



Solicitor General  
Canada

Solliciteur général  
Canada

---

---

# **PEOPLE AND PROCESS IN TRANSITION**

---

---

**Report to the Solicitor General  
by the Independent Advisory Team  
on the Canadian Security Intelligence Service**

**Canada**

---

---

**PEOPLE AND PROCESS  
IN TRANSITION**

---

---

**Report to the Solicitor General  
by the Independent Advisory Team  
on the Canadian Security Intelligence Service**

October 1987

Published under the authority of the  
Hon. James Kelleher, P.C., M.P.,  
Solicitor General of Canada

Produced by the Communications Group  
Ministry Secretariat

© Minister of Supply and Services Canada 1987

Cat. No. JS42-33/1987

ISBN 0-662-55530-9

"CSIS is a new and important institution deserving our support and understanding. We would affirm, in the strongest possible terms, that it is a vital and necessary part of the protection of those democratic ideals and principles upon which our nation is built."

Independent Advisory Team, October 1987

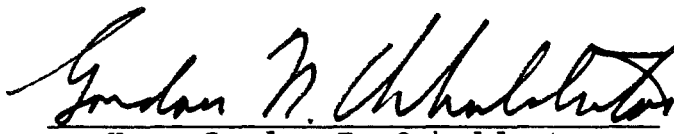
October 28, 1987

Honourable James Kelleher, P.C., Q.C.  
Solicitor General of Canada  
Sir Wilfrid Laurier Building  
Ottawa, Ontario  
K1A 0P8

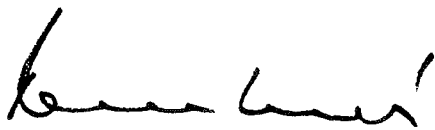
Mr. Minister:

We have the honour to submit herewith our report on matters respecting the Canadian Security Intelligence Service, which you directed us to examine on July 22, 1987. We trust that this report meets your requirements and we remain at your disposition.

Respectfully submitted,



Hon. Gordon F. Osbaldeston



Roger Tassé, Q.C.



Gérard G. Duclos

## CONTENTS

	<u>PAGE</u>
INTRODUCTION	1
A NECESSARY COMMENTARY	3
EXPECTATIONS FOR CSIS	5
PEOPLE - VISION AND CHANGE	10
Recommendations	15
THE INTELLIGENCE PRODUCT	18
Recommendations	20
COUNTER-SUBVERSION - THE SECURITY INTELLIGENCE NET	22
Recommendations	25
THE SECURITY INTELLIGENCE FRAMEWORK	27
Recommendations	28
OTHER MATTERS	29
Recommendations	30
SUMMARY OF RECOMMENDATIONS	32
GLOSSARY OF TERMS	39

---

### Appendices

- A Terms of Reference
- B List of People Interviewed

## INTRODUCTION

### Background

On June 29, 1987, the Solicitor General tabled in the House of Commons the third Annual Report of the Security Intelligence Review Committee (SIRC). In its report, the Committee raised a number of concerns about the Canadian Security Intelligence Service (CSIS). On July 22, the Solicitor General announced the formation of an independent advisory team, headed by the Honourable Gordon Osbaldeston and with Mr. Roger Tassé, Q.C. and Mr. Gérard Duclos as members. The Advisory Team was directed to develop an action plan by October 30, 1987 to address two specific issues raised by SIRC.

The first issue was whether CSIS policies on recruitment, training and development, and personnel management have provided the Service with the proper mix of skills, education and experience to meet the intelligence needs of the Government.

The second issue was whether CSIS operational policies concerning targetting, particularly in counter-subversion, have balanced effectively the needs of the state and the rights of individuals.

Also, the Advisory Team was directed to assess the requirement for further studies or action, as it deemed appropriate. (Terms of reference are attached as Appendix A.)

### Object

The object of this report is to make recommendations to the Solicitor General for the implementation of an action plan which addresses specifically the two issues outlined above, as well as other matters that have come to our attention during the course of this review.

### Methodology

We divided our work into two stages: an information gathering stage and, after preliminary conclusions had been reached, a challenge stage. The first stage comprised an intensive series of interviews, supplemented by considerable research, both of the available literature and of statistical and other information

provided by CSIS. A total of 107 interviews were carried out. (A list of those interviewed may be found at Appendix B.)

As the information gathering stage progressed, a number of trends began to appear, and tentative conclusions emerged. At this point, the Team began a challenge round of briefings. This round involved a more limited group of interlocutors, among them the Security Intelligence Review Committee, the Director of CSIS, the Deputy Solicitor General, the Inspector General, and the Intelligence and Security Coordinator. Their comments and suggestions helped shape this report.

### Acknowledgements

The Advisory Team wishes to thank everyone who was interviewed, often at some inconvenience to themselves. We especially note the willing cooperation of CSIS, which opened its organization to our critical gaze. We also thank the Solicitor General's department for providing the administrative support that we needed. We wish to make special mention of Mr. Alister Hensler of CSIS, who spent many hours acting as our official liaison officer.

Finally, we wish to express our great appreciation to the staff who worked directly with us and without whom we could not have done as much as we needed to do in the limited time available. This small staff was loaned from the Privy Council Office, the Office of the Comptroller General, the Ministry of the Solicitor General, and the Department of Justice and we thank those organizations most sincerely for making them available.



A NECESSARY COMMENTARY

We agree with SIRC when it notes that the dedication and professionalism of CSIS employees is impressive.(1) The CSIS Act created a framework, including the Service itself, the ultimate purpose of which is to protect the liberal democratic ideals upon which our country is based. In gathering the security intelligence required to protect ourselves against activities threatening these ideals, however, every precaution must be taken to ensure that individual rights are not unnecessarily infringed. The gathering of security intelligence and the protection of individual rights will be, at times, in conflict and their consistent and concurrent implementation presents a formidable challenge in judgement. Despite some widely publicized incidents, we believe that CSIS and its members are carrying out a necessary and often difficult function in a generally creditable manner.

It should not be forgotten that the proclamation of the Act created an organization that assumed immediate responsibility for the security intelligence role. Although CSIS drew most of its operational component from the Security Service of the RCMP (referred to hereafter as the Security Service), a number of new requirements were also created, many of which had to be provided from scratch. Among them were a complete management structure, an administrative system to provide the support previously drawn from the RCMP, accommodation separate from the RCMP, new communications and computer systems, and a methodology for dealing with a complicated system of external review. All of this was to be provided, as a former member of CSIS management put it, "on a shoestring." The turmoil generated in simply getting CSIS established is a factor often overlooked by the critics.

The upheaval of separation and the unaccustomed glare of what has become a very public review process have had serious adverse effects on the morale of the Service. The level of criticism has been quite high, particularly in the past year. Insofar as such criticism is well-founded, it is incumbent upon the Government and upon the management and employees of CSIS to do everything possible to correct what is wrong.

Some of the criticism, however, has been misinformed or has not presented all sides of the issue. In such cases, those of us in a position to do so must set the record straight. Otherwise, legitimate criticism of the manner in which CSIS has acted in specific instances can be distorted into a generalized attack on

---

(1) Annual Report 1986-87, page 3

the Service itself and on the function it performs. Such attacks, if unanswered, could erode CSIS morale to the point where it is irretrievable. Should this happen, Canadian national security would be at risk.

As Canadians, we should take comfort from the fact that the checks and balances put in place by the CSIS Act are working. It is largely because of them that the Advisory Team was formed by the Solicitor General.

Those who undertake to minimize the change brought about by the 1984 separation, or who seek to use our recommendations as evidence of failure, are simply not accepting the reality of the world in which CSIS must live. We can find no evidence that the CSIS Act, or the structures it established, are inappropriate. We do not believe that the Parliamentary review should be undertaken at any earlier date than 1989, as provided for in the Act. We have addressed the issues of implementation and are convinced that the job can be done within the present legislation.

