SECURITY INTELLIGENCE
REVIEW COMMITTEE

Annual Report

1986-1987

Minister of Supply and Services Canada 1987
Cat. No. JS 71-1/1987
ISBN 0-662-55252-0

Security Intelligence Review Committee
14th Floor
365 Laurier Avenue West
P.O. Box 2430, Station D
Ottawa, Ontario
KIP 5W5

(613) 990-8441: Collect calls are accepted, and the switchboard is open from 7:30 a.m. to 6 p.m., Ottawa time.

June 22, 1987

The Honourable James F. Kelleher, P.C., M.P., Q.C.
Solicitor General of Canada
House of Commons
Ottawa, Ontario
KIA OA6

Dear Mr. Kelleher:

Pursuant to section 53 of the *Canadian Security Intelligence Act*, we hereby transmit to you the Annual Report of the Security Intelligence Review Committee for the fiscal year 1986-87, for submission to Parliament.

Yours sincerely,

Ronald G. Atkey, P.C., Q.C.
Chairman

Jean Jacques Blais, P.C., Q.C.

Frank McGee, P.C.

Saul M. Cherniack, P.C., Q.C.

Paule Gauthier, P.C.

Quis custodiet ipsos custodes?

(Who is to guard the guards themselves?)

Juvenal

Contents

1. Introduction 1

Mandate 1
Relations with CSIS 2
How we operate 2
On the Record 3
Balance 3

2. Oversight 5

Formal Controls 5
Ministerial Instructions 6
CSIS Annual Report and Certificate of the Inspector General 6
The Oversight Process 7

3. How CSIS Knows 9

Behind Federal Court Warrants 9
Counting Them Up 10
Other People's Mail 11
Emergency Warrants 12
Open Sources 12
Canadian Police Information Centre 14
Academe and Officialdom 15
Inter-Organizational Arrangements in Canada 16
Foreign Arrangements 17
Unlawful Acts 18

4. What CSIS Knows 21

Legal Limits 21
Inherited Information 21
Retirement of Old Files 22
Foreign Intelligence 23
Incidental Information 24

5. What CSIS Does 25

Spin-Off Information 25
CSIS in Court 25
Assistance to Police 28
Increased Priority 26
Relations with the RCMP 27
Airport Security Alert 28
Foreign Liaison Officers 29
Persona Non Grata 29
The Public Interest 30
Front Organizations 30

6. Counter-Subversion Operations 33

Principles and Law 33
How we Proceeded 34
Transition 34
Resources 35
Human Sources 35
Targeting 35
Files on Individuals 38
Dissemination of Information 39
Five Organizations 39
Two Paths 40

7. CSIS Itself 41

Resources and Administration 41
Civilianization 42
Who is Recruited 43
Time Out at the Academy 44
Bilingualism and Equitable Participation 44
The First Class 45
Building Morale 46
Polygraph Examinations 46

8. Closing the Gaps 49

Official Languages 49
Staff Relations 52

9. Complaints 55

Kudos for Defence 55
Security Clearances 55
Complaints Against CSIS 56
Immigration and Citizenship 57
Quality of Investigations 57
Immigration Act Study 59
The New Security Policy 59

10. Tidying Up 63

Answering to Parliament 63
Outreach 63
Meetings and Conferences 63
Personnel 64
Financial Report 64

11. Looking Ahead 67

Five-Year Review 67

The Extent of Oversight 67
A Last Word 69

Appendices
A: Ministerial Directives and Directions, 1986-87 71
B: Case Histories 73
C: SIRC Personnel 77

1. Introduction

Independent, external review of security intelligence is a recent development in all the democracies. Here in Canada, it goes back only three years, to 1984, when Parliament adopted the *Canadian Security Intelligence Service Act (CSIS Act)*.

Under this *Act*, the responsibilities of the RCMP Security Service were transferred to a new Canadian Security Intelligence Service (CSIS). Our Committee, the Security Intelligence Review Committee (SIRC), was appointed to provide external oversight. An Inspector General was appointed to provide internal oversight and to report to the Solicitor General.

As pioneers entering a new area of public administration, we first faced the challenge of finding our bearings. This was very much reflected in our first two annual reports.

However, we are now beginning to zero in as we pass the mid-point of our five-year mandate. We are now equipped to analyse statistics on CSIS operations, to detect trends. We have also carried out major studies--on counter-subversion, for example--in addition to pursuing dozens of issues through written inquiries and interviews with CSIS officials.

On Course. We hope that readers of this annual report will share the sense that external review is now firmly on course. We touch on more topics and do so in greater depth than in our two previous reports.

Some themes will be familiar from our past reports. Our firm belief that CSIS is not making enough use of open sources as an alternative to covert investigations is just one example. We have also continued to report the total number of new warrants and renewals granted to CSIS by the Federal Court of Canada.

Among the subjects we have examined in greater depth are the counter-subversion program, particularly the way targets are chosen, relations between CSIS and the RCMP in counter-terrorism operations, and civilianization.

We feel mounting concern that civilianization is proceeding too slowly because of heavy recruitment of ex-police-officers. This can only perpetuate the law-enforcement approach that Parliament intended to change when it adopted the *CSIS Act*.

Mandate

In general terms, our mandate is to see that the Service carries out its work effectively but without unreasonable or unnecessary intrusions on individual rights. Specific tasks spelled out for us in the *CSIS Act* fall into two broad areas--oversight and complaints.

Oversight. Paragraph 38(a) of the *CSIS Act* directs us "to review generally the performance by the Service of its duties and functions" while paragraph 38(b) and section 40 permit us "to arrange for reviews to be conducted, or to conduct reviews" with a view to "ensuring that the activities of the Service are carried out in accordance with this *Act*, the regulations and directions issued by the Minister ... and that the activities do not involve any unreasonable or unnecessary exercise by the Service of any of its powers".

Chapters 2-8 of this report describe what we did last year to fulfil our oversight mandate.

Oversight does not mean that we are a kind of board of directors for CSIS. We do not hesitate to give advice, privately when circumstances dictate and publicly, when we can, through our annual reports and in testimony before Parliament committees.

But we do not set policy or issue orders. Nor would we want to, for that would make us active players in security intelligence and remove the freedom to criticize that is our *raison d'être*.

Complaints. Paragraph 38(c) directs us 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 certain complaints lodged with the Canadian Human Rights Commission.

Chapter 9 of this report covers our work in this area, and summary case histories are set out in Appendix B.

Relations with CSIS

The price of our independence is an arm's-length relationship with CSIS and other participants in the Canadian security intelligence establishment.

Independent, external oversight is the price that CSIS pays for its wide powers.

The Service provides us with the information we ask for, but it remains distant and wary. This is not necessarily a bad thing; too close a relationship could make it difficult for us to maintain our independence.

How We Operate

The *CSIS Act* provides that members of our Committee shall be appointed by the Governor in Council following consultations by the Prime Minister with the Leader of the Opposition and the leader of each party with 12 or more members in the House of Commons.

In making the initial appointments, the Prime Minister gave these consultations a very wide scope and invited the Leader of Opposition and the Leader of the New Democratic Party to nominate one member each while he himself nominated three members. The approval of all three leaders was sought for the complete slate. As a result, our Committee is clearly tri-partisan.

Once the appointment process was completed, however, we found it desirable to leave partisan considerations at the door. For the most part, we operate collegially, by consensus, in our oversight role. Also, the fact that we are part-timers, active in our communities and in private life, outside of government circles in Ottawa, makes it easier to focus on our task in a non-partisan way when we meet.

Complaints are usually heard by a single Committee member. While we all see the final reports, we provide legal and editorial comments only. We do not seek to discuss or amend the rationale or conclusions, following the rule that only the person who has heard the evidence at first hand can give each element in the case its proper weight. Under our conflict of interest rules, no Committee member participates at all in a case in which he or she has any advance knowledge of or association with the individual concerned.

On the Record

We have made Juvenal's much-quoted line "Who is to guard the guards themselves" the epigraph of this report. We were thinking of our relationship with CSIS. But it could be applied to us too. Parliament and Canadians must rely in large part on our Committee and the Inspector General to ensure that individual rights and freedoms are protected in the security intelligence field.

That is why, in preparing our annual report, we try to put as much as possible on the public record. The more we tell, the better Parliament and Canadians will be able to judge for themselves.

