsibility for security intelligence and security screening passed from the RCMP to the new security intelligence service. Secondly, the RCMP was accorded, for the first time in legislation, primary responsibility for investigating offences which arise out of conduct constituting a threat to the security of Canada or where the victim of an offence is an internationally protected person.

The Security Offences Act of 1984 created no new offences, but defined the circumstances under which existing offences would fall within its ambit and be linked to the national security responsibilities of the RCMP, the Solicitor General and the Attorney General of Canada. Section 2 of the Act included within their responsibilities any offence under the law of Canada where:

- "(a) the alleged offence arises out of conduct constituting a threat to the security of Canada within the meaning of the Canadian Security Intelligence Service Act or

- (b) the victim of the alleged offence is an internationally protected person within the meaning of section 2 of the Criminal Code".

Further, the Act stipulated that:

- members of the RCMP who are peace officers would have "primary responsibility to perform the duties that are assigned to peace officers in relation to any offence referred to in section 2 or the apprehension of the commission of such an offence";

- the Solicitor General could enter into arrangements with provincial governments concerning policing responsibilities with respect to security offences; and

- the Attorney General could issue a fiat establishing the Attorney General's exclusive jurisdiction over the prosecution of a security offence.

The Security Mandate of the RCMP

By virtue of the foregoing, agreements concluded with other federal departments and agencies, international agreements to which Canada is party, and Government directives, the security-related duties performed by the Force are extensive. They include:

- the prevention, detection, investigation and laying of charges in relation to security offences referred to in the Security Offences Act, or in other federal statutes such as the Criminal Code, the Official Secrets Act and the Export and Import Permits Act;

- the provision of protective security measures to safeguard VIPs, federal properties, airports and vital points from security offences or threats;

- the provision of advice to departments and agencies of the Government respecting protective security measures; and

- the consideration of threat assessments from CSIS and other sources to provide necessary protection to VIPs and special events.

To help the Force meet its national security responsibilities effectively, a number of important organizational steps have been taken.

In July 1984, at the time of separation, Ministerial direction was issued describing the expected relationship between the RCMP and CSIS; and in August 1986 a further Ministerial direction established the RCMP/CSIS Liaison Officer Program. The Minister also approved a Memorandum of Understanding between the two agencies, which has since been updated, setting out many of the requirements for effective cooperation, including the exchange of criminal extremism/terrorism information as it relates to law enforcement.

The main highlights of the MOU are as follows:

- it reaffirms the role of CSIS in investigating suspected threats to the security of Canada, and that of the RCMP in preventing security offences and enforcing the law;

- it outlines the specific security related responsibilities of each agency;

- it reaffirms the principle that the RCMP is the primary recipient of security intelligence on national security offences and, indeed, relies primarily on CSIS for such intelligence;

- it sets out undertakings by both parties to provide each other with specific types of information and provides for procedures to protect the information exchanged, consistent with the high standards required of national security information;

- it identifies certain forms of operational support that one agency may offer the other on a shared-cost basis; and

- it confirms the role of the liaison officer exchange system between CSIS and the RCMP.

In 1988, the RCMP established a National Security Investigations Directorate (NSID), and national security investigations sections, to provide expertise and dedicated resources for the investigation of offences having a national security dimension, and to supply investigative and related support for the Force's protective policing program.

Security Investigations

The security investigations mandates of the RCMP and CSIS differ, but they share a common objective. This, in turn, places a premium on effective cooperation between the two agencies.

The RCMP's mandate is to investigate individuals who may be engaging in criminal activity, whereas the CSIS mandate is to investigate and analyse security threats. These different mandates, however, do not result in mutually exclusive areas of investigative activity. At times, therefore, the RCMP and CSIS have to work side by side in discharging their respective mandates. In addition, though the two agencies' operational mandates may differ, their investigative activities have much in common. Both employ similar investigative methods and techniques to acquire information on the activities of individuals and groups, the RCMP to enable the Force to prevent crime or to lay charges, CSIS in order to report to and advise the Government with respect to threats. Because of these overlaps, special care is required to ensure that the RCMP and CSIS understand their respective roles and responsibilities, and that understandings exist to regulate their interaction. It is particularly important there be a common appreciation

of respective rights and obligations concerning the sharing, protection and use of security information.

Use of Security Information in the Courts

As the Special Committee pointed out, the use of security information in the Courts is a complex issue, and there is a special government working group now studying this issue.

The issue raises particularly sensitive and difficult questions about the balance to be struck between the state's interest in effective security intelligence collection over the long-term and its interest in effective prosecution of particular security offences, consistent with the need to protect individual rights. The use of CSIS information in a law enforcement context brings with it a substantial risk of exposing the Service's human and technical sources and investigative methods; but it may also be crucial to the successful outcome of a criminal prosecution. A careful weighing of the relative importance of protecting security intelligence and enforcing criminal laws is therefore necessary before CSIS information can be used in the Courts.

The study now underway is examining a number of options for putting mechanisms in place, whether statute or policy-based, to ensure that a proper balance is maintained in a consistent manner.

Security Protection

The RCMP's responsibility for discharging the Government's protective policing obligations, at both the national and international level, is a large one. The obligation involves the provision of security to a considerable number of people including:

- the Governor General;
- the Prime Minister;
- Ministers of the Crown;
- Members of Parliament;
- Judges of the Supreme Court of Canada and Federal Court of Canada;

- senior government officials and others designated by the Solicitor General;
- visiting foreign dignitaries; and
- resident foreign diplomatic representatives.

As well, the RCMP is charged with protecting designated federal properties such as Parliament Hill, Canadian airports, diplomatic missions and residences, and with planning and executing security operations for major visits and events across Canada.

Decisions on whether certain internationally protected persons require protection are made by the Interdepartmental Diplomatic Review Committee, chaired by the Department of External Affairs, in which the RCMP and CSIS participate. The RCMP then determines the level of protection to be provided.

The RCMP relies on intelligence and threat assessments provided by CSIS, and on criminal intelligence provided by its own units and other law enforcement agencies, to determine particular measures to be applied to a given person or property. The planning and delivery of protective services with respect to visiting dignitaries, foreign missions and major events require close cooperation with provincial authorities and the assistance of provincial, regional and municipal police forces.

In the case of airport policing, protective security arrangements approved by Treasury Board give the RCMP responsibility for security at ten international and eight other major airports in Canada. The Force's airport protective policing capability is comprehensive, with specially trained and armed personnel placed at critical access points and continuous patrols made of terminals and aircraft operating areas. The Force also supervises airport guard services, surveillance systems, and the monitoring and enforcement of airport pass systems.

Special Emergency Response Team (SERT)

To respond to terrorist incidents where attempts to secure a peaceful resolution have been unsuccessful, the RCMP has established a permanent Special Emergency Response Team. The Team consists of 49 members who can react as a whole or as two equal units. SERT was created under the authority of section 18 of the RCMP Act, pursuant to the RCMP's security enforcement and protective security responsibilities, and its use is subject to Ministerial control and accountability.