Finally, CSIS is a new and important institution deserving our support and understanding. We would affirm, in the strongest possible terms, that it is a vital and necessary part of the protection of those democratic ideals and principles upon which our nation is built.

EXPECTATIONS FOR CSIS

The McDonald Commission

The catalyst that led to the establishment of the Canadian Security Intelligence Service was the Commission of Inquiry Concerning Certain Activities of the RCMP, known as the McDonald Commission. The Commission Report, published in 1981, provided the background from which much of the CSIS Act was drawn and the policy base for most of what CSIS does and how it should do it. To determine the expectations of the Government and of Canadians in general for CSIS, one must begin with the McDonald Commission and its Report.

The McDonald Commission recognized, as had the 1968 Royal Commission on Security (MacKenzie Commission) before it, fundamental differences between security intelligence work and police work. At the risk of oversimplifying what is a complex issue, we characterize the major differences as follows:

- police deal with facts (evidence), usually after an event, whereas security intelligence agencies try to anticipate events;
- police forces must have a degree of independence from Government control, whereas security intelligence agencies require closer control to ensure that individual rights are not unnecessarily infringed, and when they are infringed, to ensure that political accountability exists;
- police activities are subject to an extensive and detailed set of rules (the Criminal Code and jurisprudence), while security intelligence activities, although provided for in the CSIS Act, involve greater judgement in their implementation; and finally,
- a security intelligence agency must keep its Government informed of threats to national security, while police work will normally culminate in evidence being laid before a Crown Attorney for presentation to the Court.(2)

---

(2) see also Freedom and Security under the Law, the second report of the McDonald Commission, page 420, paragraph 20.

Recognizing these distinctions, the MacKenzie Commission recommended separation of the Security Service from the RCMP. The government of the day did not accept the recommendation but opted instead to develop "a distinct and readily identifiable element (within the RCMP)..... increasingly separate in structure and civilian in nature" (as stated by then Prime Minister Trudeau in the House of Commons on June 26, 1969). Twelve years later, the McDonald Commission, noting that little real progress had been made, again recommended separation. McDonald's arguments for so doing were simple. In its preamble to the recommendation for a separate security intelligence agency, the Commission's Second Report stated that without separation the RCMP would vigorously resist (as it had in the past) two changes that the Commissioners felt were "absolutely crucial if the agency was to perform effectively in a lawful and proper manner:

- a) implementing management, recruiting and other personnel policies appropriate to a security intelligence agency, and
- b) developing suitable structures and procedures to ensure that the security intelligence agency is under the direction and control of government."(3)

The Commissioners were seeking the establishment of a security intelligence agency that was accountable, responsive to the principles of law and more in tune with the times. They expected the new agency to be capable of exercising a reasonable level of judgement in selecting targets and assigning investigative resources to those targets. Targetting decisions were recognized as difficult, especially when the line between subversion and legitimate dissent had to be drawn, but the Commissioners strongly believed that such decisions were necessary if the Canadian democratic system was to be adequately protected. The Commissioners believed that two things were essential if the line between subversion and legitimate dissent was to be properly drawn: well-defined and clearly communicated Government policies, and sophisticated judgement and political understanding on the part of the agency and its employees.

In order for the new agency to meet their expectations, the Commissioners assumed four prerequisites: strong direction and leadership from the Minister and his deputy, supported by a strong ministry secretariat; a more active involvement of the security and intelligence committee system, particularly in the

---

(3) Freedom and Security under the Law, page 754.

setting of intelligence priorities; strong leadership within the agency to be provided by a senior management cadre drawn from both outside and within the Security Service; and, the recruiting of personnel with a breadth of educational, professional and social backgrounds into all levels of the new agency.

### Separation and Transition

In August 1981, the McDonald Commission Report was published and the Government announced that the Security Service would be separated from the RCMP. The Security Intelligence Transition Group was formed to prepare the way. In its work the Group was guided by five basic principles that had been enunciated in the Government response to the Commission Report:

- a) Canada must have an effective security intelligence agency, capable of providing information essential to the maintenance of national security;
- b) there must be a legal framework within which the agency could conduct its activities in accordance with the rule of law, while recognizing the right of legitimate dissent;
- c) the agency must have effective internal direction and accountability;
- d) it must be effectively accountable to ministers responsible to Parliament; and,
- e) there must be an external review mechanism.

The Transition Group's recommendations, two attempts at proposed legislation (Bills C-157 and C-9), and the resultant CSIS Act all followed the overall thrust of the Commission's Report. There were, however, two significant differences. One concerned the personnel policies that McDonald saw as essential and the second affected the counter-subversion area.

Although the McDonald Commission had spent much time developing the argument for a broad mix of talents and skills to balance the dominance of police backgrounds in the Security service, the development of administrative and personnel policies to meet the Commission's expectations was left until after separation. Upon separation, therefore, the new agency had very little in the way of a blueprint for the implementation of such

policies. Personnel management within CSIS was made more difficult by the provisions of the Act concerning the rights of former members of the Security Service either to a position within CSIS or to return ("bridgeback") to the RCMP within the first two years. The turmoil of setting up a completely new organization and the ongoing (and some would argue increasing) demands of the operational environment ensured that the requirement for a better blend of skills and talents would become subordinated to other, more urgent priorities. An opportunity was missed to change the mix of skills and abilities within CSIS.

In the counter-subversion area, the Commission had proposed a relatively narrow definition of subversive activities: "activities directed towards or intended ultimately to lead to the destruction or overthrow of the democratic system of Government in Canada."(4) Section 2(d) of the Act broadened that definition to:

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

Section 2 of the Act also added an explicit exclusion of lawful advocacy, protest or dissent as threats to the national security, unless they were carried out in conjunction with activities that had been defined as threats earlier in Section 2.

Another significant difference between the Commission's approach to counter-subversion and that of the CSIS Act involved the use of investigative techniques. The Commission had recommended that only non-intrusive techniques be used to collect intelligence on subversive activity.(5) After some considerable debate, Parliament did not accept this proposal. The Act allows the use of intrusive methods against subversive activities, but with a 60-day time limit on all such warrants (as opposed to one year in all other cases).

The proclamation of the CSIS Act also brought with it a number of changes that significantly altered the role of the Service. These changes were at odds with the then corporate culture of the RCMP Security Service, and required the

---

(4) Freedom and Security under the Law, page 1067, recommendation 2d.

(5) Ibid., page 1067, recommendation 3

development of a new and different corporate culture. Among the most significant changes were:

- a) CSIS employees were no longer part of a "peace officer" force and therefore had no enforcement role; when enforcement was required, it was to be carried out by separate police agencies;
- b) although investigation was still a requirement, there was to be increased attention paid to research and analysis, with an unfamiliar emphasis on open source information; and,
- c) although secrecy was still very much an operational requirement, the new structure and procedures required by the CSIS Act to ensure direction and control by the Government subjected the new agency to much more public view and political scrutiny.

PEOPLE - VISION AND CHANGE

We reviewed the human resource situation inside CSIS today and found an organization still very much in a state of transition. In retrospect, the expectations of all of us as to the time it would take to achieve the fundamental changes in skills and abilities recommended by McDonald and sought by the Government were overly optimistic, given the realities of separation and transition. Section 66(1) of the CSIS Act limited the possibilities for the better blend of skills and talents that McDonald wanted, at least in the near term, by stating that:

all officers and members of the Force and all persons appointed or employed under the Public Service Employment Act assigned to the Security Service....become employees of the Service (CSIS).

This legislated staff carryover, the eventual exercise of their "bridgeback" rights by some ex-members of the RCMP, and the CSIS human resource management policies since separation have set the stage for much of the criticism that the Service is now enduring.

Much of this criticism centres on the issue of "civilianization", a term surrounded with so much confusion and misunderstanding that it has lost whatever meaning it may once have had. We feel obliged to redefine the issue into the broader question of people and organizational change. CSIS must project the image of an organization that is in tune with the times -- "sophisticated", as one consumer of security intelligence has put it. To accomplish this, the Service must modify its culture, and with it, its mix of people.