We are, of course, constrained by the statutory requirement to avoid revealing anything that would compromise national security. Under the *Act*, CSIS reviews the draft report and advises us about any information that it believes might do so. Some detailed supporting information is left out of the published report as a result of this process, but we do not feel that anything of great significance has been lost.

Balance

Annual reports by oversight or auditing bodies usually provide a litany of criticisms rather than a balanced picture. This is to be expected.

In addition, our annual report is constrained by our inability to comment on CSIS's successes, for national security reasons. There have been a number of successes, particularly in the fields of counter-espionage and counter-terrorism.

This report is not, therefore, a complete picture; it is a view through slightly parted curtains. If we were able to pull the drapes wide open, we would include much more information on the important and effective work accomplished day in, day out by the Service. It is an important national institution worthy of continued public support.

The dedication and professionalism of CSIS employees is impressed upon us anew at every contact we have with them from one end of the country to the other.

2. Oversight

Does CSIS protect the national interest as effectively as possible? Is it efficient--in terms of both management goals like financial integrity and policy goals like "civilianization" and official bilingualism? Does it give enough weight to individual rights and freedoms?

In its simplest terms, our oversight mandate is to keep a running score on these questions on behalf of Parliament and the Canadian people. Our particular role is to watch over the delicate balance between national security and individual freedoms.

Oversight is the topic of this chapter and the six that follow. We begin with formal controls on CSIS. We then deal with various issues loosely grouped under three headings: gathering information, managing information and putting information to use. An in-depth study that we made of CSIS's counter-subversion program overlaps all these themes, so it has a chapter of its own. We conclude with a review of some internal management issues and a chapter on a major study that we undertook, at the request of the Solicitor General, on official languages and staff relations issues in CSIS.

Formal Controls

Because of its wide powers of investigation and the secrecy that unavoidably surrounds much of its work, CSIS comes under a variety of controls, both judicial and administrative.

Before using its most intrusive powers, it must convince a judge of the Federal Court of Canada to issue a warrant (Part II of the *CSIS Act*). Indeed, it must first convince the Solicitor General, whose personal approval is required for each warrant application.

There are a number of other circumstances when CSIS requires the personal consent of the Solicitor General to do something--before it enters into an agreement with a province, for example (section 17 of the *Act*).

In addition, the Solicitor General issues instructions to CSIS on the conduct of particular cases or of entire classes of cases (subsection 6(2) of the *Act*).

The Solicitor General has his own watchdog on CSIS, the Inspector General (sections 30-33 of the *Act*). The Inspector General issues an annual certificate setting out whether he is satisfied with the secret annual report that the Director of CSIS makes to the Solicitor General, whether the Service has remained within the *Act* and the Solicitor General's instructions in its operational activities and whether it has made unreasonable or unnecessary use of its powers.

Our oversight mandate takes in all these controls (section 38 of the *CSIS Act*). We examine the Solicitor General's instructions, the annual report of the Director and the certificate of the Inspector General, and we keep an eye on warrants.

Warrants are dealt with in the next chapter. In this chapter we briefly report our observations on the other formal controls.

Ministerial Instructions

Two kinds of instructions are issued by the Solicitor General--ministerial directives and ministerial direction. Directives are policy statements, laying down how operations of a given class are to be handled. They usually require that certain matters be referred to the Solicitor General for decision on a case-by-case basis.

Direction, on the other hand, typically takes the shape of correspondence on specific cases, in which the Solicitor General may incidentally provide policy guidance or establish precedents that can be applied to other cases.

In last year's annual report, we indicate that we had a number of outstanding questions after reviewing the Compendium of Ministerial Direction containing all known directives and direction to the former RCMP Security Service and to CSIS. We are satisfied with the answers that CSIS and the Ministry of the Solicitor General have given us since then.

We also indicated last year that CSIS was reviewing the Compendium, looking for things that might have to be amended to conform with the *CSIS Act*. We understand that the task is now nearly complete, and we look forward to receiving the results.

New Business. We received copies of nine new directives and directions in 1986-87. A list can be found in Appendix A to this report. Two arrived late in March, and we were unable to examine them before the end of the fiscal year under review. We are satisfied that those we had a chance to study do not involve any unreasonable or unnecessary use of the Service's powers, nor do they impinge unduly on individual rights or privacy.

The Solicitor General also advised us in 1986-87 that seven directives and directions been withdrawn. One, dealing with security assessments, has been replaced with instructions. The others had also been overtaken by events.

As part of our review of statistics on operational activities, we now monitor the number of operations approved by ministerial directives. This will bring to light any significant changes that we need to look into more deeply.

From our experience, we are able to say that operations so sensitive that they require explicit ministerial authority are not numerous.

However, we discovered during 1986-87 that we had not been receiving copies of all documents that we consider ministerial directives or ministerial directions. The difficulty lay in a narrow interpretation that was being given to the legal description of these instructions.

At our request, CSIS is now reviewing all correspondence with the Solicitor General so gaps in our files can be filled in and we do not face the same problem again.

CSIS Annual Report and Certificate of the Inspector General

We have examined both the annual report of the Director to the Solicitor General and the certificate of the Inspector General for the calendar year 1986, and we are satisfied that they provide a realistic overview of the Service's work.

Because of their classification--Secret in the case of the annual report, Top Secret in the case of the certificate--we cannot disclose their contents.

However, what we learned from them has provided additional depth to the observations we make on our own authority in this report and will help to guide our continuing oversight activities.

We take this occasion to express our appreciation for the energy, industry and thoroughness shown by the Inspector General.

The Oversight Process

We conclude this chapter with a few facts about our oversight operations generally.

Computer Age. We entered the computer age in 1986-87, getting the data-processing capacity we need to carry out our mandate "to compile and analyse statistics on the operational activities of the Service" (subparagraph 38(a)(vii) of the *CSIS Act).*

Security considerations put a strict limit on how much we can say about what we learn through statistical analysis.

However, we have continued our practice of reporting warrant statistics (page 10 of this report). And statistical analysis also lies behind much of what we say about the extent to which CSIS has used various investigative tools, the CSIS budget and spending, the effects of the *CSIS Act* on operations, and progress towards civilianization.

The value of statistical analysis is that it gives us a basis for putting pertinent questions to CSIS without requiring us to undertake the impossible task of examining every operation.

Statistics have been secured from CSIS on resource allocation, warrants, the use of sources, campus operations, personnel, the targeting of groups and individuals for investigation, illegal acts and other matters. Most data is provided on a quarterly basis.

In most fields, we had data for only one quarter in 1986-87, so our analytical work was necessarily limited. It was, of course, impossible in these cases to plot trends. As we accumulate more information, we expect statistical analysis to be an important tool in oversight.

None of the data we have seen suggested an unreasonable or unnecessary use by the Service of its powers.

Formal Inquiries. We make formal, written inquiries to CSIS--145 of them in 1986-87. At year-end, only 18 were awaiting answers.

We derive our questions from many sources. Some are suggested by our own research, of course, and some emerge from our investigation of complaints.

Others are prompted by news reports--for example, in 1986-87, stories about alleged fund-raising for Contra rebels in Nicaragua, recruiting by the white-supremacist Aryan Nation, alleged surveillance of a peace activist who met with a suspected Soviet agent, immigration applications from people alleged to have been involved in torture and murder in Chile, and many more.

We kept a watching brief on investigation of the Air India disaster of June 23, 1985. There is, unfortunately, nothing we can say publicly, beyond giving an assurance that we will continue to follow developments.

We also pursue with CSIS questions put to the Director by members of Parliamentary committees, which he cannot answer in such public forums. Some of those that came up when the Standing Committee of the House of Commons on Justice and Solicitor General questioned the Director on December 11, 1986, have been answered to our satisfaction; we are waiting for responses to the rest.

Briefings. We met as a Committee with the Solicitor General, and the Chairman met frequently with the Solicitor General, the Deputy Solicitor General, the Director of CSIS and the Inspector General.

We make a point of holding our regular meetings in various cities across Canada, and we take advantage of these occasions to visit local CSIS offices, where we meet management and staff and are briefed on operations. In 1986-87, we visited the Ottawa Region, the Prairie Region in Edmonton, the Atlantic Region in Halifax, the Quebec Region in Montreal and the Toronto Region.