CHAPTER VII: FOREIGN INTELLIGENCE

The CSIS Act accords the Service a primary mandate for security intelligence, i.e. the collection of intelligence on threats to the security of Canada. But the CSIS Act also accords CSIS a limited mandate for foreign intelligence, i.e. the collection of information or intelligence on the activities, capabilities and intentions of foreign states and persons. This chapter discusses the Government's general foreign intelligence activities and objectives, the limitations and controls which are applied to them, and the supporting role which CSIS plays in this program.

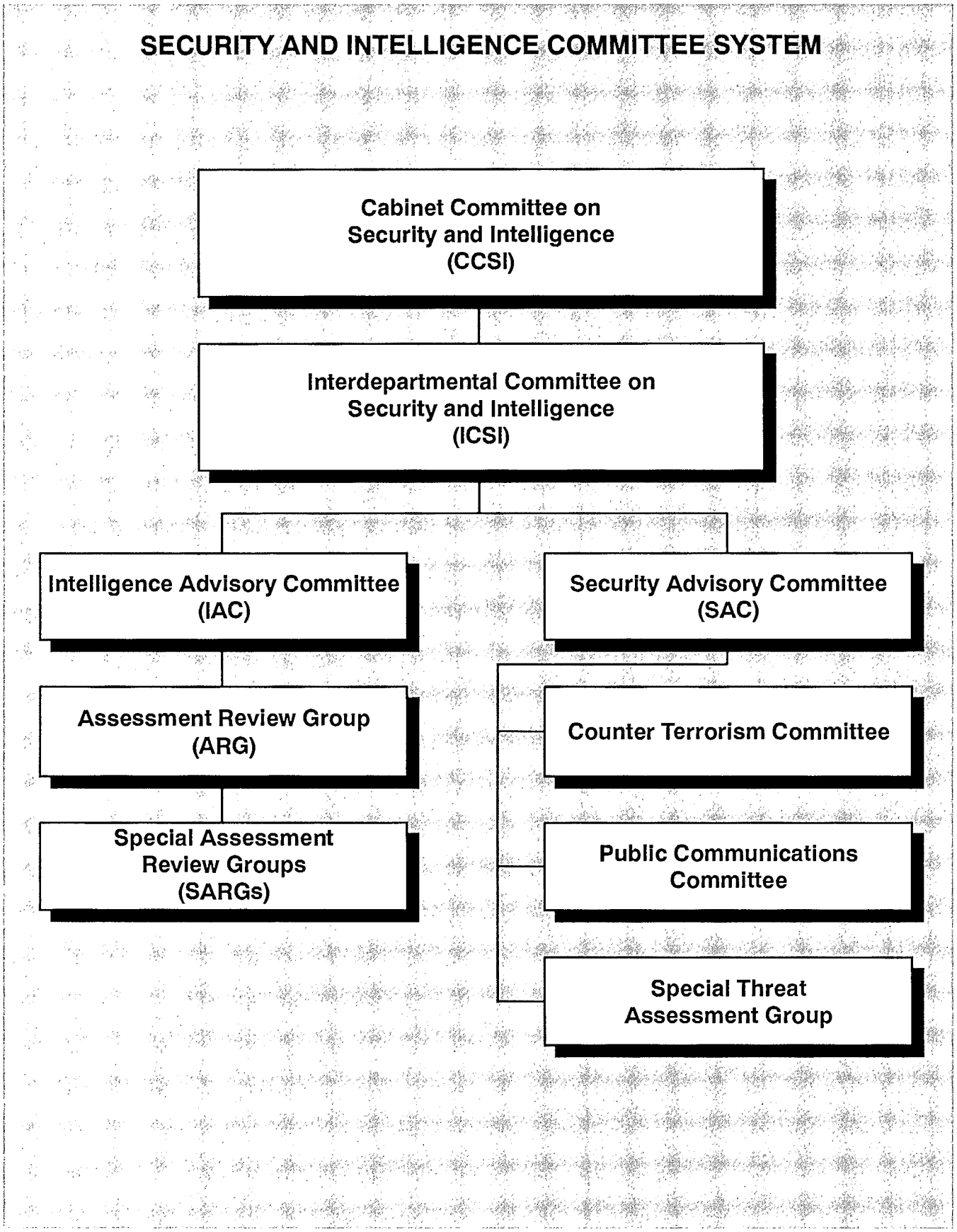
The foreign intelligence activities of departments and agencies other than CSIS were beyond the terms of reference of the Special Committee. But as the Committee made a number of recommendations on broader foreign intelligence issues, some general background is provided to ensure a better understanding of the program.

Foreign Intelligence

Foreign intelligence refers to information or intelligence concerning the capabilities, intentions or activities of foreign states, corporations, or persons. It may include information of a political, economic, military, scientific or social nature, and can produce information with security implications.

Since World War II, the main departments of the Government of Canada active in the foreign intelligence sector have been the Department of External Affairs and the Department of National Defence. These two departments gather information from open sources and through exchanges with allied countries. In addition, the Communications Security Establishment (CSE) intercepts foreign radio, radar and other electronic emissions, and CSIS assists in the collection of foreign intelligence in Canada in accordance with section 16 of the CSIS Act.

Canada's post-war foreign intelligence program was devised to support the country's foreign and defence policy, and it served the country well throughout the era of superpower confrontation. But the world has been changing dramatically in the past two years, and Canada now faces a more complex set of international challenges than


SECURITY AND INTELLIGENCE COMMITTEE SYSTEM
Cabinet Committee on Security and Intelligence (CCSI)
Interdepartmental Committee on Security and Intelligence (ICSI)
Intelligence Advisory Committee (IAC)
Assessment Review Group (ARG)
Special Assessment Review Groups (SARGs)
Security Advisory Committee (SAC)
Counter Terrorism Committee
Public Communications Committee
Special Threat Assessment Group

ever before. As a result, the Government has been reviewing Canada's foreign intelligence program to ensure it continues to meet the Government's needs. Issues such as the identification of foreign intelligence priorities, methods of collecting foreign intelligence, and procedures for assessing intelligence are all being re-evaluated in order to maintain the effectiveness of the program.

Oversight and Coordination

The mechanisms that currently oversee the foreign intelligence sector are effective. At their apex is the Cabinet Committee on Security and Intelligence (CCSI), chaired by the Prime Minister. Its members include those Ministers whose departments and agencies have primary responsibility for security and intelligence policy and operations. CCSI provides policy direction to both the security sector and the foreign intelligence sector. Supporting CCSI is the Interdepartmental Committee on Security and Intelligence (ICSI), chaired by the Clerk of the Privy Council and consisting of deputy minister level officials of departments and agencies active in the security and intelligence field. ICSI receives direction from and assists CCSI in establishing intelligence priorities.