SIRC, in its Annual Report, raises two separate issues that are part of the same general theme. The first of these is the absence of sufficient progress towards the goal of a broader mix of skills, education and backgrounds ("civilianization" in SIRC's terms). The second is the more traditional one of representation that has its basis in law and Government policy. Although SIRC chose only to deal with francophone representation, we would broaden the issue to include women and minorities.

We believe that the CSIS population must not only possess diverse educational, social and experience backgrounds, but also should have a representation of women, francophones and minorities similar to the rest of the public service.



For an organization to initiate successful change, it must have: effective leadership; effective human resource management; integrated recruitment, training and career development; and, a remolding of the corporate culture to encourage different values and to enhance self-esteem.

### Leadership and Organizational Structure

The importance of leadership in organizational change is so obvious there is a temptation not to state it. But the unique situation of CSIS within Government makes the consideration of this element mandatory. In the section on The Security Intelligence Framework, we will examine the external structures affecting leadership. Within CSIS, we have observed a formal, hierarchical decision-making process that has tended to isolate the Director and that is unsuited either to the redefined security intelligence activities or to the management of people in today's world.

We have observed, for example, that the Service's corporate planning capability is limited to operational concerns, and does not play a role in the overall integration of CSIS policy and programs. We have also observed that the compartmentalized CSIS management committee structure inhibits the accommodation of new or different points of view, does little to encourage effective communication within the Service, and does not provide a corporate level perspective to program priorities and resources. The Director must chair important internal management committees for his leadership to be manifest.

We shall comment in the following section on how the organizational structure inhibits coherent direction and effective communication between the various elements that must produce intelligence reports. This communication problem is present throughout the Service and can be traced to an inbred proclivity for secrecy as well as to the organizational structure itself. It is a problem that must be corrected if good leadership is to be possible. There are also problems with the Service's communications with the rest of Government.

We would argue that the creation of a secretariat, reporting directly to the Director, would redress many of these problems. In addition to acting as an executive secretariat for the key CSIS management committees, this unit would be charged with corporate policy and planning and with the coordination of the Service's outward communications with major stakeholders in

the security and intelligence community, with external review bodies, with the Government at large, and generally with the public.

Bearing in mind the specific organizational recommendations made in this report, the Director should review the structure of his organization and the committees that support it, with a view to reshaping them to allow himself more direct control of the operations of the Service.

### Human Resource Management

We gathered information on two aspects of human resource management: the blend of skills and talents required in a security intelligence agency and the representational issues (women, francophones and minorities). Despite the expectations of the McDonald Commission and the Government, CSIS has not made significant progress in improving its skills mix, except at the desk officer level; very little change has been made at the supervisory or management levels. The representational picture is also disappointing. Although the CSIS population is 27% francophone, the ratio in the operational and senior management categories is noticeably lower, and the representation of women is even worse. The problems that CSIS has had in the recent past in implementing its bilingualism policies have been well documented and need not be repeated here. A plan is under preparation by CSIS to address this issue. Suffice it to say, as SIRC has pointed out, CSIS has much work to do.(6)

Finally, in gathering statistical information for this part of the report, we observed that the CSIS management information systems were unable to provide all the detail that we would have liked. When the Security Service separated from the RCMP, it did not bring a management information system with it, and so CSIS had to build or acquire one. Like a number of other requirements, this one took a back seat to higher priorities, although CSIS is now in the process of enhancing its system.

We have commented earlier on certain extenuating circumstances that have affected progress in broadening the

---

(6) For a detailed review of this issue, the reader is referred to the SIRC Annual Report, 1986-87 (part 8) and to the SIRC report Closing the Gaps: Official Languages and Staff Relations in the Canadian Security Intelligence Service.

base of skills and talents. We believe, however, that the time is right to initiate change.

### Recruitment, Training and Career Development

We are convinced that a renewed effort must be made to further diversify the CSIS personnel profile. It is as true today as it was when the McDonald Report was published that the balance between investigative skills (which are necessary) and other skills and talents must be improved. A new and vigorous hiring strategy is needed to address this imbalance. CSIS has no problem in attracting individuals with investigative skills, and interest from individuals with other skills, education and experience has been high in the past, particularly at separation. Recruitment must go beyond the issue of skills mix and address representational imbalances as well. Finally, the strategy must aim at improving the balance at all levels of the Service, but in this regard it must be balanced with a complementary program of advancement from within.

The Sir William Stephenson Academy was a good approach to recruit training. However, other training initiatives were less successful. Although the Academy's location left something to be desired, its course content, the experience and dedication of its staff, and its residential approach to training produced graduates who were knowledgeable and dedicated. The orientation of non-operational staff, the training of "direct entries" (recruits with specific backgrounds who bypassed the Academy process), and continuation training at all levels have been less successful. This can be attributed, in part at least, to the turmoil of separation and a lack of resources. The time is now ripe, however, for a concentrated effort to deliver a full range of induction, in-service and professional development training.

Career development within CSIS has been curiously lacking, although in the beginning there appears to have been a plan, at least for Academy graduates. CSIS employees cannot easily be moved about without their consent and positions are filled on the basis of individual competition, factors which limit flexibility in career development. Employees wishing to broaden their experience should have the opportunity to do so, and lateral moves within the Service should be encouraged for such employees. Indeed, certain employees should be given the opportunity to gain experience elsewhere in the Canadian security and intelligence community and in the public service at large. Finally, although we have said it before, it bears repeating

here: any program to improve the mix of skills and talent from the outside must not be seen as unduly restricting advancement. A good career development program is essential.

### The Corporate Culture

The organizational antecedent of CSIS, the manner in which the Service was established, and the unaccustomed glare of publicity have resulted in an organization that is uncomfortable in the limelight and not used to close political scrutiny. After three years of transition, CSIS still looks very much like the Security Service. Compartmentalization and secrecy stifle communication; priorities are driven by operational rather than strategic considerations; case-oriented, investigative techniques are given undue emphasis (although these techniques are a necessary component of the intelligence process); and, there is an inbred distrust of the "system". There has been much resistance to change.

The Service is still clearly in transition, as we have noted. The events of the past few months, although they have undoubtedly been traumatic for all concerned, have served to focus attention on the Service's problems. At the same time, they have generated a desire for solutions that will put the transition process back on the right track. Change has become something to be sought after, something to be encouraged. The role of CSIS is necessary to Canada, but it must be properly executed -- and seen to be so executed. Changes in the Service are needed, some detailed and easy to quantify and others more ethereal and vaguely defined. The most important agent of change must be CSIS itself. The Service must take responsibility for dealing openly with its people in this climate of change. Only in this way can an appropriate set of values be developed and the self-esteem of the Service and its people be established.

CSIS cannot do it alone. It must be supported by the security intelligence community and the Government. This theme will be explored further in the section on The Security Intelligence Framework.

## Recommendations

1. Changes should be made to the organization and to the management committee structures of CSIS which will strengthen the leadership of the Director in the corporate policy, planning, and human resource management of the Service, as follows:
  - the Director's office include a Secretariat responsible for corporate policy, planning, coordination, and communications;
  - the Director personally chair the key internal management committees of CSIS and ensure broad representation from all parts of the Service;
  - the Director establish and chair a Human Resource Management Committee to provide a better focus on human resource management issues; and,
  - the Director appoint a Deputy Director (Personnel) who would be responsible for all Personnel Services, Training and Development, and Official Languages.
  
2. A human resource management plan must be developed and implemented to improve the skills mix at all levels of the Service, to redress representational imbalances, to refine and implement the Service's bilingualism program, and to respond to the recommendations on training and career development made in this report. It must be supported by a strong internal communications package, and should include specific goals by which to measure progress.
  
3. Comprehensive personnel management information systems, now under development in CSIS, must be completed as soon as possible in order to provide human resource planners and management with the comprehensive human resource information necessary for decision-making.
  