Our visit to Montreal came in November, in the last stages of our special study on official languages and staff relations in CSIS (reviewed in Chapter 8). Discussions with both managers and staff there helped give us a feel for the situation when we sat down to write our report on this inquiry.

3. How CSIS Knows

This chapter focusses on information-gathering by CSIS and some issues it has raised.

Behind Federal Court Warrants

To make use of its most intrusive powers, CSIS requires warrants issued by judges of the Federal Court of Canada. These powers include wiretapping, eavesdropping by microphone, capturing optical images, intercepting recorded communications, searching for documents and paraphernalia, and intercepting mail.

Though not required by law to do so, we read some affidavits sworn in support of warrant applications.

But the affidavits have already been seen by both the Solicitor General and by judges of the Federal Court of Canada before they reach us, so we started to go behind the affidavits to examine the operational files on which they are based.

Because these files are not seen by anyone outside the Service except the Inspector General and us, this provides a distinct second line of defence against unreasonable or unnecessary use by CSIS of its powers.

We found that affidavits were generally factual but, not surprisingly, tended to present the case for the use of intrusive techniques rather than a balanced ledger of pros and cons.

Devil's Advocate. When CSIS asks for a warrant, there is, of course, no advocate for the target.

We are informed that the Solicitor General makes sure, in reviewing warrant applications, that everything being sworn to is an ascertainable fact, not merely a conclusion the investigator has drawn from the facts, and he sends some applications back for amendment before he lets them go to the Federal Court. Indeed, we are informed that he has rejected some requests outright. We welcome his vigilance.

We are also mindful of the role played by the presiding Federal Court judge in each case. While no applications have been turned down by the Court, searching questions have been asked from the bench and conditions designed to protect individual rights have been imposed in the order granting the warrant (see, for example, page 20 of this report).

But the controls now exercised by the Solicitor General and by judges are no stronger than the personal commitment of the people involved. As for us, our review comes after the fact; if there were ever flagrant abuse, we could make our concern known to Parliament, but too late to stop it from taking place.

The Solicitor General, in consultation with CSIS, should consider whether there ought to be a "devil's advocate" at some stage of the procedure--either before the Federal Court or before the Solicitor General himself--to argue the case against the warrant.

This is something that Parliament too might consider when the *CSIS Act* gets its five-year review in 1989.

Basket Clauses. Generally speaking, targets are named in warrants. The location where a warrant can be exercised is specified. "Basket clauses" allow intrusive powers to be used at the same location against unnamed associates of the target, who may be identified only after the warrant is granted. Otherwise CSIS would have to return to the Federal Court for a new warrant each time an associate of the target surfaced.

The Inspector General is currently looking into the issue of who can designate targets under basket clauses in warrants.

We too have a concern about the use of basket clauses and are looking into it. The first question is whether it is acceptable at all. If so, the next question is who within CSIS--or the Ministry of the Solicitor General--should have the power to designate additional targets not named in the warrant.

Counting Them Up

As part of our oversight routine, we have started to compile quarterly statistics on warrants. With our new computer capacity, we can now examine the use of warrants in the aggregate and broken down by types of powers, regions and targets. Aggregate figures for the calendar years 1985 and 1986 are shown in Table 1.

Table 1. New and Renewed Warrants Granted to CSIS, 1985 and 1986

	1985	1986
New warrants	82	94
Warrants renewed	27	11
Total	109	105
Average duration of warrants (days)	173.6	162.2

(Source: CSIS)

Raw data such as we provide here do not permit meaningful comparisons with pre-1985 warrant statistics.

Before the *CSIS Act* took effect on July 16, 1984, warrants for security intelligence investigations were issued under the *Official Secrets Act*. Each of these warrants ordinarily permitted the use of one power against one target.

Warrants issued since then under the *CSIS Act* can be far more sweeping. One of these warrants can authorize the use of many powers against many targets.

Maximum. We are discussing with CSIS the best ways to present the maximum amount of information to the public about warrants and the use of intrusive powers.

We continue to have some concern that aggregate warrant statistics under the *CSIS Act* do not give as accurate a picture of the level of intrusive activities as did the statistics that used to be published under the *Official Secrets Act.*

We get enough information from CSIS to let us develop more revealing statistics ourselves and publish them. But without evidence of abuse, we respect the Service's position that the full story cannot be told without divulging information of significant intelligence value.

This is another issue that Parliament may want to take up when the *CSIS Act* gets its five-year review in 1989.

Other People's Mail

We made a particular study of mail-opening. After the outcry a few years ago over illicit mail-opening by the RCMP, some Canadians were uneasy when CSIS got the legal power to intercept mail, even if this power was subject to the same warrant requirements as any other intrusive activity.

They may have imagined squads of men and women in trench coats and slouch hats, huddled over tea-kettles, steaming open letters to somebody's Aunt Tillie and solemnly recording tidbits of family gossip.

The picture we got was quite different. Apart from the fact that tea-kettles have been overtaken by high-tech methods, very few envelopes had been opened by the end of 1986.

We have reason to expect that mail interception will increase. Only technical difficulties prevented the Service from intercepting the mail of two further targets in 1986. As 1987 began, CSIS held some warrants granting mail-opening powers, ready for use as the need presented itself. A single warrant can cover more than one address.

CSIS says it intends to use this power only when there is reason to suspect that an individual or organization is using the mail to further a threat to national security.

We will continue to monitor mail-opening.

Canada Post is cooperating with CSIS, and a formal memorandum of understanding between the two organizations is being prepared. It will come to us in due course for examination.

We would be pleased to see provisions for cooperation at a less intrusive level than the interception of mail. Tracing, for example. Canada Post is in a position to provide CSIS with lists of the names and addresses that targets correspond with. One issue is whether this, too, should require a warrant.

Emergency Warrants

Before leaving the use of intrusive powers, we raise once more the question of emergency warrants.

An application for a warrant ordinarily originates with an investigator. There is internal review by senior officers and by a formal Warrant Review Committee. Under the *CSIS Act*, each application must be approved by the Solicitor General personally before it goes to a judge of the Federal Court.

Cumbersome as it sounds, this procedure has been streamlined enough to ensure that whenever CSIS has needed a warrant, it has been able to get one in time. Sooner or later, though, an operation is bound to be weakened because a warrant could not be secured quickly enough.

Could This Happen? In our last annual report we outlined a scenario in which CSIS heard at the last minute about a terrorist stopping over briefly in Canada between flights. An instant warrant might be needed so that meetings the terrorist held during the stopover could be monitored. This is the kind of occasion when current procedures may be too slow.

We suggested that the *Act* might be amended so that the Director of CSIS could issue a warrant himself in emergencies, subject to speedy review--within 48 hours, say--by a judge of the Federal Court. We suggested that there should also be an early report to the Solicitor General and to us.

We still believe that special circumstances call for special measures and that some emergency warrant procedures should be written into the *Act*.

To help Parliament when the *Act* gets its five-year review in 1989, we have started to compile statistics on the length of time it takes to obtain warrants. These statistics could help pinpoint any bottlenecks in the system as well as document the need for special measures.

Open Sources

One way that CSIS can limit its reliance on intrusive powers is by mining open sources like scholarly publications and the mass media, both foreign and Canadian.

We are far from satisfied that CSIS takes open sources seriously enough as an alternative to undercover work. The use of open sources remains a pale imitation of what the McDonald Commission envisaged and what we have repeatedly urged for the sake of both effective security intelligence operations and minimum intrusion on personal privacy and freedoms.

We acknowledge that the Service started to create reference sections in regional offices in 1986-87 and that it expanded the Open Information Centre at Headquarters.

This Centre now has a technical services section, a research unit, an Emergency Operations Centre and two reference units. A User Committee was established to help the Centre stay abreast of the Service's real needs, and additional staff was appointed. Some vacancies remain but the key positions have been filled.

Bilingual Service. In particular, we are pleased that the Open Information Centre now employs more bilingual staff and plans an increase to three from one in the number of French-language computer data bases it has access to.

As we note elsewhere in this report (Chapter 8), the Service has lagged badly in giving its Francophone and Anglophone employees equal opportunities to work in their own languages, and every step toward this goal is welcome.

However, services available in French are still far less than those available in English, and we urge all possible speed in carrying out plans to increase the volume of French-language information and services in French. In particular, we hope that a greater use of foreign French-language open media will ensue.