The Prime Minister, the Secretary of State for External Affairs, the Minister of National Defence and the Solicitor General are all accountable to Parliament for the decisions of CCSI and the operations of their respective departments and agencies regarding foreign intelligence matters. The House of Commons standing committees on External Affairs and International Trade, and on National Defence and Veterans Affairs, allow for additional parliamentary consideration of foreign intelligence issues. Foreign intelligence sector departments and agencies are also subject to the scrutiny of the Courts, the Auditor General and the Privacy Commissioner.

The Deputy Clerk (Security and Intelligence, and Counsel), supported by the Security and Intelligence Secretariat in the Privy Council Office, provides overall policy co-ordination for the sector. The Deputy Clerk chairs the Intelligence Advisory Committee (IAC), which is responsible for coordinating the interdepartmental production of foreign intelligence and security assessments. The IAC consists of senior officials from those departments and agencies involved in security and intelligence. It ensures the distribution of intelligence assessments to concerned Ministers, departments and agencies, within an appropriate timeframe.

The Special Committee has suggested that the Government look into the merits of creating a central intelligence assessments office, to provide long-term strategic analyses. However, the IAC system meets current demands for both short-term and strategic

intelligence. The ICSI and the IAC itself monitor and adjust intelligence production procedures to ensure that the product effectively meets users' evolving requirements. In the Government's view, the creation of a national assessments office would be particularly difficult to justify in a time of restraint.

Communications Security Establishment

An important additional element of the government's foreign intelligence program is the Communications Security Establishment (CSE). CSE is under the control and supervision of the Department of National Defence.

The Establishment is responsible for two programs:

- information technology security (INFOSEC); and
- signals intelligence (SIGINT).

Under the INFOSEC program, CSE provides technical advice, guidance and service to the Government on the means of ensuring Federal Government telecommunications security and on aspects of electronic data processing security. Under the SIGINT program, CSE, with the support of the Canadian Forces Supplementary Radio System, collects, studies and reports on foreign radio, foreign radar and other foreign electronic emissions in order to provide foreign intelligence to the Government.

The Minister of National Defence is accountable to Parliament for CSE. The Minister approves CSE's major capital expenditures, its annual Multi-Year Operation Plan, and (with CCSI) major CSE initiatives with significant policy or legal implications.

The Chief of CSE is accountable to the Deputy Minister of National Defence for financial and administrative matters, and to the Deputy Clerk (Security and Intelligence, and Counsel) in the PCO for policy and operational matters.

In addition, arrangements have been put in place to ensure that CSE responds to the Government's foreign intelligence requirements in a manner that is lawful, effective and sensitive to changes in international relationships. These include the following:

- CSE has in-house legal counsel from the Department of Justice, and consults with senior Justice officials on legal issues;

- CSE consults frequently with senior officials in the Privy Council Office, the Department of National Defence and the Department of External Affairs;

- CSE is subject to internal Department of National Defence administrative review mechanisms; and

- CSE submits its strategic plan and all new policy proposals for review by ICSI, which in turn reports to CCSI.

Thus, a broad accountability system for CSE is in place. Nevertheless such an accountability system can always be improved and the Government has been considering providing the Minister of National Defence with some additional capacity for review of CSE. Once a decision is taken on the most appropriate approach, an announcement will be made.

CSIS and Foreign Intelligence

CSIS has a limited mandate to assist in the collection of foreign intelligence in Canada.

The Service's foreign intelligence mandate is outlined in section 16 of the CSIS Act. In recognition of the inherent unsuitability of combining in one agency both security intelligence and foreign intelligence functions, section 16 of the CSIS Act provides strict limitations on the Service's foreign intelligence role.

First, CSIS may "assist" in the collection of foreign intelligence, only in response to a request from either the Minister of National Defence or the Secretary of State for External Affairs.

Second, it may only assist in the collection of foreign intelligence "within Canada".

Third, the Service is prohibited from directing its foreign intelligence activities against any Canadian citizen, permanent resident of Canada or Canadian corporation.

SECTION 16 - FOREIGN INTELLIGENCE ASSISTANCE

"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 sub-section (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."

Experience to date has shown that CSIS has fulfilled these responsibilities effectively under the terms of the CSIS Act. In light of the changes which have been taking place in the world, it is clear CSIS will need to continue to provide support to External Affairs and National Defence in the collection of foreign intelligence.

A Canadian Foreign Intelligence Service?

Canada's own foreign intelligence collection resources, coupled with existing intelligence-sharing arrangements with allies, meet national foreign intelligence requirements. But if the international environment evolves to the point where existing arrangements can no longer fully meet national requirements, the Government will have to assess carefully what alternative arrangements might be needed.

The removal of the prohibition against CSIS operating abroad through deletion of the words "within Canada" from section 16 of the CSIS Act - as suggested by the Special Committee - would impinge on the Service's primary mandate for security intelligence. It is also worth noting that the objectives of a foreign intelligence service are fundamentally different from those of a domestic security service. While the former seeks to learn of the capabilities and intentions of foreign states, and must conduct its intelligence gathering activities on the territory of foreign states, the latter is more narrowly focussed on domestic counter-intelligence and counter-terrorism objectives. Different controls are therefore required for the different services. For this reason, the collection of foreign intelligence and security intelligence are separate functions in other Western democracies.

CHAPTER VIII: INVESTIGATING THREATS

In order to fulfil its mandate to report to and advise the Government of Canada on threats to the security of Canada, the Service undertakes counter-terrorism (CT) and counter-intelligence (CI) investigations of various types and durations. This chapter describes the Service's investigative process, including approval and control mechanisms.

LAUNCHING AN INVESTIGATION

CSIS investigations under section 12 of the CSIS Act may originate with information received from any of a variety of sources -- for example, a police force, a foreign security or intelligence agency, a human source or a concerned citizen. Regardless of the point of origin, all CSIS investigations are subject to the same regime of stringent controls imposed by the CSIS Act, Ministerial directions and Service policies. These controls ensure that the "strictly necessary" provision in section 12 is applied, and that investigational techniques are proportional to the gravity and probability of the suspected threat.

Intelligence officers review incoming information and assess the need to target -- that is, launch an investigation into -- the activities of a person, group or organization. After an intelligence officer makes an initial determination that an investigation may be required, a rigorous process of challenges and controls commences. That process starts with the investigator's supervisor and may lead, in the case of investigations involving certain intrusive techniques, to the Federal Court in Ottawa.

Making Targetting Decisions

The Service's targetting policy was substantially revised in 1988. The central feature of the revised targetting policy is the designation of three collection levels -- Level 1, Level 2 and Level 3 -- each with specified investigative techniques and approval procedures.

The investigative approaches associated with these three levels are cumulative, in that techniques and resources used in a higher collection level may also include those of the lower level(s).

Level 1 investigations -- which are for short durations -- enable investigators to collect and retain information from open information sources and, for example, from records held by foreign police, security or intelligence organizations.

Level 2 represents a greater degree of intrusiveness and may, for example, include interviews and limited physical surveillance. Level 2 investigations may be initially approved by a senior CSIS manager in a Region or at Headquarters, but can only be renewed under the authority of a senior operational committee -- the Target Approval and Review Committee (TARC).