4. CSIS, in consultation with the Ministry Secretariat, should prepare for submission to the Governor-in-Council a series of regulations governing human resource management, in accordance with section 8(4) of the CSIS Act.

5. Annual attrition should be used as a basis for an intensive program of interdisciplinary recruitment at all levels of the Service, aimed at balancing the skills mix and representation of women, francophones and minorities in the Service.
6. The Sir William Stephenson Academy must be re-established by September 1, 1988 as a permanent training facility at a site which provides an appropriate bilingual learning milieu offering a full range of residential and non-residential training and professional development courses for employees at all levels of the Service.
7. A new entry program must be designed considering the following provisions and should be in place by April 1, 1988:
  - the curricula previously offered at the Academy for new recruits and the Intensive Basic Course should be realigned and modularized as a single entry program so that all recruits at every level attend the same program;
  - the new entry program should be designed and managed by training specialists who ensure that the curriculum is responsive to operational needs and reflects the results of the validation exercise currently being conducted on the first three academy courses and on the Intensive Basic Course;
  - the new entry program must include basic sessions and sessions which are tailored to the needs of individuals with two backgrounds: those with and those without investigative experience. The basic sessions should focus on a comprehensive understanding of the CSIS Act, security and intelligence methods and practices, and the organization, role and operations of CSIS. The tailored sessions should deal with analytical, investigative and trade skills; and,
  - basic sessions should be scheduled in conjunction with recruitment activities so that all new recruits attend immediately upon appointment; the tailored sessions should be offered after completion of six months of on-the-job training.
8. All employees should participate in a new, revised CSIS orientation program, commencing immediately.

9. All newly appointed senior management staff should be obliged to participate in the Public Service Commission's Management Orientation Program. Those already in a position to do so should attend, on a priority basis, within twenty-four months.
10. The career paths of CSIS staff should provide for movement within both the security intelligence community and the public service generally when their qualifications are appropriate to the positions/opportunities available, and in particular:
  - senior management personnel should be rotated out to other public service duties every five to six years of their service in CSIS. This should be undertaken as a personal responsibility by both the Director, CSIS and the Chairman of the Public Service Commission.

THE INTELLIGENCE PRODUCT(7)

"Intelligence product is the raison d'être of a security intelligence agency." This statement, made by one of our interlocutors, highlights the way in which CSIS is judged by the rest of the Canadian intelligence community, and by the Government at large. The statement also is consistent with the views of the McDonald Commission and with section 12 of the CSIS Act, which provides the mandate for the collection, analysis and distribution of security intelligence:

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. (emphasis added.)

Intelligence and information collected by CSIS is used to develop two general categories of intelligence product: operational intelligence and broadly based or strategic intelligence. The former relies heavily (but not exclusively) upon investigative techniques, is usually short term, and is produced for specific consumers or for a specific purpose. CSIS itself is a major consumer of this type of intelligence. Operational intelligence and the investigations that support it also are building blocks for the more strategic threat analysis. The latter relies more heavily on research using information from all sources, tends to be longer term and more global in scope, and is produced for an interdepartmental audience or for the Government as an entity.

In its latest Annual Report, SIRC argues that the Service's intelligence product does not meet the expectations of the McDonald Commission or the needs of the Government. SIRC attributes this to two factors: that CSIS relies too heavily on investigative, case-oriented, covert intelligence and does not make enough use of open source information; and, that the research function within CSIS is poorly organized and resourced, and is not used to its full potential.

---

(7) A Glossary of Terms as we have used them may be found at the end of this report.



We surveyed a number of intelligence consumers. The consensus of this group was that CSIS operational intelligence is of a high quality, but that there is not enough of it. Some of our interlocutors stated that CSIS did not seem aware of what sorts of operational intelligence might be of interest to its consumers. This was attributed to a lack of understanding of the needs of the rest of Government on the part of CSIS and many of its analysts. On the other hand, intelligence consumers must tell CSIS what they want. It was also noted that, despite some improvements that have been made since separation, strategic intelligence is still inadequate. A complaint often heard was that CSIS tended to produce threat assessments in a vacuum, assessments that could have benefited from assistance available elsewhere in the intelligence community. The terms of reference for the interdepartmental security and intelligence committee structure were recently revised, giving the Intelligence Advisory Committee(8) a larger role in the production of security intelligence. The more active participation of CSIS in the production process that these changes will allow should improve the quality of CSIS strategic analysis.

We have observed serious problems in CSIS organization that affect intelligence production. The three segments of the CSIS research and analysis function (operational analysis, strategic analysis and the "research" function) are carried out in three separate directorates. Coordination is difficult and the three entities are often at cross purposes. This has affected the Service's ability to produce intelligence that is responsive to Government needs.

Furthermore, CSIS has a serious internal communications problem, one that is attributable to the Service's predilection for secrecy and compartmentalization. Operational analysts view their tasks (which contribute to a specific objective such as a persona non grata action) as the main role of the Service and neither understand nor sympathize with the role of the strategic intelligence analysts. Until very recently, there has been no apparent action on the part of senior management to improve the situation.

---

(8) The Intelligence Advisory Committee is an interdepartmental committee chaired by the Intelligence and Security Coordinator in the Privy Council Office. It is a mixed group of consumers and producers that establishes interdepartmental assessment priorities and maintains a continually updated work program.

We see no reason to disagree with the SIRC commentary on the quality of security intelligence. We would add, however, that there is room for optimism. Many of the analysts with whom we spoke were impressive, both in their attitude and in the mix of backgrounds and skills that they bring to the task. Their dedication is unquestioned.

We agree with the SIRC criticism of the CSIS research function, but we do not agree that the research section should be producing reports on its own. The present "research" function in CSIS would be more properly described as a reference function. A properly staffed and equipped reference section should be an indispensable component of the research and analysis function. The Open Information Centres, and the reference function generally, are improperly staffed and under-resourced, particularly insofar as their French language capability is concerned. These centres are considered a "service" and, since they are not linked directly to the analysis organization, they suffer from a lack of guidance and direction.

The absence of clearly defined intelligence priorities, the lack of a coordinated system for production, and inadequate reference facilities go a long way towards explaining the Service's apparent hesitancy to exploit open source material to its full potential. It cannot be attributed simply to the "case-oriented approach of police work".(9) Intelligence analysts will use whatever information is available to prepare their reports, whether drawn from open sources or not, so long as it can be verified. Open information is often preferred and used (although it may not always be so identified), since it allows the resultant report to be less highly classified and therefore more widely circulated.

### Recommendations

11. The three components of the research and analysis function (operational analysis, strategic analysis, and reference information) must be placed under one functional direction.
12. Reference centres should be staffed only with properly qualified research assistants and equipped with extensive reference material in both official languages.

13. CSIS should continue to improve the quality of its threat assessments and make every effort to enhance its use of open information. On balance we remain convinced that important threat assessments, certainly at the strategic or environmental level, could be completed primarily on the basis of open information.
14. CSIS must develop a strategic plan for intelligence production. The plan would be based on Government intelligence priorities and reflect an integrated approach to the collection, analysis, and dissemination tasks.

COUNTER-SUBVERSION - THE SECURITY INTELLIGENCE NET

In its Annual Report, SIRC raises a concern that "the counter-subversion program casts its net too widely." (10) In its view, too many Canadians are under surveillance as a result of the CSIS targetting process. SIRC observes that individuals often are targetted simply because they are members of a target group or because they come into regular contact with someone who has already been targetted. According to SIRC, "the present process takes insufficient account of potential harm to the principles of personal freedom and privacy." (11) SIRC recommends that the Counter-subversion Branch be eliminated and its role split between the other two operational branches, Counter-terrorism and Counter-intelligence. SIRC also recommends that CSIS targetting policy and practices be changed to provide a more equitable balance between the nature and urgency of the threat, on the one hand, and individual rights and the integrity of social institutions, on the other.