Research. In general, we believe that the Service is not making the most of its opportunities to use open sources.

The research unit gives us great concern. In our last annual report, we noted that the Service had preferred to select researchers from among its "street-wise" intelligence officers, and we suggested that experienced, university-trained professionals would be more appropriate choices.

This point unfortunately needs to be made again. For, although new researchers appointed to this unit are university-educated, they do not have the broad experience in research and government that we think essential.

Furthermore, these researchers are only temporarily assigned to the research unit. They are to be replaced eventually by people with lower job classifications, who will require the appropriate training.

We also believe that better use could be made of the research unit. It now clips items from the media and searches computer data bases for information requested by investigators and analysts.

Researchers do not carry out analyses of their own or even prepare summaries of information on file. This represents a wasted opportunity. It is impossible to resist the suspicion that it reflects the case-oriented approach of police work.

We concur with the McDonald Commission's observation that "security intelligence reports should be less case-oriented; greater attention should be paid to providing government with longer term, more broadly based assessments of security threats facing Canada".*

---

* *Freedom and Security under the Law,* the Second Report of the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (Ottawa, 1981), page 607

Research unit staff are in a unique position to give the Service a global perspective as active researchers--detecting new trends as they take shape, for example.

The Open Information Centre has two ways of handling information. Through its Emergency Operations Centre, it can quickly get information about fast-breaking events reported in the mass media. At a second stage, information is drawn from clippings and computerized data bases.

This is a more comprehensive approach than there has been in the past, but it still begs the question whether research unit staff could be playing a more important analytical role.

Further Needs. Our inquiries revealed that the use made of the Open Information (by operating units is not systematically recorded and analysed. We suggest that doing this would be a first step towards seeing where effective use could be increased.

We also encourage the Service to complete its network of regional reference centres quickly as possible.

Canadian Police Information Centre

Despite some improvement in 1986-87, the Service's access to the Canadian Police Information Centre (CPIC) remains woefully inadequate.

CPIC is a computerized, radio-linked network that gives officers of the RCMP and provincial and municipal police forces instant access to information in three data banks by the RCMP. These banks cover:

- Vehicle registrations.
- The police records of individuals and outstanding warrants for their arrest.
- Other relevant information about these individuals.

The potential usefulness of CPIC to CSIS is self-evident. Ready access to information on vehicle registrations alone would be invaluable to CSIS surveillants as they follow targets.

But the Service has had to fight every inch of the way to gain even partial access.

The reason--as it is lamely explained to us--is that CPIC was designed to serve “peace officers" and CSIS investigators are not technically "peace officers".

This is nit-picking. When CPIC began, security intelligence fell within the domain of the RCMP, and the people who carried out this work were peace officers. In CSIS, they are civilians without, for example, a peace officer's powers of arrest.

Same Duties. But CSIS investigators have the very same duties and responsibilities that security intelligence investigators had in the RCMP. If CPIC was needed for security intelligence work then, it is needed now.

In both our previous annual reports, we expressed frustration over difficulties CSIS faced in gaining direct access to CPIC. We discussed the issue with the Commissioner of the RCMP personally. Finally, in our last annual report, we urged the Solicitor General, who is responsible for both CSIS and the RCMP, to intervene.

He did so, and the CPIC Advisory Committee has since granted CSIS direct access to the vehicle registrations data bank. But direct access to other banks is limited to counter-terrorism operations only.

When CSIS wants any other CPIC information--the criminal record of a counter-subversion target, for example--it must go to the RCMP, which punches in the request and passes back the read-out.

This entails unnecessary delay, and it fosters an unwarranted notion that CSIS is a junior partner to the RCMP.

Turf Battle. Even the limited direct access CSIS has now is imperfect--to put it mildly. As 1986-87 ended, the RCMP had supplied CSIS with only four CPIC terminals. There was still no terminal at CSIS Headquarters. More were on order, but there is no doubt in our minds that the delay represented continued reluctance to treat CSIS as an equal partner.

Meanwhile, thousands of police officers in quiet suburbs have CPIC terminals mounted under the dashboards of their cruisers, letting them check out teenagers loitering in a parking lot as easily as they could check out the getaway car in a bank robbery.

But no CSIS surveillant in hot pursuit of a suspected terrorist has a similar opportunity to get an instant reading on his quarry.

We see no reason why CSIS should make do with anything less than unlimited access through an adequate number of terminals. This is a classic example of institutions charged with great responsibilities giving priority instead to parochial turf concerns.

Academe and Officialdom

Concerns have been raised in various forums, including the Standing Committee of the House of Commons on Justice and Solicitor General, about fishing expeditions in post-secondary institutions of learning and the use of public servants as regular informants.

Post-Secondary Institutions. Information-gathering at institutions of higher learning must maintain a delicate balance between two social values.

On the one hand there is academic freedom, which implies the opportunity, if not the duty, to express dissent peacefully, without fear of harassment. Many times in history, one generation's radicalism has become the next generation's pillar of social order. Democracy itself has had its times of disrepute.

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 have now confirmed that the Solicitor General's instructions and policy on campus operations by CSIS conform to the position established for the RCMP and agreed to by the Canadian Association of University Teachers in 1963, that:

> There is at present no general RCMP surveillance on university campuses. The RCMP does, in the discharge of its security responsibilities, go to the universities as required for information on people seeking employment in the public service or where there are definite indications that individuals may be involved in espionage or subversive activities.

The activities in question are now those defined by section 2 of the *CSIS Act* as "threats to the security of Canada".

The decision whether to carry out investigative activities on campus is further limited by a ministerial directive of June 8, 1984. It provides that investigations should occur only where there are "objective indications that individuals may be involved in activities judicial to Canada", and it requires ministerial approval for certain kinds of investigation.

Public Servants as Sources. Concerns have been raised about the use of federal government employees as sources because of the pressure they might feel to cooperate with in order to protect their jobs.

A secret directive issued by the Solicitor General lays down general principles governing the use of federal employees as sources.

Inter-Organizational Arrangements in Canada

Apart from the issue of undercover sources in federal jobs, CSIS needs access to records held by police forces and other government agencies--federal, provincial, local and foreign--to do its job effectively and efficiently.

Perhaps CSIS's most important partner is the RCMP. Indeed, the relationship has many ramifications that we defer our discussion of it to a special section in Chapter 5.

Formal arrangements between CSIS and other bodies require the prior approval of the Solicitor General, and we review them after the fact.

Federal Departments. In 1986-87, we got copies of memoranda of understanding with three federal departments, giving CSIS access to personal information as permitted under paragraph 8(2)(e) of the *Privacy Act*--that is, information required to enforce any law or carry out a lawful investigation.

The departments are Revenue Canada (Customs and Excise), the Department of Secretary of State and the Canada Employment and Immigration Commission. There are two agreements with the Canada Employment and Immigration Commission.

This brought the total number of agreements with federal departments and agencies to six; there were already agreements with Canada Post* and the Department of External Affairs.

We are satisfied that these agreements adequately protect personal privacy while providing CSIS with enough access to do its job.

Provinces and Police. Copies of five memoranda of understanding providing for liaison and exchanges of information with provincial government departments and with police forces other than the RCMP came to us during 1986-87.

These agreements are with British Columbia, Alberta, Ontario, Prince Edward Island and Nova Scotia.

We found them unobjectionable from the privacy point of view.

But we noted with some concern that they do not appear to be binding. We hope they will not prove to be the seedbed of future problems if CSIS needs information that the provinces or police are, for any reason of their own, reluctant to give.

We also take the occasion to suggest that CSIS keep full and accurate records of all contacts under these memoranda.

And we urge high priority for the negotiation of agreements with the remaining provinces to ensure a smooth, rapid flow of information both ways when it is needed.

Foreign Arrangements

Arrangements with foreign governments generally cover exchanges of information to meet three needs--vetting applications for visas and immigration, carrying out security clearances and, finally, protecting the respective national interests of Canada and the other country.

CSIS also has some arrangements with sister security and intelligence agencies for cooperation in such matters as professional training.

In 1986-87, we got copies of five new and revised agreements with foreign governments. We also saw copies of the ministerial direction authorizing each agreement. All were in order.

There have been concerns that CSIS did not clearly distinguish between foreign liaison arrangements that were merely desirable and those that were strictly necessary.

---

* Earlier, we indicated that an agreement is still being worked out with Canada Post to govern mail-opening operations. The agreement referred to here deals with Canada Post's own files.