Level 3 investigations permit the use of more intrusive techniques. These may include special operations conducted under warrants authorized by the Federal Court under section 21 of the CSIS Act.

The approval of the Solicitor General is required for investigations of the activities of individuals or organizations defined by paragraph 2(d) of the CSIS Act, if the investigative means to be used go beyond open published information.

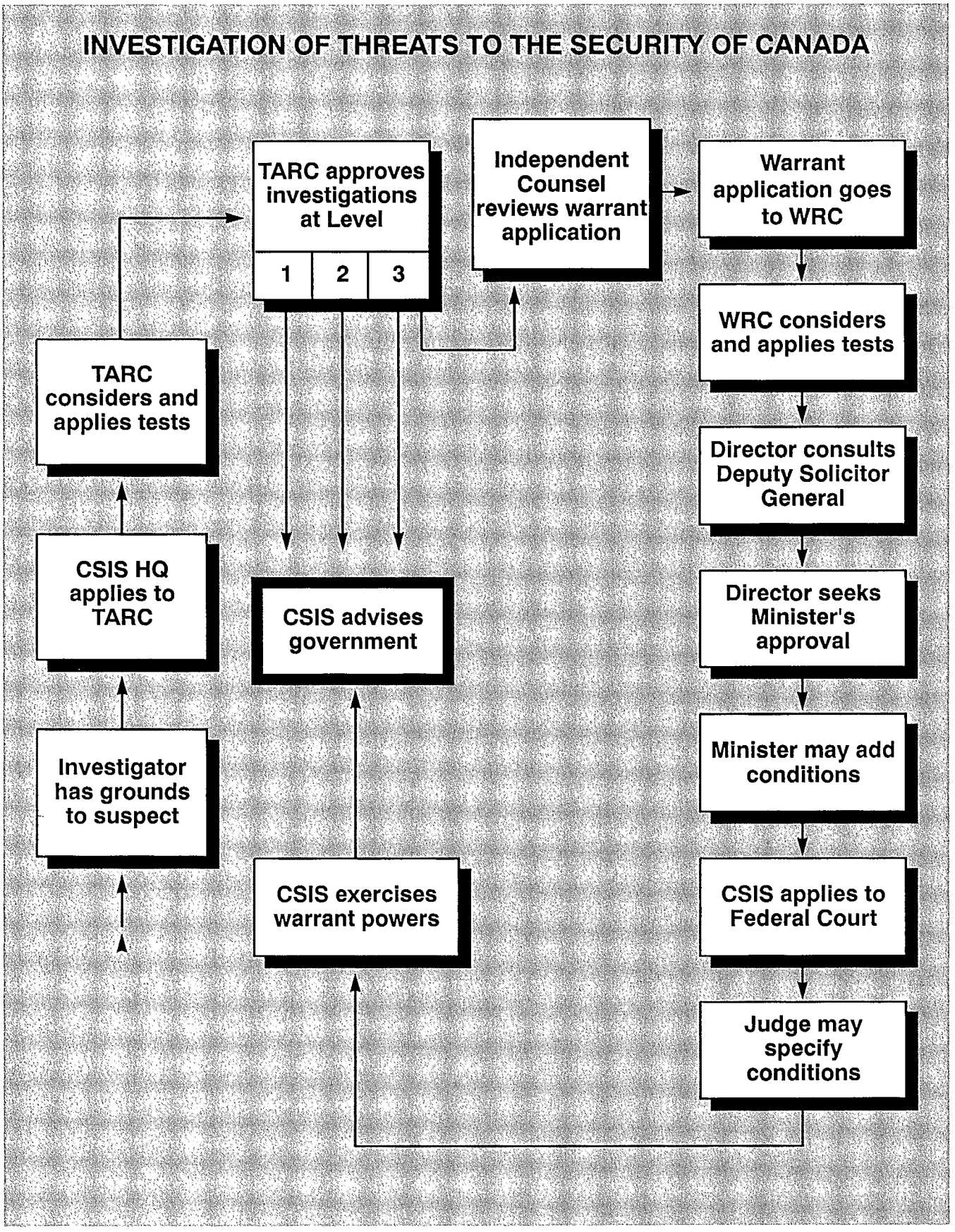
The Service's targetting policy requires officials authorized to approve investigations, including TARC, to:

- consider the reliability and weight of the information supporting the request;

- consider the seriousness and probability of the activities suspected of constituting the threat; and

- weigh the need to investigate against concern for the rights and freedoms of the target, and of any other person who may be affected by the investigation.

All CSIS investigative activities must, of course, abide by Ministerial directions, such as those dealing with the conduct of investigations, the use of human sources and investigations on university campuses.


INVESTIGATION OF THREATS TO THE SECURITY OF CANADA
TARC approves investigations at Level
1
2
3
Independent Counsel reviews warrant application
Warrant application goes to WRC
WRC considers and applies tests
Director consults Deputy Solicitor General
Director seeks Minister's approval
Minister may add conditions
CSIS applies to Federal Court
Judge may specify conditions
CSIS exercises warrant powers
CSIS advises government
Investigator has grounds to suspect
CSIS HQ applies to TARC
TARC considers and applies tests

The Target Approval and Review Committee (TARC)

TARC is chaired by the Director of the Service. It includes senior CSIS managers and representatives from the Ministry of the Solicitor General and the Department of Justice. TARC submissions are prepared, usually in consultation with the Regions, by the appropriate Headquarters Branch and are supported by the Branch Director General before TARC.

At TARC meetings, members consider whether a proposal conforms with law and policy, and assess whether the proposed investigative level and duration are appropriate to the target and the seriousness and probability of the threat. As the Director explained when he appeared before the Special Committee, TARC members are senior officials with the breadth of experience and perspective to make appropriate targetting decisions. Not all TARC submissions are approved, nor do they all survive the TARC process unscathed. Some are approved at lower or higher levels than requested, or for longer or shorter durations, while others are rejected.

The Service's use of certain intrusive techniques is subject to a requirement for prior judicial authorization.

CONDUCTING WARRANT INVESTIGATIONS

In order to employ certain covert and intrusive investigative methods -- mail opening and telephone interception, for example -- CSIS must apply to the Federal Court for a warrant. During appearances before the Special Committee, the Director of CSIS and other government officials described the care taken in the warrant acquisition process and mentioned the many steps involved. In its report, the Special Committee noted that this process, which has undergone extensive adjustments and fine-tuning since 1984, is "working well". The Government shares that opinion.

TARC authority at the highest levels is required in order to apply for a Federal Court warrant. After clearing this hurdle, an investigator prepares a draft application for a warrant for presentation to the Federal Court. The application normally consists of a draft warrant and an accompanying affidavit. Section 21 of the CSIS Act prescribes the

content of the affidavit, which must satisfy a Federal Court Judge that there are reasonable grounds to believe a warrant is required to enable the Service to investigate a threat.