The counter-subversion function provides a useful and revealing window into the entire security intelligence operation, and it is impossible to view it in isolation. A serious study of this function soon leads one to the entire targetting process and thereby illuminates most of the weaknesses in the Service's corporate culture. Many of the problems that SIRC has raised in the counter-subversion area have their origins in the more general issues discussed elsewhere in this report.

The security intelligence framework required to support the targetting process, although nominally in place, has not functioned as was intended (see The Security Intelligence Framework). The priority-setting role of this framework has never really been exercised. The blend of skills and talents needed to support the targetting process, investigation and analysis is not adequate, as we have already noted (see People - Vision and Change). One of the McDonald Commission's most telling arguments for a better skills mix was the need to enhance the ability to differentiate correctly between subversion and dissent.

Finally, McDonald argued, and we agree, that analysis should have a dominant effect on all significant activities of a security intelligence agency, including the setting of reasonable collection priorities. In the treatment of subversion, this analysis must determine first and foremost the strategic threats

---

(10) Annual Report 1986-87, page 36

(11) Ibid., page 37

posed by subversive activity. Threat analysis must exhaust all the appropriate sources of information, beginning with open information. Indeed, in dealing with subversion, open source analysis should take precedence over the more intrusive investigative techniques.

The requirements for investigation and analysis will vary according to the activity under review. In espionage and terrorism, for example, the threats usually emanate from foreign governments and their intelligence services, or from well-trained, highly motivated terrorist organizations. If not dealt with, these groups could cause serious harm to the country or to individual Canadians. In order to properly gauge these threats, the Service must employ the full range of intrusive techniques, supplemented by whatever open source material is available.

To the extent that the subversion threat originates in the domestic environment, it seldom brings with it the same danger and urgency as the other types. Those domestic threats that do pose significant danger usually involve activities that can be more properly treated as terrorism or foreign interference, and can be dealt with as part of the CSIS counter-terrorism or counter-intelligence functions. If individual rights are to be given proper consideration, threat analysis for domestic subversion must use open sources in the majority of instances. Only infrequently will the seriousness of the threat demand more intrusive techniques. That option must be available as a last resort, but it must not be granted lightly.

SIRC has observed that CSIS operations in counter-subversion are too broadly based and that they rely too heavily on intrusive techniques. After reviewing the allocation of CSIS operational resources and studying some specific counter-subversion operations, we have reached the conclusion that the Service applies too many resources in this area.

Furthermore, we believe that the legal and policy framework used by CSIS in this area must be further developed. For example, the linkage between the "strictly necessary" provision of Section 12 of the Act and the targetting and collection processes of the Service has not been adequately made. The result, in our opinion, is that too many resources, many of them of an intrusive nature, have been committed to the investigation of what are "low-level" subversive activities.

In our judgement, most of the investigative duties and functions now carried out in the Counter-subversion Branch could be effectively reassigned as part of the counter-intelligence or counter-terrorism functions.(12) This would leave a residue of functions that would legitimately fall under Section 2(d) of the Act. These would still have to be monitored, keeping in mind the objective of the McDonald Commission that the "difficult line be drawn", but in the majority of cases this could be accomplished as part of the threat analysis function.

The CSIS operational targetting and collection policy is currently under review within the Service. In our view, that policy must provide for the protection of individual rights as envisioned by the McDonald Commission. This would require strict adherence to the following principles:

- a) the rule of law must be respected;
- b) investigative means must be proportional to the gravity and imminence of the threat;
- c) the requirement to use intrusive techniques must be weighed against possible damage to civil liberties;
- d) except in emergencies, less intrusive techniques must be used first; and,
- e) the more intrusive the technique, the higher the authority that is required for its use.

Once these conditions have been satisfied, and a decision to investigate is taken, the law intends and the Government expects CSIS to pursue its investigation to its logical conclusion. There are no sanctuaries or safe havens from which individuals can engage with impunity in activities threatening to the security of Canada. (13)

---

(12) See also SIRC Annual Report 1986-87, page 40.

(13) SIRC expressed a similar view on page 16 of its Annual Report, 1986-87, when it stated: "On the other hand, CSIS must be able to pursue its investigations wherever hostile intelligence officers or their agents, terrorists or subversives lead it."

We agree with the McDonald Commission view that the use of human sources is an essential component of a security intelligence collection program. The use of this very intrusive investigative tool must be centrally directed and controlled at the Director's level, both when human sources are initially employed or when they are reassigned. Although some direction does exist, the use of human sources should be the subject of comprehensive ministerial direction.

### Recommendations

15. The Counter-Subversion Branch should be eliminated and its duties and functions reassigned. Foreign influenced activities detrimental to the interests of Canada should become the responsibility of the counter-intelligence function while surveillance of acts of serious violence for the purpose of achieving political objectives should be assigned to the counter-terrorism function.
16. The residue of activities that fall under section 2(d) of the CSIS Act should normally be assessed through the use of open information; recourse to highly intrusive techniques should be available when dictated by the severity of the threat, but on a very limited basis and subject to the revised targetting and warrant review processes.
17. The Ministry Secretariat, in collaboration with CSIS, should develop, in the form of a Ministerial directive, the policy standards and "operational interpretations" necessary to establish an operational framework for section 2(a) to (d) of the CSIS Act.
18. A comprehensive legal/policy framework relating to section 12 of the CSIS Act should be completed by the Ministry Secretariat on an urgent basis, in consultation with CSIS and the Inspector General and referred to the Department of Justice for review. The framework should establish standards to permit CSIS to define the linkage between the "strictly necessary" criteria of the section and the targetting and intelligence-gathering processes.
19. The scope and intensity of the security intelligence net should be the subject of a ministerial directive to CSIS.
20. The Ministry Secretariat and CSIS should collaborate in the preparation of a comprehensive ministerial directive on the principles and policies governing the conduct of CSIS investigations.

21. CSIS should complete the redrafting of its targetting policy; the policy must be based on the principles, enunciated by the McDonald Commission, underlying the system of powers and controls for intelligence gathering.
22. We support the CSIS effort to reduce the number of investigative and authorization levels to implement investigations. We also support the Service's efforts to achieve a better balance in the range of intrusive investigative techniques provided for at each level.
23. The Director must chair both the Warrant Review Committee and the Target Approval and Review Committee, thereby setting the tone and direction for the Service.
24. The membership of the Warrant Review Committee should be expanded to include representation from the Privy Council Office or the Department of Justice at the Assistant Secretary/Assistant Deputy Minister level. The Ministry Secretariat should be represented by the Assistant Deputy Solicitor General, Police and Security Branch.
25. The warrant review process should include a fully independent warrant review function staffed by Counsel directly responsible to the Deputy Solicitor General. Counsel should have unrestricted access to CSIS/Ministry Secretariat information relevant to the proposed investigation in order to challenge the reliability of operational information supporting warrant applications.
26. CSIS human source operations should be governed by comprehensive, ministerially approved direction to the Service. The use of this very intrusive investigative technique must be centrally directed and controlled by the Director, CSIS.



THE SECURITY INTELLIGENCE FRAMEWORK

As noted earlier, the McDonald Commissioners had as a primary objective to bring the new security intelligence agency "under the direction and control of government." They postulated a three-level framework within which this control would be exercised and intelligence priorities set. The first level was to be an act of Parliament to provide the legal basis, to give specific powers to the Solicitor General and the Deputy Solicitor General, and to establish lines of external direction for the Service. The second level was to be the Government, through a strengthening of the security intelligence committee system that was already in place. The committee system (in McDonald's scenario) would provide the forum for the Government to exercise its ultimate responsibility for the security of the nation and would allow intelligence priorities to be set and transmitted to the new agency. The third level was to be the agency itself, which would implement Ministerial direction and convert broad Government intelligence priorities into specific subject areas about which it would gather intelligence and report.

The CSIS Act defines roles and responsibilities for the Solicitor General, the Deputy Solicitor General and the Director, CSIS. As a general comment, we believe that those roles and responsibilities have not yet been fully realized. We have found that interaction between CSIS and the Ministry Secretariat has been driven by operational rather than policy considerations. Broad ministerial direction has usually arisen from the need to deal with specific operational cases rather than as part of a strategic or policy thrust. We have observed also that the interdepartmental committee structure has not operated to its full potential.