We are of the opinion, supported by independent legal advice, that the "strictly necessary" rule found in the *CSIS Act* (section 12) does not apply to the conclusion of agreements with foreign governments. It is sufficient that such agreements be conducive to the protection of national security. But we are pleased, nonetheless, that the Solicitor General has sought clearer statements of necessity from CSIS in its proposals for new arrangements.

So that we can monitor arrangements with foreign governments more knowledgably in future, we have asked the Solicitor General to start sending us copies of the letters in which the Secretary of State for External Affairs comments on each arrangement as it is proposed.

Two continuing foreign liaison issues call for particular comment--the legacy of arrangements negotiated by the RCMP and, second, the position of CSIS liaison officers in certain Canadian missions abroad.

The RCMP Legacy. Early in 1985, we received from CSIS thousands of pages that it inherited from the former RCMP Security Service, setting out existing arrangements with foreign governments and their agencies. In our previous annual reports, we recommended that these arrangements be reviewed in light of the new *CSIS Act* and renegotiated.

Since then, a new consolidation of foreign arrangements has been prepared, examined by the Department of External Affairs and approved by the Solicitor General.

We have come to the conclusion, supported by independent legal counsel, that the transition provisions of the *CSIS Act* are broad enough to validate foreign arrangements originally entered into by the RCMP, making renegotiation unnecessary on purely legal grounds.

In consolidation, CSIS also let some arrangements lapse. This was sensible; some that were appropriate for a police force like the RCMP (whose members have, for example, powers of arrest) were inappropriate for a civilian security and intelligence service (whose members do not).

Liaison Officers. CSIS has security liaison officers in some Canadian missions abroad, responsible for providing timely and relevant information and assessments on security matters to the Service and to the authorities of the host countries.

We have examined the role these officers play and find it consistent with the *CSIS Act*.

But we found some confusion about the respective responsibilities of CSIS's liaison officers and the RCMP liaison officers who are also posted to some missions. We will return to this subject in our general discussion of CSIS-RCMP relations (page 29).

Unlawful Acts

The Director reported, under the *CSIS Act* (section 20), that an employee may have overstepped the law on the job by failing, on two separate occasions, to obtain routine signatures

from a supervisor on documents authorizing certain acts. The employee has been reprimanded and is now well aware of the requirement for the signature. We agree that no charges are warranted.

There have also been a small number of incidents in which CSIS employees have been investigated by management for misbehaviour off the job. These investigations led to dismissal or resignation. Since they are not related to the work of the Service, we regard them as a matter of personnel administration.

Solicitor-Client Privilege. However, there was a serious breach, which the Director did not report as such, when records of solicitor-client communications were retained in three of the Service's five regions for about a year, in defiance of conditions written into the relevant warrants by Federal Court judges.

The problem arose when new instructions from Headquarters on the retention of records generally were misunderstood, and it was swiftly corrected when it came to light. Because of their privileged nature, the records had been sealed, and they are being destroyed as required by the warrants.

Gap. In the short term, no material harm was done. We have read the report of the Inspector General who, after a thorough investigation, came to the same conclusion. However, this situation highlights a gap in the *CSIS Act;* unlike the *Criminal Code*, it affords no protection to solicitor-client communications.

On the face of it, this is disturbing. People should be free to discuss their legal affairs in complete frankness with their lawyers, confident that what they say will not be disclosed without their consent. This is the essence of solicitor-client privilege.

So we looked into this matter closely and discussed it on three separate occasions with CSIS at the deputy director level.

As a result of media reports,* we also made inquiries about a specific case of intercepted communications between a lawyer and his client. We were satisfied that there were genuine security concerns to justify interception in this case. We also noted that the information gained was not passed on to any other agency.

Delicate Balance. This left us with the overall issue to consider. As in so many other areas of security intelligence, there is a delicate balance to be maintained.

Without reference to any particular incident, it is easy to imagine circumstances in which interceptions would be justified--when the lawyer appeared to be a co-conspirator with the "client" against the national interest or when a lawyer acted as a message centre for conspirators. Not even under the *Criminal Code* is the lawyer's gown roomy enough to shelter communications that concern illegal acts involving the solicitor.

---

* Notably in *The Globe and Mail*, Toronto, January 8, 1987.

Federal Court judges have made a practice of writing particular protections for privileged solicitor-client communications into warrants, as follows:

- Prohibiting the interception of communications at the office or residence of a solicitor or at any other place ordinarily used by a solicitor for the purpose of consultation with clients. (This parallels the protection found in the *Criminal Code.)*

- Restricting the interception of calls made between the target and the solicitor (or the solicitor's employee) to calls that the Director or a regional director general determine are related to the threat specified in the warrant.

Present Arrangements. CSIS has procedures for giving effect to these conditions. When a record is made of communications between a solicitor and the client, it is submitted to the Director or a regional director general. If he determines that the communication does not further a threat to the security of Canada, all records of the communication are destroyed and no disclosure is made.

Except as we have explained above, we believe that these procedures are respected. But we are not satisfied that this is enough.

One concern is that, like the Solicitor General's review of warrant applications and our review of the operational files behind them, these safeguards rely on individual commitment--that of Federal Court judges to keep writing them into warrants. Unless the safeguards are written into law, that could change at any time.

This is a further issue that Parliament may want to consider when the *CSIS Act* gets its five-year review.

4. What CSIS Knows

Having examined in the last chapter how CSIS gets information, we turn now to its management of information. Is CSIS keeping unnecessary confidential information, especially about individual Canadians? How is the information that it accumulates used? In this chapter we focus on the first question, leaving the second to be dealt with in Chapter 5.

Legal Limits

The *CSIS Act* sets two important limits on the collection of information, as follows:

- The information must be related to "threats to the security of Canada" (section 2).
- Such information may be collected to the extent that is "strictly necessary" to deal with activities that can reasonably be suspected of being threats (section 12).

For easy reference, it may be worth quoting section 2's definition in full here. It says that the term "threats to the security of Canada" includes:

> (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,
> (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)*.

Inherited Information

Against this background there are serious legal as well as ethical questions to be asked about information in operational files that CSIS inherited from the RCMP Security Service.

Some of it was gathered during the unhappy period documented by the McDonald and Keable Commissions, when some investigators let their genuine concern for national security run away with their appreciation of privacy and the right to engage in democratic dissent. We are also thinking of information dating back to the heyday of protest and the so-called New Left in the 1960s.

No one knows everything that is in these files, because they have not all been systematically reviewed. But, in light of the McDonald and Keable findings, some concern is reasonable: Does all this information meet section 2's definition of a threat to the security of Canada? Is it all still strictly necessary as required by section 12?

If the answer to either of these questions is No, then more questions arise. Does CSIS have legal authority to keep unnecessary or irrelevant information on file? Might any initiative based on such information be subject to challenge before the courts?

CSIS has resisted our urgings that it review all these files and weed out material that does not meet the requirements of sections 2 and 12. There are, we admit, some real difficulties.

Moratorium. In the short term there is the moratorium placed on file destruction following the Deschênes Commission's discovery that old immigration files it needed in its investigation of alleged war criminals had been routinely destroyed. We return to the question of out-of-date CSIS files in a moment.

Even if the moratorium were lifted, it would be a gargantuan task to go through these files one by one, getting rid of any inappropriate information.

At another level, we must recognize too that gathering and looking for threatening patterns in apparently innocent bits and scraps of information is the business CSIS is in.

Anyway, said CSIS, it should be enough that inappropriate information found in these files not be used; that is what our Committee is for--to blow the whistle if limits like the "strictly necessary" rule are overstepped.

We don't shrink from our responsibility to monitor the Service's use of information. But we also face a problem of scale; we can hardly watch every move of every member of the Service. And we find it hard to imagine that irrelevant information, even if it is not technically "used", would not at least colour the approach of an investigator or analyst who saw it.

So we would still like to see these files systematically weeded. The task could be reduced to manageable proportions if it were done progressively, on a pre-determined schedule over a period of years.

We were pleased to learn in the course of the year that the Solicitor General shares our concerns and has asked CSIS to develop file retention standards in conformity with sections 2 and 12 of the *CSIS Act*.