As a consequence of the 1987 Osbaldeston Report, each application for a Federal Court warrant is thereupon reviewed by an Independent Counsel supplied by the Department of Justice. The Independent Counsel meets with the Service's affiant and other CSIS officials who worked on the affidavit to challenge the reliability of the operational information that is essential to support an application. The Independent Counsel must be satisfied that this information:

- is contained in CSIS records;
- appears to be reliable;
- is accurately reflected in the affidavit; and
- is presented in its proper context.

On the conclusion of this review, the Independent Counsel submits a report to the Deputy Solicitor General certifying the elements listed above.

The draft application is then considered by the Warrant Review Committee (WRC) which is chaired by the Director and includes senior CSIS officials, the Independent Counsel and representatives from the Ministry Secretariat and the Department of Justice. The WRC debates the merits of the draft application, considering in particular whether it conforms to law and policy. The Committee subsequently approves, amends or rejects the application.

In accordance with subsection 7(2) of the CSIS Act, the Director consults the Deputy Solicitor General, and the warrant application is discussed at a meeting which the Solicitor General holds with the Director and the Deputy Solicitor General. As a result of this consultation, the Minister may accept the application as presented, request changes in it, impose conditions on the execution of powers being requested, or reject it.

Once approved and signed by the Solicitor General, the warrant application is considered by the Federal Court during a hearing held under appropriate security conditions in a courtroom in Ottawa. In accordance with section 21 of the CSIS Act, the presiding judge may specify "such terms and conditions as the judge considers advisable in the public interest".

The Special Committee recommended that certain protections now provided by judicial conditions be embodied in the governing legislation. The Government's view is that codification would not alter the stringency with which warrant requests are tendered and treated, and could reduce the Court's flexibility to tailor conditions to meet the needs of particular requests for powers. The Government is, however, studying the merits of consolidating existing practices in a Ministerial direction.

The CSIS Act establishes maximum allowable periods for the duration of warrants issued by the Federal Court. The duration finally set by the Court reflects the specific requirements of the investigation. In considering what duration to request, investigators carefully observe the principle of proportionality that guides all CSIS investigations. Further consideration of the appropriate duration is given at the WRC and by the Solicitor General before granting approval for the application to go forward to the Court.

As explained above, there are many checks, balances and control mechanisms in place to regulate investigations. The Government is of the view that the appearance of an amicus curiae or "devil's advocate" at Federal Court hearings, as recommended by the Special Committee, would not enhance the rigour of the CSIS warrant application process. Similarly, given the comprehensive body of rules and procedures now governing warrant applications, the Government believes that specific regulations embodying these are not presently required.

The Special Committee also expressed concern about the adequacy of physical security in facilities being used by the Federal Court for warrant hearings. Although temporary secure facilities now made available are adequate, the Government supports the view that a more appropriate arrangement would have the secure premises co-located with the Federal Court Building. Plans to accomplish this are underway.

CSIS Warrants and the Charter

The Government is sensitive to concerns that the warrant provisions of the CSIS Act may not be sustainable under the Canadian Charter of Rights and Freedoms.

Since the coming into force of the Charter, both Parliament, in enacting legislation, and the Government, in implementing legislation, have taken seriously their responsibilities to ensure that both existing laws and new statutory measures conform with the Charter.

The Government is particularly aware of its responsibility with respect to the warrant provisions of the CSIS Act, given the intrusiveness of the powers sought by the Service. For this reason, the Government has put in place a stringent set of internal controls to ensure that scrupulous care is taken in the use of these powers, and has kept the warrant process fully up to date with evolving jurisprudence on the Charter.

As the Special Committee noted, this jurisprudence includes the case of Atwal v. The Queen, in which the courts have:

- found the warrant provisions of the CSIS Act sustainable under the Charter; and
- acknowledged that standards applicable to law enforcement matters may not be appropriate or applicable to security intelligence matters.

The Government believes that there is no present need to undertake a review of the findings of the courts in the Atwal case on the constitutionality of the warrant provisions. However, the Government will continue to monitor the findings of the courts to ensure the warrant regime remains consistent with evolving jurisprudence.

Requirement for a Warrant

The Government will seek judicial authorization for the use of a particular investigative technique when it is reasonable to assume that the use of that technique by the state will interfere with or intrude upon a recognized constitutional expectation of privacy on the part of an individual. Thus, a warrant will be sought in cases where the use of such a technique might otherwise contravene a statutory prohibition and where the Charter places constraints on the state's use of such a technique.

The Special Committee recommended that the CSIS Act be amended to include "participant surveillance" -- electronic surveillance consented to by a participant in a private communication -- within the warrant provisions. As a result of the Supreme Court decision in the case of Duarte v. The Queen, CSIS took steps to include the investigative technique of participant surveillance within the warrant regime. The Government is of the view that statutory amendment is unnecessary, given the decision of the Supreme Court.

Both the Special Committee and SIRC have recognized that it is neither necessary nor appropriate to require prior judicial authorization for the use of human sources. The Government is of the view that the use of certain other investigative powers should

also continue to be controlled through Ministerial direction and Service policy, rather than through judicial means.

The Role of SIRC and the Inspector General

All CSIS operations may be reviewed and monitored by the SIRC and the Inspector General. The Special Committee recommended that SIRC be authorized under the CSIS Act to compile and publish warrant statistics. The Government fully supports keeping the public and Parliament as informed as possible on Service activities, where these activities have a significant potential for intruding on individual rights and freedoms. The Government believes, however, that particular care must be taken with information which requires protection in the national interest. The Government supports SIRC's current practice of reporting warrant statistics in its Annual Report.

CHAPTER IX: EXTERNAL REVIEW AND COMPLAINTS

The Security Intelligence Review Committee (SIRC) conducts independent external review of CSIS.

Independent external review is an innovative and important component of the national security system established by the CSIS Act. Responsibility for this function was given to the Security Intelligence Review Committee (SIRC), a non-partisan committee of Privy Councillors. The 1984 legislation assigned three main tasks to SIRC:

- to review CSIS performance of its duties and functions;
- to investigate and report on complaints with respect to "any act or thing done" by the Service; and
- to investigate complaints concerning denials of security clearances, and denials of citizenship or immigration status based on security considerations.

These are challenging and demanding tasks. SIRC members and staff have performed them well over the years, providing a valuable service to the Government, Parliament and the Canadian people.

The Special Committee has made a number of recommendations for statutory amendment which would expand SIRC's role. Given SIRC's importance as presently constituted, the Government does not agree with these proposed amendments. In the Government's view, they would have the effect of either diffusing SIRC's functions with respect to CSIS or diminishing Ministerial accountability. Several other issues raised by the Special Committee in respect of SIRC are currently before the Courts. The Government does agree, however, with some of the Special Committee's recommendations regarding the SIRC appointment process.

This chapter describes SIRC's current functions and provides the Government's position on many of the Special Committee's recommendations regarding SIRC.