We note that the security intelligence decision-making process is being changed to address the kinds of problems that SIRC and we have noted. The interdepartmental committee system has recently undergone a review that has resulted in the updating of the terms of reference of its key committees. The Ministry Secretariat is being reorganized, with a view to making it more effective in playing its role. A new Director has been appointed for CSIS, and a number of Deputy Director positions are vacant. These factors offer an opportunity to introduce other significant changes. The climate for change is right.

The CSIS Act provides to the Minister a legal basis for the setting of broad intelligence priorities. Therefore, CSIS can be directed by the Government, in a formal and systematic way, as to what its broad collection priorities ought to be prior

to setting its own operational priorities. The preparation of a formal statement of these priorities, begun some months ago, should be accelerated and completed. The Interdepartmental Committee on Security and Intelligence (supported by the Intelligence Advisory Committee) will reinforce the priority-setting process. The Minister and his departmental staff are responsible for managing the priority-setting process. In this way, the Service is not left to determine its own operational priorities without the overall political direction that McDonald sought to achieve.

The Advisory Team believes that the primacy of the Solicitor General in the decision-making process must be constantly emphasized. He is the linchpin in both the legal framework and the Government policy framework. It is essential that the Solicitor General continue to exert political control.

### Recommendations

27. A reconfirmation of the roles and responsibilities and an assessment of the expectations of the roles to be played by the major office holders in the national security framework are required. In particular, the primacy of the role of the political executive in the provision of direction in the national security framework must be re-emphasized, as follows:
  - CSIS, in close collaboration with the Ministry Secretariat and after interdepartmental consultation (Interdepartmental Committee on Security and Intelligence), should prepare an annual overview of the threat to the security of Canada for submission to the Solicitor General;
  - the annual threat overview should be reviewed by Cabinet, thereby formally establishing national security intelligence priorities;
  - the Solicitor General must issue broad security intelligence priorities to CSIS; and,
  - the Ministry Secretariat and CSIS should collaborate in the preparation of a comprehensive ministerial direction (section 6(2), CSIS Act) to ensure that the Solicitor General has full accountability for the policy, program and expenditure planning process; the corporate management review and decision-making process; and the review and approval of operational activities as required by statute and policy.

OTHER MATTERS

Our terms of reference and the available time restricted detailed review to the issues surrounding "civilianization" and the counter-subversion process. As we have noted previously, however, it is impossible to review these areas without becoming aware of other issues, some of them important, that affect CSIS and the structure surrounding it. Most of these will require further review or detailed examination by the Ministry Secretariat or the Director of CSIS, or by the two organizations in concert. We recommend that this review and examination be conducted using the staff that has been brought together to produce this report.

Many of the recommendations that follow are motivated by the desire to give to CSIS the organizational pride and high morale that it must have to carry out the necessary and difficult function that the McDonald Commission envisioned.

Throughout our review we were continually aware that CSIS has had serious resource problems. On the one hand, the Service was established without due regard for the real costs of many "housekeeping" matters. On the other hand, we have observed that CSIS applies too many operational resources against some types of target, and that the allocation of these resources needs further review.

We can state without further study that there must be more capital expenditure for accommodation and administrative needs. The Service still shares many operational and administrative facilities with the RCMP. A large percentage of CSIS employees still go to work in the morning at RCMP headquarters, making it rather difficult to generate and maintain the esprit de corps that is so important. We suggest that the decision to occupy the East Memorial Building was a mistake.

In summary, there is enough doubt surrounding the whole question of CSIS resources to make the issue a prime candidate for further review.

To provide the Service with the Government direction and guidance it needs, the Ministry Secretariat must take a more active role. In order for the Secretariat to meet this requirement, its staff will require augmentation.

We are concerned about the controversial and often very adversarial situation that arises from the publication of the SIRC Annual Report. Although we recognize the need for the external review function to be independent, we believe that the present process runs the risk of serious damage to the morale of the Service. Some means must be found to defuse some of the unnecessary controversy in advance of publication.

### Of Special Concern

During our review, we had brought to our attention a number of examples of either factual mistakes or errors in judgement on the part of CSIS with respect to the decision-making process leading to the granting or denial of citizenship or permanent resident status. SIRC has also expressed concern about this process. (14) Section 17 of the Act provides a basis for CSIS to enter into formal agreements with other government departments to perform its "duties and functions"; these duties include the carrying out of security assessments under Section 13. We believe that issues surrounding citizenship and immigration are of sufficient public concern to necessitate some recommendations in this report.

The preparation of security assessments in such cases is the responsibility of the security screening unit in CSIS. This unit is also responsible for the preparation of security assessments on Government employees. SIRC has commented on the considerable backlog of security assessment requests that CSIS is faced with, and, although we are aware that some steps have been taken to remedy the situation, we are nonetheless concerned that the situation has not sufficiently improved.

### Recommendations

28. A complete review of CSIS capital and operating resource requirements should be completed by March 31, 1988 in order to determine a baseline from which to set reasonable and adequate resource levels for the Service.
29. A Long Term Capital Plan must be prepared at once as part of this review, in order to address necessary capital requirements of the Service in such areas as physical accommodation, EDP support, and trade-craft technology.

---

(14) see Annual Report, 1986-87 page 58

30. An immediate solution to the CSIS accommodation problem must be found, bringing all headquarters functions together in a building that can be adapted to meet the needs of CSIS, both human and technological.
31. The requirements of the Ministry Secretariat to support the Solicitor General in the administration of the CSIS Act and in other security responsibilities should be determined on a priority basis and adequate resources provided.
32. In a process similar to that so effectively used by the Auditor General, SIRC should inform the Service in advance of the content of its Annual Report and offer the opportunity for CSIS to initiate appropriate corrective action or to clarify or explain its position; SIRC could then acknowledge and publish any corrective action or CSIS statement of clarification or explanation.
33. In relation to CSIS' responsibility to provide security assessments (for security clearance purposes), we recommend that:
  - arrangements for the supply of security assessments by CSIS to the departments of the Secretary of State and Employment and Immigration be formalized in accordance with section 17 of the CSIS Act;
  - the present policy on the processing of objections on security grounds be revised to allow review by the Solicitor General of these objections before they are transmitted to the Secretary of State or the Minister of Employment and Immigration. Objections on security grounds should be accorded the same rigor of review as warrant applications;
  - sufficient additional resources be applied to clear the security assessment backlog by March 31, 1988; and,
  - a detailed study be made within CSIS of the security assessment process with a view to streamlining its operation.
34. A major public awareness/information initiative should be undertaken by the Ministry Secretariat and by CSIS itself to improve Canadian understanding of the purposes, processes and means by which our national security concerns are met and to remove from the popular lexicon many of the myths that have characterized the debate in recent years.

SUMMARY OF RECOMMENDATIONS

PEOPLE - VISION AND CHANGE

Leadership and Organizational Structure

1. Changes should be made to the organization and to the management committee structures of CSIS which will strengthen the leadership of the Director in the corporate policy, planning, and human resource management of the Service, as follows:
  - the Director's office include a Secretariat responsible for corporate policy, planning, coordination, and communications;
  - the Director personally chair the key internal management committees of CSIS and ensure broad representation from all parts of the Service;
  - the Director establish and chair a Human Resource Management Committee to provide a better focus on human resource management issues; and,
  - the Director appoint a Deputy Director (Personnel) who would be responsible for all Personnel Services, Training and Development, and Official Languages.

Human Resource Management

2. A human resource management plan must be developed and implemented to improve the skills mix at all levels of the Service, to redress representational imbalances, to refine and implement the Service's bilingualism program, and to respond to the recommendations on training and career development made in this report. It must be supported by a strong internal communications package, and should include specific goals by which to measure progress.
3. Comprehensive personnel management information systems, now under development in CSIS, must be completed as soon as possible in order to provide human resource planners and management with the comprehensive human resource information necessary for decision-making.