Retirement of Old Files

This brings us back to the question of retiring and destroying entire files that have outlived their usefulness--a concern we inherited from the McDonald Commission.*

As a result of the McDonald Commission's observations, the RCMP Security Service and the Dominion Archivist--who is responsible for assessing and approving proposals to retain or destroy federal records--developed disposal schedules for inactive files.

---

* *Freedom and Security under the Law*, the Second Report of the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (Ottawa, 1981), page 521

In the late 1970s, there was a major disposal of files that had been opened before 1973. Then between July, 1984, when CSIS took over from the Security Service, and February, 1985, when the moratorium described above came into effect, some 77,800 files with no security intelligence value were destroyed after review.

Today, more than 67,000 files are ready for destruction once the moratorium ends.

We are keeping an eye on this issue and have asked for copies of the disposal schedules. We note that government policy calls for a review of such schedules every five years, and we were encouraged to learn that CSIS launched such a review with the Dominion Archivist in December, 1986.

Foreign Intelligence

Another issue became apparent when we examined the flow of information in one operational branch of CSIS.

It seemed to us that information supplied by friendly foreign intelligence services might too easily be accepted by CSIS at face value; it may not be getting the same critical scrutiny as information from Canadian sources.

Indeed, we sensed that CSIS might be too quick to accept the foreign policy underpinnings of this information instead of recasting it in terms of Canadian policy (see, for example, page 37 of this report). Canada has its own national interests, distinct from the interests of any other nation.

The McDonald Commission pointed out the danger of adopting the "outlook and opinions of a foreign agency, especially an agency which has come to be depended upon heavily".* The warning remains timely.

Due Weight. The *CSIS Act* requires the Service to consult with the Department of External Affairs on various aspects of international relations (paragraphs 17(l)(b) and 19(2)(b). We encourage closer collaboration between CSIS and this Department in the assessment of international events and the conduct of CSIS's activities to ensure that Canadian foreign policy gets its due weight.

The McDonald Commission also noted, incidentally, that greater use of open information could be a bulwark against excessive dependence on one or more foreign agencies. This supports our contention that CSIS should be making greater use of open sources (see page 12 of this report).

---

* *Freedom and Security under the Law*, the Second Report of the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (Ottawa, 1981), page 632

Incidental Information

In 1986, CSIS developed new policy for dealing with information acquired inadvertently although it has nothing to do with national security concerns. CSIS defines two categories of such information--"spin-off" and "incidental".

Spin-offs are information with potential use in criminal law enforcement, national defence the conduct of external relations or the general pursuit of the national interest. We deal with it in the next chapter of this report.

Incidental information is everything else that is not necessary to national security. Such information is--quite properly--destroyed.

There are some kinds of information that CSIS should clearly be deaf to--and mute about. For example, it must never interfere in the democratic process by letting the government know about anything like the electoral strategy of a legitimate opposition party. We believe that it has never done so.

5. What CSIS Does

The bottom line is how CSIS's information is used. Some issues this raises are the subjects of this chapter. Cooperation with the police is one major use that can be made of CSIS information, so operational relationships with the RCMP are also dealt with here.

Spin-Off Information

We ended the last chapter with a discussion of "incidental information" that is destroyed because it is not useful either for national security purposes or for criminal law enforcement, national defence, the conduct of international relations or otherwise in the national interest.

Unsolicited information that could be useful for one of these non-security purposes is termed "spin-off" information. Under the *CSIS Act* (section 19) it can be passed on to the appropriate authorities.

If CSIS were firing off advisories in all directions with spin-off information, we might worry that it was casting its net wider than "strictly necessary" (section 12 of the *CSIS Act)* and concerning itself with more than threats to the security of Canada.

In fact, our concern is that the Service seems too cautious in this regard.

CSIS in Court

The Service's jealousy of its secrets has been spotlighted for the public more than once as its officials have interrupted trials and cut off questioning of their colleagues, citing the *Canada Evidence Act.* Subsection 36.1 (1) of this *Act* provides that:

> A Minister of the Crown in right of Canada or other person interested may object to the disclosure of information before a court, person or body with jurisdiction to compel the production of information by certifying orally or in writing to the court, person or body that the information should not be disclosed on the grounds of a specified public interest.

Section 36.2 provides for the hearing of objections in the Federal Court of Canada when it is alleged that disclosure "would be injurious to international relations or defence or security" and also for appeals.

Headlines like "Spywork: How it can close down a court" *(Toronto Star,* June 21, 1986) and "Gag order needs no reasons" *(Ottawa Citizen,* June 7, 1986) have been the result of CSIS interventions under the *Canada Evidence Act.*

This is not an unexpected issue. Keeping sources and "tradecraft" secret is a preoccupation of all security and intelligence services. Protecting human sources is a special concern. An informant whose cover is blown may not be useful any more. And potential sources are bound to shun a service that does not protect them from exposure and its consequences.

All Relevant Evidence. Nonetheless, we feel that means must be found to ensure that all relevant evidence is heard by the courts--if not by the public--in criminal cases. For one thing, CSIS evidence might tend to show the innocence of the accused; in such a case silence seems to weaken the fundamental principle that before our courts a person is innocent until proven guilty.

We note that the *Criminal Code* makes provision for excluding the public from rooms for reasons of "public morals, the maintenance of order or the proper administration of justice" (section 442).

Would it help if "national security" were added to the list? The difficulty is that would not exclude the accused, who might have a clear interest in such matters as identifying informants and learning CSIS procedures.

So there is no easy answer. It is another issue that Parliament may wish to take up when the *CSIS Act* gets its five-year review in 1989.

Assistance to Police

This leads us into the whole issue of CSIS relations with the police. For CSIS is tight-lipped not only in court. Because of its concern for the secrecy of its operations, it has at times withheld information from the police.

We share the view of the McDonald Commission* that CSIS ordinarily has a duty to tell the police what it knows about criminal activities. If, for example, a surveillant parked in the shadows sees someone stealthily cutting glass out of a jewelry store window, looking for all the world like a burglar at work, the police should ordinarily be called in. This is permitted under paragraph 19(2)(a) of the *CSIS Act*.

We acknowledge that there are exceptions--when a police investigation, and perhaps evidence at a subsequent trial, would irremediably compromise a vital security operation. For example, if the arrival of a police car would prompt important targets to move to a new location unknown to the Service.

Regional Directors General decide whether information about criminal activities should be passed on to the police. Guidelines are set out in an Operational Bulletin issued under the authority of the Director of CSIS.

On Its Merits. What the rules boil down to is that each case is considered on its merits in light of the seriousness of the supposed offence, the protection of CSIS sources and the potential for damage to CSIS's operational capability if its involvement in reporting the offence became known. The Service is looking into the need for more formal guidelines.

---

* *Freedom and Security under the Law*, the Second Report of the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (Ottawa, 1981), page 605

Our preference is already clear. We are content to see decisions made by the regional directors general. But we believe that the criteria should be set in a new ministerial directive, to shelter them from any arbitrary change that CSIS itself. might make in future.

Relations with the RCMP

While senior managers in both CSIS and the RCMP seem increasingly comfortable within their respective boundaries, it has obviously been harder to plot the line inch by inch in the field.

The term "healthy tension" has been used to describe the situation, but we think it would be even healthier if it were a little less tense. We are encouraged, though, that problems are recognized and that steps are being taken to deal with them.

The Solicitor General has provided us with a copy of a memorandum of understanding between the RCMP and CSIS, consolidating a number of arrangements for cooperation and for sharing services and administration.

He informed us that he had deferred approval of chapters on CPIC and information sharing. We support this decision. CPIC we have already discussed (page 14 of this report). As for information sharing, we have written to the Solicitor General to voice our concerns that there may be duplication of effort between CSIS and the Crime Intelligence Branch of the RCMP.

With these reservations, the memorandum provides a firm base for relations that are smoother because they are clearly defined in a number of mundane areas like accommodations, air services, multilingual translation services, pay administration, photographic services, printing and the use of secure telecommunications devices and electronic data processing.

Liaison Officers. The Solicitor General established an exchange of liaison officers between the CSIS and RCMP counter-terrorism programs in the latter part of 1986.

Counter-terrorism is where the CSIS and RCMP mandates touch most closely and are most likely to grate. There are, as the Director of CSIS, among others, has pointed out,* two needs in this field.

There is an intelligence need directed at predicting and sidetracking incidents--the CSIS domain. And a law enforcement need directed at apprehending criminals and assembling sufficient evidence to convict them--the RCMP domain.