THE ORIGINS OF SIRC

When the CSIS Act was being drafted, it was recognized that the success of the new national security system would depend largely on Parliamentary and public confidence in the integrity of the system. Several options for providing independent external review of the Service's performance of its mandate were considered.

One option was to assign the independent external review function to a committee of Parliament. There would be practical difficulties, however, in providing legislators with direct access to information about CSIS operations, much of which simply could not be disclosed publicly, including third-party information and information about:

- CSIS capabilities, techniques and investigative methods;
- ongoing operations;
- technical sources;
- the identity of targets; and
- the identity of human sources.

Moreover, within the Canadian parliamentary system, legislators have traditionally been free to publicly use information, from whatever source, in discharging their duties to their constituents, their parties and the House. Providing parliamentarians with classified documents, or creating a permanent parliamentary structure with national security responsibilities, it was believed, could inhibit the independence of legislators.

Another option, therefore, was selected -- the SIRC option. SIRC was established as a surrogate for Parliament. It consists of Privy Councillors who are not sitting members of either the House of Commons or the Senate. SIRC has full access to CSIS information, except Cabinet confidences, and is free to investigate all aspects of CSIS operations. Though required to maintain confidentiality, SIRC submits public annual reports.

Specific tasks spelled out for SIRC in the CSIS Act fall into two broad categories -- review and complaints.

SIRC'S REVIEW MANDATE

SIRC's review role is a cornerstone of the accountability framework established by the CSIS Act.

CSIS has a statutory mandate and a framework of Ministerial direction which recognize that its activities are sanctioned by law and are to be conducted in accordance with the rule of law, including the Charter. For its part, SIRC has a mandate to review the propriety of CSIS activities, with emphasis on the delicate balance between national security and individual freedoms.

Section 38 of the CSIS Act directs SIRC to review generally the performance by the Service of its duties and functions. This includes reviewing:

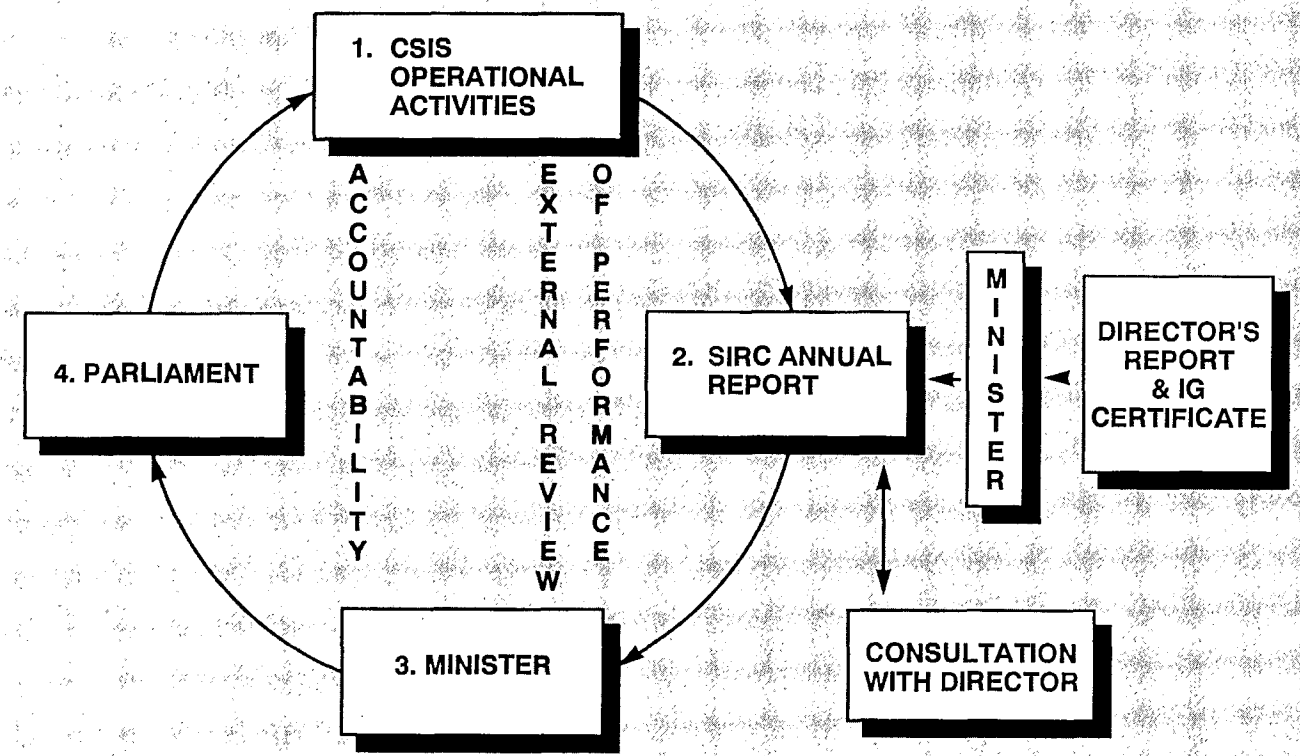
- CSIS Annual Reports and certificates of the Inspector General;
- Ministerial direction;
- CSIS arrangements with domestic and foreign governments and agencies;
- section 20 reports on unlawful conduct; and
- regulations.

Section 40 of the legislation makes SIRC responsible for reviewing the Service's compliance with the CSIS Act, its regulations and Ministerial direction, as well as reviewing CSIS activities to ensure they do not involve an unreasonable or unnecessary exercise of powers.

Related functions set out in the legislation include monitoring requests for CSIS to assist in the collection of foreign intelligence, and compiling and analyzing statistics on the Service's operational activities.

SIRC's review role is an ex post facto one. Were SIRC to become involved in the day-to-day operations of the Service, it could find itself in the invidious position of having to account to Parliament for the management and operations of CSIS. The CSIS Act clearly provides that this is the responsibility of the Minister. The Government believes the balance of the CSIS Act should not be altered in any way that would diminish Ministerial responsibility -- either in principle or in practice.

EXTERNAL REVIEW CYCLE



SIRC Reports

SIRC reports on its review work to the Minister, Parliament and the public. Under section 53, SIRC must provide the Solicitor General with an Annual Report, which the Minister must then table in Parliament. Section 54 also permits SIRC to furnish the Solicitor General with special reports, either on its own initiative or at the Minister's request.

SIRC consults the Director to ascertain if portions of its reports or statements should not be made public on the grounds of national security. In addition to the specific provisions found in the CSIS Act, the Access to Information Act provides guidance in deciding such matters. In the event of a dispute between SIRC and the Director, the matter would be referred to the Solicitor General for further consideration.

Given the principle of Ministerial accountability, the Government believes the SIRC Annual Report should continue to be referred to the Minister for tabling in Parliament.

SIRC and Ministerial Responsibility

Parliament, through SIRC, has a window into the policy regime governing CSIS. SIRC, by its Annual Reports, ensures that Parliamentarians have an opportunity to pose informed questions to the Minister about CSIS.