4. CSIS, in consultation with the Ministry Secretariat, should prepare for submission to the Governor-in-Council a series of regulations governing human resource management, in accordance with section 8(4) of the CSIS Act.

#### Recruitment, Training and Career Development

5. Annual attrition should be used as a basis for an intensive program of interdisciplinary recruitment at all levels of the Service, aimed at balancing the skills mix and representation of women, francophones and minorities in the Service.
6. The Sir William Stephenson Academy must be re-established by September 1, 1988 as a permanent training facility at a site which provides an appropriate bilingual learning milieu offering a full range of residential and non-residential training and professional development courses for employees at all levels of the Service.
7. A new entry program must be designed considering the following provisions and should be in place by April 1, 1988:
  - the curricula previously offered at the Academy for new recruits and the Intensive Basic Course should be realigned and modularized as a single entry program so that all recruits at every level attend the same program;
  - the new entry program should be designed and managed by training specialists who ensure that the curriculum is responsive to operational needs and reflects the results of the validation exercise currently being conducted on the first three academy courses and on the Intensive Basic Course;
  - the new entry program must include basic sessions and sessions which are tailored to the needs of individuals with two backgrounds: those with and those without investigative experience. The basic sessions should focus on a comprehensive understanding of the CSIS Act, security and intelligence methods and practices, and the organization, role and operations of CSIS. The tailored sessions should deal with analytical, investigative and trade skills; and,

- basic sessions should be scheduled in conjunction with recruitment activities so that all new recruits attend immediately upon appointment; the tailored sessions should be offered after completion of six months of on-the-job training.
8. All employees should participate in a new, revised CSIS orientation program, commencing immediately.
  9. All newly appointed senior management staff should be obliged to participate in the Public Service Commission's Management Orientation Program. Those already in a position to do so should attend, on a priority basis, within twenty-four months.
  10. The career paths of CSIS staff should provide for movement within both the security intelligence community and the public service generally when their qualifications are appropriate to the positions/opportunities available, and in particular,
    - senior management personnel should be rotated out to other public service duties every five to six years of their service in CSIS. This should be undertaken as a personal responsibility by both the Director, CSIS and the Chairman of the Public Service Commission.

#### THE INTELLIGENCE PRODUCT

11. The three components of the research and analysis function (operational analysis, strategic analysis, and reference information) must be placed under one functional direction.
12. Reference centres should be staffed only with properly qualified research assistants and equipped with extensive reference material in both official languages.
13. CSIS should continue to improve the quality of its threat assessments and make every effort to enhance its use of open information. On balance we remain convinced that important threat assessments, certainly at the strategic or environmental level, could be completed primarily on the basis of open information.



14. CSIS must develop a strategic plan for intelligence production. The plan would be based on Government intelligence priorities and reflect an integrated approach to the collection, analysis, and dissemination tasks.

COUNTER-SUBVERSION - THE SECURITY INTELLIGENCE NET

15. The Counter-Subversion Branch should be eliminated and its duties and functions reassigned. Foreign influenced activities detrimental to the interests of Canada should become the responsibility of the counter-intelligence function while surveillance of acts of serious violence for the purpose of achieving political objectives should be assigned to the counter-terrorism function.
16. The residue of activities that fall under section 2(d) of the CSIS Act should normally be assessed through the use of open information; recourse to highly intrusive techniques should be available when dictated by the severity of the threat, but on a very limited basis and subject to the revised targetting and warrant review processes.
17. The Ministry Secretariat, in collaboration with CSIS, should develop, in the form of a Ministerial directive, the policy standards and "operational interpretations" necessary to establish an operational framework for section 2(a) to (d) of the CSIS Act.
18. A comprehensive legal/policy framework relating to section 12 of the CSIS Act should be completed by the Ministry Secretariat on an urgent basis, in consultation with CSIS and the Inspector General and referred to the Department of Justice for review. The framework should establish standards to permit CSIS to define the linkage between the "strictly necessary" criteria of the section and the targetting and intelligence-gathering processes.
19. The scope and intensity of the security intelligence net should be the subject of a ministerial directive to CSIS.
20. The Ministry Secretariat and CSIS should collaborate in the preparation of a comprehensive ministerial directive on the principles and policies governing the conduct of CSIS investigations.

21. CSIS should complete the redrafting of its targetting policy; the policy must be based on the principles, enunciated by the McDonald Commission, underlying the system of powers and controls for intelligence gathering.
22. We support the CSIS effort to reduce the number of investigative and authorization levels to implement investigations. We also support the Service's efforts to achieve a better balance in the range of intrusive investigative techniques provided for at each level.
23. The Director must chair both the Warrant Review Committee and the Target Approval and Review Committee, thereby setting the tone and direction for the Service.
24. The membership of the Warrant Review Committee should be expanded to include representation from the Privy Council Office or the Department of Justice at the Assistant Secretary/Assistant Deputy Minister level. The Ministry Secretariat should be represented by the Assistant Deputy Solicitor General, Police and Security Branch.
25. The warrant review process should include a fully independent warrant review function staffed by Counsel directly responsible to the Deputy Solicitor General. Counsel should have unrestricted access to CSIS/Ministry Secretariat information relevant to the proposed investigation in order to challenge the reliability of operational information supporting warrant applications.
26. CSIS human source operations should be governed by comprehensive, ministerially approved direction to the Service. The use of this very intrusive investigative technique must be centrally directed and controlled by the Director, CSIS.

#### THE SECURITY INTELLIGENCE FRAMEWORK

27. A reconfirmation of the roles and responsibilities and an assessment of the expectations of the roles to be played by the major office holders in the national security framework are required. In particular, the primacy of the role of the political executive in the provision of direction in the national security framework must be re-emphasized, as follows:

- CSIS, in close collaboration with the Ministry Secretariat and after interdepartmental consultation (Interdepartmental Committee on Security and Intelligence), should prepare an annual overview of the threat to the security of Canada for submission to the Solicitor General;
- the annual threat overview should be reviewed by Cabinet, thereby formally establishing national security intelligence priorities;
- the Solicitor General must issue broad security intelligence priorities to CSIS; and,
- the Ministry Secretariat and CSIS should collaborate in the preparation of a comprehensive ministerial direction (section 6(2), CSIS Act) to ensure that the Solicitor General has full accountability for the policy, program and expenditure planning process; the corporate management review and decision-making process; and the review and approval of operational activities as required by statute and policy.

#### OTHER MATTERS

28. A complete review of CSIS capital and operating resource requirements should be completed by March 31, 1988 in order to determine a baseline from which to set reasonable and adequate resource levels for the Service.
29. A Long Term Capital Plan must be prepared at once as part of this review, in order to address necessary capital requirements of the Service in such areas as physical accommodation, EDP support, and trade-craft technology.
30. An immediate solution to the CSIS accommodation problem must be found, bringing all headquarters functions together in a building that can be adapted to meet the needs of CSIS, both human and technological.
31. The requirements of the Ministry Secretariat to support the Solicitor General in the administration of the CSIS Act and in other security responsibilities should be determined on a priority basis and adequate resources provided.

32. In a process similar to that so effectively used by the Auditor General, SIRC should inform the Service in advance of the content of its Annual Report and offer the opportunity for CSIS to initiate appropriate corrective action or to clarify or explain its position; SIRC could then acknowledge and publish any corrective action or CSIS statement of clarification or explanation.
33. In relation to CSIS' responsibility to provide security assessments (for security clearance purposes), we recommend that:
- arrangements for the supply of security assessments by CSIS to the departments of the Secretary of State and Employment and Immigration be formalized in accordance with section 17 of the CSIS Act;
  - the present policy on the processing of objections on security grounds be revised to allow review by the Solicitor General of these objections before they are transmitted to the Secretary of State or the Minister of Employment and Immigration. Objections on security grounds should be accorded the same rigor of review as warrant applications;
  - sufficient additional resources be applied to clear the security assessment backlog by March 31, 1988; and,
  - a detailed study be made within CSIS of the security assessment process with a view to streamlining its operation.
34. A major public awareness/information initiative should be undertaken by the Ministry Secretariat and by CSIS itself to improve Canadian understanding of the purposes, processes and means by which our national security concerns are met and to remove from the popular lexicon many of the myths that have characterized the debate in recent years.