At the stage when a criminal conspiracy is afoot, before an incident has occurred, the two domains overlap. CSIS-RCMP cooperation is plainly essential. The *CSIS Act* provides for

---

* House of Commons, *Minutes of Proceedings and Evidence of the Standing Committee on Justice and Solicitor General*, December 11, 1986.

this overlap by setting out quite clearly the intelligence responsibilities of CSIS and the law enforcement responsibilities of the RCMP (sections 12 and 61).

Airport Security Alert

Unfortunately, what we actually found in a case study of one counter-terrorism operation--the "airport security alert"--was turf battles and distrust.

The story began in December, 1985, when police were tipped to an alleged Libyan plot to place a bomb on a commercial airline flight originating in Ottawa.

Security precautions were subsequently increased at major airports, at considerable cost to the taxpayer and considerable inconvenience--to say nothing of anxiety--to travellers. Furthermore, the threat diverted public safety personnel from other important duties and disrupted routine police investigations.

Whether it was because the information was frivolous or because early exposure of the conspiracy and efforts to head it off led to its cancellation, no explosion occurred. Airport security precautions returned to normal.

Case Study. Fresh from the Air India and Narita Airport disasters of 1985, Canadians heaved a sigh of relief and went on with their business. We too went on with our business and seized the opportunity to make a thorough case study of how CSIS and police forces work together in an anti-terror operation.

This case was a good example of where counter-terrorism, criminal investigation and security intelligence all come together, requiring the cooperation of various players and the need for working closely within their roles and functions.

We are not, of course, at liberty to publish our full report. Besides security considerations, some of our informants were promised confidentiality in return for their cooperation. The RCMP and the Ottawa City Police, which were responsible for the criminal investigation, are not answerable to us. But we are grateful to them, as well as to CSIS, for their unstinting help in this inquiry.

However, we have made a report to the Solicitor General with our conclusions and recommendations.

Reticence. It was not clear to us that CSIS was a full participant in the *ad hoc* task force that took shape to track down the alleged conspirators. It quickly became very obvious that the flow of information between CSIS and the police could have been better.

The reticence worked both ways. The police, who had the original tip, waited six days before calling on CSIS for help, for example. We had the impression that the RCMP, in particular, felt that this was exclusively a police operation.

On the other hand, CSIS missed an opportunity to counter that feeling when it did not take up an invitation to assist in some surveillance.

Guidelines. Indeed, we discovered that CSIS and the RCMP had yet to completely mesh their mandates in counter-terrorism. While the exchange of liaison officers mentioned above is a valuable step, we see a need for formal operational procedures. Among issues that procedures should deal with are:

- Limits that can be put on the use of shared information.

- How responsibility for surveillance duties should be shared.

Meanwhile, we recommended that the Ministry of the Solicitor General carefully monitor the liaison arrangement and keep the Solicitor General informed of progress.

We also recommended ministerial direction to encourage appropriate sharing of information in the investigation of terrorist activities that require the attention of both CSIS and the RCMP, even on such sensitive matters as the identity of sources, recognizing that intelligence ultimately required for court proceedings should be provided in a way that protects future intelligence initiatives.

Public Relations. One finding was that local police forces do not seem fully aware of CSIS's role. So we have recommended that CSIS undertake a public relations exercise to provide law enforcement organizations with information on its mandate, role and activities, reminding them that it is separate from the RCMP.

This would encourage local police forces to deal with CSIS directly as well as with the RCMP in meeting terrorist threats.

In a similar vein, we recommended high priority for completion of the network of mutual cooperation agreements between CSIS and provinces (see page 17). None was in effect at the time of the airport security alert.

Perfect airport security at all times is not possible; there will always be ways to disrupt the peace that travellers in Canada generally enjoy. This makes it doubly important to ensure unreserved cooperation of the kind that the Solicitor General has moved to bring about between the RCMP and the Service.

Foreign Liaison Officers

Progress is being made outside the country, at Canadian missions where CSIS and the RCMP both have liaison officers. It has been agreed that CSIS now vets visa applications--as we believe it should under the letter and the spirit of section 14 of the *CSIS Act.*

It should be noted that CSIS and the RCMP have mutual assistance arrangements in posts where only one or the other has a liaison officer. This seems to work well.

Persona Non Grata

CSIS did make good use of its findings to identify foreign agents operating in Canada under the cloak of diplomatic immunity.

As a result of information it passed on to the Department of External Affairs, two members of foreign missions were declared *persona non grata* in 1986-87 and were sent home. Six more were voluntarily recalled home from Canada.

The Public Interest

Statutory rules govern disclosure to a minister other than the Solicitor General or, in specified circumstances, the Secretary of State for External Affairs or the Minister of National Defence, and disclosure to a public servant when it is "essential in the public interest and that interest clearly outweighs any invasion of privacy that could result" (paragraph 19(2)(d) of the *CSIS Act).*

The consent of the Solicitor General is required and, under subsection 19(3), the Director must make a report to us afterwards.

We received no reports on such disclosures in 1986-87.

Front Organizations

The *CSIS Act* does not contemplate disclosure to voluntary organizations or their members in case of infiltration by persons who may want to use them for purposes that could represent a threat to the security of Canada.

We raised this issue in last year's annual report, pointing out that loyal Canadians who belong to infiltrated groups or groups threatened with infiltration deserve to be alerted if some means can be found of communicating appropriate information.

Was there also some way, we asked, in which individuals who join a "front organizations" because they support its overt aims could be warned of its covert objectives?

Since then we have learned in CSIS briefings that hostile foreign intelligence services have, indeed, infiltrated some organizations and that substantial funding from foreign sources has been detected.

If CSIS were to publish such information, it would, in the process, reveal carefully guarded sources of information. It would be naive to suggest that those being watched do not know it. But publication of any detail could compromise surveillance.

---

* A definition we suggested was: "An outwardly independent organization whose promotion of idealistic, humanitarian and non-partisan political issues serves to obscure its covert objective of promoting public support for policies and initiatives of the organization or foreign power by which it is controlled". We added that "membership in a front organization should not be construed as knowledge of, agreement with, support of or adherence to the organizations objectives".

We do not have any easy answers to offer. As we did last year, we simply suggest that this is a problem Parliament might want to address when the time comes to review the *CSIS Act*.

A Vigilant Canadian. Meantime, we were heartened by one result of our reference to this matter last year.

After reading our annual report reference, a person deeply committed to a cause undertook to subject a front organization executive to vigorous and penetrating questioning. The executive finally tacitly acknowledged the real purpose of the organization, which had little to do with that cause.

Our reader promptly withdrew support and persuaded other, like-minded persons to do the same.

If we could count on equal vigilance on the part of all Canadians, we could abandon the search for a means through which members of front organizations and organizations subject to infiltration could be warned.

6. Counter-Subversion Operations

Counter-intelligence and counter-terrorism offer little room for disagreement. A given foreign nation either spies on us or it does not. No exception can be taken to counter-intelligence aimed at protecting our secrets from those that do.

Similarly, there is no place for terrorism in a country like ours with well-entrenched democratic means for gaining and using power. Any of us could be the innocent victim of a terrorist act. Clearly, those who would use violence to reach their political goals must be detected and stopped.

Counter-subversion is different. The right of peaceful dissent is the bedrock of democracy. Yet there are a few Canadians who proclaim their belief in the need for violent revolution. And even peaceful dissent may be secretly perverted by foreign powers whose goals are not the goals of most Canadians.

Grey Zones. At what point does dissent make an individual or an organization a legitimate target for the Counter-Subversion Branch of CSIS? How much talking about violence does it take to raise a real threat of violent acts? When does contact with foreign powers become detrimental to the interests of Canada?

Many such questions can be asked, and the answers turn up rich soil where honest disagreement can flourish. This is why we made counter-subversion the subject of our first branch-wide study of CSIS.

We are restricted in what we can say, of course. However, we can describe the research we undertook and set out some findings and recommendations.

Our criticisms of the system are not, we stress, directed at the men and women who carry out counter-subversion programs. We were impressed by the dedication and talent brought by both management and staff to their work and by the real difficulties they face in applying the *CSIS Act* in this grey zone.

Nonetheless, it is our duty to flag the concerns that our study gave us and to encourage CSIS to correct weaknesses in the system.