When Ministerial directions are issued to the Service, copies are immediately forwarded to SIRC, which has a statutory responsibility to review them. Given the role of SIRC to provide independent external review, the Government believes it would not be appropriate for SIRC to be directly involved in the government's policy-making process.

SIRC has provided the Minister and Parliament with its opinion of various Ministerial directions. The Minister, however, is responsible for determining if the range and impact of direction are adequate and appropriate, and is accountable to Parliament for this. Chapter X addresses this subject.

The Special Committee has recommended that SIRC be given access to Cabinet confidences. Government direction is provided to CSIS through the vehicle of Ministerial direction. SIRC receives copies of such direction by statute and, in addition, has access to all documents under the control of the Service, except Cabinet confidences. The Government sees no need to depart from the longstanding practice of protecting the confidentiality of Cabinet documents.

Effectiveness, Efficiency and Financial Review

To date, SIRC has not felt constrained from commenting on a wide variety of topics arising from its review function. The Special Committee recommended, however, that the CSIS Act be amended to provide SIRC with an explicit mandate to monitor and review the effectiveness and the efficiency of the Service.

The Government is responsible for the direction, control and management of CSIS and for accounting to Parliament for the performance of the Service. Key elements of the Government's responsibility are its ability to ensure CSIS compliance with law and policy, and to assess and promote effectiveness and efficiency in the way CSIS performs its functions.

The Special Committee also recommended that the CSIS Act be amended to authorize SIRC to undertake financial reviews of the Service in conjunction with the Auditor General.

The Government is of the opinion that the "value for money" audit carried out by the Auditor General is a clearly established, specialized role, applied comprehensively and consistently across Government. The Auditor General is responsible for providing Parliament with information on the Government's use of public funds and is mandated to "call attention to anything that he considers to be of significance and of a nature that should be brought to the attention of the House of Commons". The Auditor General's office has the resources, knowledge, skills and independence to carry out this function responsibly.

The Auditor General's role is different and distinct from that assigned to SIRC. To establish a statutory involvement for SIRC in the functions of the Auditor General could result in duplication. It would be unfortunate, in the Government's view, to foster confusion regarding the functions of the two agencies.

The Government's position is that it would be injurious to national security to publicly reveal details of CSIS expenditures, on the grounds this would reveal operational capabilities to CSIS targets. Financial accountability is a key element of Ministerial responsibility. As Ministers are answerable to Parliament for managing their departments and agencies, Parliament is entitled to expect Ministers to assure Parliament that internal and external accountability systems are in place to provide independent, objective assessments of the Government's use of public funds.

SIRC'S COMPLAINTS FUNCTION

SIRC's second major function is that of a complaints tribunal -- to investigate complaints that anyone makes about the activities of the Service, complaints about the denial of security clearances in Public Service employment, in the supply of goods and services to the Federal Government and in immigration and citizenship matters, as well as to investigate the security aspects of complaints lodged with the Canadian Human Rights Commission.

To enable SIRC to investigate complaints, certain powers and responsibilities were included in the CSIS Act. These have been amplified by "Rules of Procedure" developed by SIRC. This regime requires that:

- SIRC must notify the Director and relevant Deputy Head on the commencement of an investigation, except when the Director is notified pursuant to section 41;

- SIRC must conduct its investigations in private; and

- SIRC may summon witnesses and receive evidence. In performing this function, SIRC has a right of access to all information under the control of CSIS and the Inspector General, with the exception of Cabinet confidences, that is relevant to the conduct of the investigation.

Section 41: "Any act or thing done by the Service"

Pursuant to section 41 of the CSIS Act, an individual may complain to SIRC about "any act or thing done by the Service". The complainant must first bring the complaint to the attention of the Director. Should the Director not respond within a reasonable period of time, or should the complainant be dissatisfied with the Director's response, SIRC is required to investigate the matter.

The Report of the Special Committee reflects concern about the possible "deterrent" effect of requiring individuals to complain first to the Director. The purpose of requiring the initial approach to be made to the Director is to allow the Director to respond to and resolve the complaint to the satisfaction of the complainant before requiring the complainant to embark upon a potentially lengthy and costly complaint to SIRC.

Nonetheless, the complainant can bring the matter to the attention of SIRC if the complainant is dissatisfied with the Director's response. To dispense with the requirement of first notifying the Director would diminish the Director's effective managerial control and accountability. Nor would this recommendation necessarily save time on the part of the complainant, for the Director may be able to solve the complaint expeditiously and to the satisfaction of the complainant. Any remedial action the Director might institute as a consequence of the complaint would be reviewed by SIRC.

Section 42: Security Clearance Complaints

Section 42 of the CSIS Act provides a right of complaint to SIRC for individuals who have been denied employment, or have been dismissed, demoted or transferred solely on account of the denial of a security clearance. The Government officials responsible for granting or denying security clearances are identified in section 29 of the CSIS Act. These officials -- referred to as "Deputy Heads" -- include deputy ministers of departments, heads of certain agencies and, for the remainder of the Public Service, persons designated by Order in Council. A Deputy Head who denies a clearance is required to notify the individual of the denial. SIRC is then obliged to investigate any complaint the individual may make following the denial of the security clearance.

The Special Committee has recommended that a right of access to SIRC pursuant to section 42 be broadened to include any individual who is denied a clearance.

Individuals who do not currently enjoy a right of access to the complaints procedures of section 42 following the denial of a security clearance have another avenue of redress through the Federal Court. The Government acknowledges, however, that the current situation is less than satisfactory. The Government undertakes to review and consider the most appropriate remedies available in legislation or policy to extend access to individuals who believe their rights have been denied. In the meantime, the availability of Federal Court review does provide some relief to such individuals.

The Special Committee also raised concerns relating to the delays in processing security assessments by the Service. It suggested that a right of complaint to SIRC under section 42 might be a means of redress.

The Government is aware of the difficulties experienced by individuals as a result of delays in completing security assessments. Additional resources have been allocated

to address this problem. As the Special Committee acknowledges, CSIS has made "significant headway" in reducing the number and length of delays and, in fact, many of the causes of delay are beyond the control of the Service.

The Special Committee supports the notion that the recommendations of SIRC following a complaint under section 42 of the CSIS Act be binding on Deputy Heads. This matter is currently the subject of litigation. The Federal Court of Appeal has held that such SIRC recommendations are binding on a Deputy Head, but the Government has been granted leave to appeal this decision to the Supreme Court of Canada.

A cornerstone of sound security management throughout the government is the accountability of Deputy Heads. This principle is recognized through the specific authority assigned to Deputy Heads to grant or withhold security clearances. If SIRC rulings in respect of security clearances were final and binding, Deputy Heads and Ministers would be obliged to hire a person whom they distrust. If such a person were later to commit a serious breach of security, the question would arise as to who should take responsibility.

CSIS, not the Deputy Head, carries out the investigation necessary to a consideration of the granting of a security clearance. SIRC, in its review of the Service's investigation, may compel witnesses to attend and may complete investigations. SIRC then presents its findings and "recommendations" to the Deputy Head. The final decision must remain, however, with the Deputy Head and the Minister who are required to protect and control access to the classified information within their control.