GLOSSARY OF TERMS

SECURITY INTELLIGENCE:

Information and intelligence relevant to the identification and assessment of threats to the security of Canada. Activities which constitute such threats are defined in S.2 of the CSIS Act. CSIS investigates and advises Government in relation to these threats.

INTELLIGENCE PRODUCT:

Information and intelligence from all sources, which is processed and evaluated. In terms of intelligence product one speaks of Intelligence Estimates, Intelligence Analysis, etc.

OPERATIONAL INTELLIGENCE:

Security intelligence related to the investigation of particular activities considered threatening to the security of Canada. Investigation in these circumstances is often said to be "case-oriented". Operational intelligence would include, for example, reports on the activities of a specific foreign intelligence organization or one of its members operating in Canada.

STRATEGIC INTELLIGENCE:

Security intelligence that is evaluated in the context of other Canadian national interests. This level of analysis, for example, would seek to assess the impact of clandestine or deceptive activities by foreign governments in influencing or interfering in a particular ethnic community in Canada.

SECURITY INTELLIGENCE FRAMEWORK:

The legal and policy arrangements which define the parameters of security intelligence activity within the control and direction of Government.

SECURITY ASSESSMENT:

As defined in section 2 of the CSIS Act, this term means "an appraisal of the loyalty to Canada, and, so far as it relates thereto, the reliability of an individual". CSIS provides security assessments variously (under sections 13, 14, and 15 of the CSIS Act) in relation to the processing of applications for permanent resident status and the granting of Canadian citizenship. Security assessments are also prepared in relation to the security clearance process for Government employees and contractors.

TERMS OF REFERENCE

Pursuant to the direction of the Solicitor General, an advisory team will conduct an independent review of:

- i) the concerns expressed by the Security Intelligence Review Committee (annual Report tabled in the House of Commons on June 29, 1987) specifically addressing CSIS "civilianization" initiatives and counter-subversion operational policies, as well as the
- ii) concerns raised by independent observers about possible adverse effects on the civil liberties of Canadians as a result of CSIS's counter-subversion activities.

In a report to be provided to the Solicitor General by October 30, 1987, the advisory team will present a plan of action to address:

- i) the framework of operation policies required to support CSIS counter-subversion activities, including targetting, and
- ii) the design of personnel management policies intended to support a security intelligence service comprised of personnel with a wide variety of backgrounds and skills.

In its provision of advice to the Solicitor General, the advisory team will assess the requirements for further studies as appropriate.

LIST OF PEOPLE INTERVIEWED

NOTE: Some individuals were interviewed more than once, others as part of a group.

MEMBERS OF PARLIAMENT

Hon. Perrin Beatty	Minister of National Defence (former Solicitor General)
Hon. Robert Kaplan	Former Solicitor General
Hon. James F. Kelleher	Solicitor General of Canada
Hon. Allan Lawrence	Former Solicitor General
Hon. Elmer MacKay	Minister of National Revenue (former Solicitor General)
John Nunziata	Liberal Party Solicitor General Critic
Svend Robinson	New Democratic Party Solicitor General Critic

MEMBERS OF THE SENATE

Hon. William M. Kelly	Chairman, Senate Special Committee on Terrorism and the Public Safety
Hon. P. Michael Pitfield	Chairman, Senate Special Committee on the Canadian Security Intelligence Service

SECURITY INTELLIGENCE REVIEW COMMITTEE

Hon. Ronald G. Atkey	Chairman
Hon. Jean Jacques Blais	Member
Hon. Saul M. Cherniack	Member



SIRC (continued)

Hon. Paule Gauthier	Member
Hon. Frank McGee	Member
Maurice Archdeacon	Executive Secretary
Annie Demirjian	Executive Assistant
Arthur Graham	Director of Research

PRIVY COUNCIL OFFICE

Stan F. Carlson	Executive Secretary, Intelligence Advisory Committee
Dr. N. d'Ombraïn	Assistant Secretary to Cabinet (Machinery of Government)
James E. Harlick	Security and Intelligence Secretariat
Horst Intscher	Assistant Secretary to Cabinet (Security and Intelligence)
John L. Manion	Associate Secretary to Cabinet (former Secretary to the Treasury Board)
J. Blair Seaborn	Intelligence and Security Co-ordinator
Paul M. Tellier	Clerk of the Privy Council and Secretary to Cabinet

TREASURY BOARD SECRETARIAT

Michael E. Francino	Assistant Secretary, Program Branch
Diane MacLaren	Analyst, Program Branch
Michael Williams	Group Chief, Program Branch

MINISTRY OF THE SOLICITOR GENERAL

P.R. Ansell	Ministry Secretariat
David Davidson	Director General, Communications
Fred E. Gibson	Former Deputy Solicitor General
J.B. Giroux	Office of the Inspector General, CSIS (former Director General, RCMP Security Service)
Ian Glen	Assistant Deputy Solicitor General, Police and Security
V.E. Gooch	Director of Security Policy
Dr. Richard Gosse	Inspector General, CSIS
Alasdair MacLaren	Director General, Security Planning and Coordination
John L. Tait	Deputy Solicitor General of Canada

ROYAL CANADIAN MOUNTED POLICE

Norman D. Inkster	Commissioner (from September 1, 1987)
Roy Moffatt	Deputy Commissioner, Administration
Robert H. Simmonds	Commissioner (before August 31, 1987)

CANADIAN SECURITY INTELLIGENCE SERVICE

Eric Boulet	President, CSIS Employees Association
T. Darcy Finn	Former Director
Reid M. Morden	Director

Three Deputy Directors

Two Acting Deputy Directors

Six Regional Directors-General

CSIS (continued)

Seven Directors-General

Eleven other employees

OTHER INTERVIEWS

Archie Barr	Former Deputy Director, CSIS
André Bissonnette	Former Deputy Solicitor General
Alan Borovoy	General Counsel, Canadian Civil Liberties Association
Robin Bourne	Formerly of the Ministry of the Solicitor General
D. Bracie	Director of Research, Senate Committee on Terrorism and the Public Safety
Jean-Paul Brodeur	Université de Montréal
David Charters	Centre for Conflict Studies, University of New Brunswick
A. Stuart Farson	Centre of Criminology, University of Toronto
Richard French	Minister of Communications, Government of Quebec (former Privy Council Office official)
Pierre Gagnon	Author of <u>Closing the Gaps, Official Languages and Staff Relations in the Canadian Security Intelligence Service</u>
Me. Guy Gilbert	Member, Commission of Inquiry Concerning Certain Activities of the RCMP
Me. Jean Keable	Chairman, Commission d'enquête sur des opérations policières en territoire québécois

Jacqueline Krieber	Université Laval
Gaétan Lussier	Chairman, Canadian Employment and Immigration Commission
Justice D.C. McDonald	Chairman, Commission of Inquiry Concerning Certain Activities of the RCMP
D.S. Rickerd	Member, Commission of Inquiry Concerning Certain Activities of the RCMP
Hon. Gordon Robertson	Former Secretary to Cabinet
Professor Reginald Roy	University of Victoria
Professor Peter Russell	University of Toronto (former Director of Research for the McDonald Commission)
J.M. Shoemaker	Former Senior Assistant Deputy Solicitor General, Police and Security
Jacques Shore	Former Director of Research, SIRC
John Starnes	Former Director General, RCMP Security Service
Alan Sullivan	Assistant Deputy Minister, Political and International Security Affairs, Department of External Affairs
James H. Taylor	Under Secretary of State for External Affairs
John Venner	Former Deputy Director, CSIS