Assistance to Complainants

The Special Committee has raised concerns that complainants may not have access to independent legal advice when appearing before SIRC. It has proposed that SIRC be given authority to offer assistance or to award costs in certain circumstances.

The Government believes this question needs to be addressed on a Government-wide basis. The costs of extending powers to provide assistance or award costs across the broad range of federal tribunals would be significant and could not be undertaken without careful study.

Federal Court Review

The Special Committee suggested that the provisions in the Federal Court Act allocating jurisdiction for review of SIRC proceedings are confusing and should be clarified by allocating jurisdiction to the Federal Court of Appeal. The Committee also proposed that procedures be developed to facilitate the transfer of files and documents.

Recent amendments to the Federal Court Act have clarified this situation by vesting exclusive jurisdiction for review of SIRC proceedings with the Trial Division. The matter of Federal Court access to information is being considered by an interdepartmental technical working group and is also before the Courts.

SIRC'S JURISDICTION AND MEMBERSHIP

The Special Committee has suggested SIRC should review the operations of other agencies and other functions. The Government believes such an expansion of SIRC's mandate could diminish its capacity to perform its current statutory role. Moreover, other departments and agencies in the security and intelligence sector are already subject to controls and review suited to their mandates. These controls are exercised by Ministers, the Courts, and internal and external review agencies, including the Commissioners for Privacy, Access to Information and Human Rights. To the extent that CSIS interacts with other agencies of Government, these relationships fall within SIRC's purview.

The Special Committee has made several recommendations relating to the size of SIRC and method of appointment of SIRC members. The CSIS Act provides that SIRC should consist of a chairman and no fewer than two and no more than four members. All of these individuals are to be members of the Privy Council who are not sitting members of the House of Commons or Senate. The Governor in Council makes SIRC appointments, after consultation by the Prime Minister with the leaders of main opposition parties in the House.

The Government recognizes the need for consultation with opposition leaders regarding appointments to SIRC. The Government also agrees with the Special Committee's recommendation that appointments to SIRC continue to be staggered and that appointees be subject to being called before the Standing Committee. In the Government's view, provisions regarding the number of SIRC members cover both present and anticipated requirements.

CHAPTER X: PARLIAMENT AND THE PUBLIC

The review of the CSIS Act and the Security Offences Act by a Special Committee of the House of Commons recognized the important role elected representatives play in the national security system. To ensure on-going parliamentary scrutiny of Canada's national security system, the Acts relied on Ministerial accountability to Parliament and on external review by SIRC.

To give effect to the principle of accountability, the Solicitor General and senior officials have appeared regularly before the House of Commons Standing Committee on Justice and the Solicitor General -- as the Special Committee noted in its report. In addition, the Government conveyed a considerable amount of information to the Special Committee, which had not previously been available, to assist it in its review.

SIRC is also accountable to Parliament, through the Annual Reports it must submit -- to the Minister and through the Minister to each House -- on its activities during the preceding year. As explained in Chapter IX, SIRC was created in large part to act as Parliament's surrogate in the sensitive area of security intelligence, and the CSIS Act conferred on it broad powers to review the Service's performance of its duties and functions. In its report, the Special Committee expressed the view that SIRC had served it well in identifying issues of current concern to Canadians.

Building Confidence

Because these accountability arrangements have been working well, the Government believes they should be left intact. But the Government recognizes that effectiveness is not the whole story; there must also be confidence, on the part of Parliament and the public, that the national security system is functioning in the best interests of the country.

Confidence, in turn, is a function of knowledge. As the Solicitor General observed when testifying before the Special Committee, security requires secrecy for effectiveness, but there must not be secrecy for secrecy's sake. To refuse to discuss national security issues publicly with Canadians is to encourage mistrust and ignorance.

The challenge is to achieve both effectiveness and confidence, by finding an acceptable trade-off between secrecy and openness. The following outlines the ways the Government will pursue this objective.

Informing Parliament

The Government believes Parliament can be provided with more information on the national security system and undertakes to make more information publicly available, as has been done throughout On Course.

Government officials will, of course, continue to respond as positively as possible to questions put to them when called to appear before the Standing Committee on Justice and Solicitor General to brief Parliamentarians on particular security issues. Officials testifying before parliamentary committees will still be bound by obligations to their Minister, and to the Government, not to disclose information that is confidential on grounds such as national security, privacy or advice to Ministers. The only person who may in some instances, have some discretion in deciding to release such information is the Minister and officials should not be criticized for abiding by their obligations.

An Annual Ministerial Statement on National Security

The Government agrees with the Special Committee that the annual release of a report on security intelligence matters, which could be tabled in Parliament, could contribute significantly to informed public debate. Therefore, at the time of tabling of the Main Estimates, the Solicitor General will provide Parliament -- beginning in 1992 -- with an annual statement on the national security issues that face our country. This statement will discuss the major national security issues that were dealt with during the previous year, and highlight directions for the year ahead.

The Minister's statement will be accompanied by a public Annual Report from the Director, which will include a discussion of the threat environment.

Making Direction Public

The Government also agrees with the Special Committee that greater openness in respect of Ministerial direction would help build confidence in the existing control and accountability mechanism.

In the early 1980s, most of the Ministerial directions being issued sought to focus the activities of the Service. Many were highly classified, on the grounds that public disclosure of the constraints applying to security intelligence operations would assist adversaries in defeating them. This remains the Government's view. But more recent Ministerial directions have dealt with matters that did not need to be highly classified, and the contents of some of these have since been made public by Ministers. A notable example was the direction on national requirements for security intelligence, the essential elements of which were made public by the Solicitor General in a speech in 1989.

The Government believes that the existing CSIS Act provision, which exempts Ministerial direction from automatic parliamentary review under the Statutory Instruments Act, should be maintained. As noted earlier, SIRC is given copies of Ministerial directions. But the Government is also prepared to make the main policy principles of key Ministerial directions available to Parliament and the public. Chapters II and V convey a great deal of this information, and the Solicitor General's annual statements can serve to keep Parliament abreast of new directions as they are issued.

A Second Review by Parliament

Five years was not a long time to implement legislation creating important new institutions. As the foregoing indicates, the Government fully supports the idea of providing Parliament with more information to help it meet its responsibilities, but the Government is unwilling at this time to contemplate structural changes which could upset the balance of the national security model inaugurated in 1984. While changes might be required in future, the Government believes it would be premature to consider such steps as augmenting the powers of SIRC or creating a permanent parliamentary sub-committee to oversee security intelligence issues -- possibly to the detriment of the independence of the legislators who might thereby be vested with some "accountability" responsibilities of the executive arm of government.

The Special Committee itself was reluctant to make a comprehensive recommendation on how Parliament should review security issues over the long term. But it did propose two options, one of which was another review of the CSIS Act and the Security Offences Act by Parliament. The Government accepts that idea and undertakes to arrange for another parliamentary review beginning in 1998.