Principles and Law

As our standard, we adopted five basic principles from the McDonald Commission,* as follows:

- The "rule of law" is paramount.
- The means of investigation must be proportionate to the gravity of the threat and the probability of its realization.
- The need for given investigative techniques must be weighed against the damage they might do to personal freedom and privacy or to valued social institutions.

---

* *Freedom and Security under the Law*, the Second Report of the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (Ottawa, 1981), pages 513-514

- The more intrusive the technique, the higher the authority that must be required to approve its use.
- Except in emergencies, less intrusive techniques must be preferred to more intrusive techniques.

We were also guided, of course, by the *CSIS Act*, notably:

- The definition of "threats to the security of Canada" (section 2), in which Parliament was careful to exclude "lawful advocacy, protest or dissent". (The text of the definition can be consulted on page 21 of this report.)

- The requirement (section 12) that information be gathered only "to the extent that it is strictly necessary".

How We Proceeded

In our study, we examined policy and operational procedures to determine whether they met statutory requirements, and we discussed these procedures with senior CSIS managers.

We covered planning and accountability processes, the resources and investigative used in counter-subversion (compared with the resources and tools used by the Counter-Intelligence and Counter-Terrorism Branches), the number of paid sources, the amounts such sources are paid, targeting procedures, the number and nature of files opened on Canadians, and the amount of information disseminated to the Canadian and foreign governments about Canadians.

We also examined actual cases to see how policies and procedures are put into practice.

All of this was done against the background of McDonald Commission findings and an examination that we made of reform of the FBI (Federal Bureau of Investigations) in the United States in the mid-1970s. We met in Washington with officials of the FBI and with senior staff of the Permanent Select Committee of the House of Representatives on Intelligence and the Senate Select Committee on Intelligence.

Transition

We reviewed transitional activities--efforts to orient staff and to change policy and regulations in 1984, when the *CSIS Act* came into force and CSIS took over security and intelligence responsibilities from the RCMP Security Service.

More than two years after the switchover, the review of procedures remained incomplete. The Operational Manual was still outdated and even, at some points, contrary to the spirit of the *Act*.

This was disturbing, but CSIS is aware of the problem and is putting the manual through a drastic revision. We look forward to examining the new version as soon as possible.

We learned that all Security Service investigations reviewed in 1984 were continued by CSIS--although sometimes under justifications rewritten to ensure conformity with the new *CSIS Act.* Two investigations reviewed only at a later stage were dropped.

Resources

Counter-subversion gets a relatively small share of CSIS resources. Testifying before the Standing Committee of the House of Commons on Justice and Solicitor General last year* the Director set the figure at "under five per cent".

While we appreciate the basis on which the Director spoke, we think that "10 per cent, or slightly more, of operational resources" is a more realistic statement. Nonetheless, this is a relatively small proportion.

During our study, we found some frustration among CSIS investigators who felt that counter-subversion was the neglected step-sister of the CSIS family, with inadequate resources compared with counter-intelligence and counter-terrorism. Indeed, we found that counter-subversion sometimes seemed to be used as a personnel pool that could be drawn on to meet urgent needs in other operational branches. The Counter-Subversion Branch is taking steps to improve morale.

Human Sources

A separate Human Sources Branch serves all operational branches. It focusses mainly on paid sources. It seeks, for example, to ensure that they are reliable. It also has rules about what paid sources can and cannot be asked to do. But it does not do the same for regular unpaid sources.

There is no central control of "tasking"--that is, telling sources, both paid and unpaid, exactly what targets to monitor and what kind of information is wanted. Tasking is the responsibility of individual operational branches.

Targeting

The choice of primary targets for investigation is overseen by a Target Approval and Review Committee (TARC) composed of senior CSIS managers, advised by counsel. Like the Human Sources Branch, it serves all the operational branches.

---

* House of Commons, *Minutes of Proceedings and Evidence of the Standing Committee on Justice and Solicitor General,* December 11, 1986

TARC authorizes targeting for specified periods of time, so it deals with renewals as well as with new targets.

It makes its decisions after examining Subject Evaluation Reports (SERS) prepared by investigators.

Groups are targeted on the basis of section 2 of the *CSIS Act*. In counter-subversion, undue foreign influence and the potential for violence are the criteria most often used.

Individuals can also be targeted on the basis of section 2. But most individuals become targets automatically because of their relationship with a targeted group.

Not every subject who is targeted is actively investigated. The decision to investigate particular individuals is made by regional or branch managers based on the apparent threat, the information called for in CSIS's annual plan, and the availability of resources.

Some targeted individuals are investigated actively (a warrant may be sought to tap their telephones, for example) and some passively (in some cases amounting to no more than the accumulation of items about them from the press).

As anyone might guess, leaders of targeted groups are more likely to be watched closely than are rank-and-file members who, in turn, are more likely to be watched closely than are sympathizers who are not members. The term "leaders" includes influential mentors as well as people who hold office in the targeted group.

The categories of individual to be investigated because of their relationship with a targeted group are chosen by TARC.

But there is also another class of targets, composed of everyone in regular contact with a person already targeted for active investigation by TARC. These second-stage targets are identified in the field and do not come to TARC's attention at all.

For a number of reasons, we are concerned that the counter-subversion program casts its net too widely.

Targeting by Category. One way of looking at the TARC process is as we have described it above--that is, targeting entire categories of persons. Another is that individuals are targeted without reference to the actual threats, if any, that they personally pose to the security of Canada.

We find this insufficiently precise. Some groups under covert foreign influence, for example, may include only a few members who are aware of that influence. Even in groups with radical visions of the future, violence may be the preferred means for only a few members. It is not self-evident that all the officers of front groups would necessarily know these groups' covert agendas or undertake activities damaging to the security of Canada.

We think it would be more useful to explore means for warning such people of the organizations' real purposes (see page 30 of this report).

Our concern extends even more strongly to the people we have described above as secondstage targets--those identified merely because of repeated contact with a targeted individual.

Potential Harm. From what we have said about targeting by category, it follows that the present process takes insufficient account of potential harm to the principles of personal freedom and privacy.

Nor does the targeting process concern itself with the harm that can be done to valued social institutions if, for example, surveillance frightens members away from voluntary associations that would otherwise give them opportunities to promote legitimate causes and to devote their talents and resources to charitable purposes.

We urge that SERs always include a balanced discussion--pro and con--of the damage that investigation could do to individual freedoms and privacy and to the integrity of social institutions. The SERs that we saw were silent on these issues.

What Constitutes a Threat? Some of the threats described by CSIS are clear-cut; all loyal Canadians would agree that they deserve the Service's unremitting attention. But some left us perplexed.

One SER, for example, spoke of a certain organization's "attack on the anti-communist, pro-U.S. government of El Salvador ... in direct support of ... policy objectives to ... blunt American foreign policy initiatives". We cannot agree that a non-violent attack on U.S. foreign policy is necessarily a threat to the security of Canada.

On the other hand, there seems to have been minimal CSIS interest in fund-raising inside Canada for the Contra rebels in Nicaragua--although this seems to meet section 2's criterion of "activities within ... Canada ... in support of the ... use of acts of serious violence against persons or property for the purpose of achieving a political objective within ... a foreign state".

This contrast lends weight to our concern (see page 23 of this report) that CSIS may too readily accept the foreign policy objectives of our allies as its own and neglect Canadian foreign policy.

Magnitude of the Threats. CSIS seems to share our view that Canada faces minimal threats from many of the groups targeted by the Counter-Subversion Branch.

We recognize the real threats posed by a few. However, CSIS is expending money and effort on too many counter-subversion targets and it is intruding on the lives and activities of too many Canadians in this area.

Recommendations. We have already suggested that SERs always include a discussion of the harm that investigation could do to individual freedoms and privacy and to the integrity of social institutions.

In addition, TARC should reconsider its practice of targeting entire categories of people and examine the possibility of treating individuals as individuals. SERs would then have to document the need for investigation of individuals one by one.

We suggest that SERs also include explicit discussions of (a) the magnitude of the threat and (b) its imminence, (c) the need for the type of investigation envisioned compared with less intrusive alternatives and (d) the goals of investigation.

They should rely less on isolated incidents and more on a coherent argument for the targeting decision that TARC is asked to make.

In the same vein, we would also be more comfortable if greater efforts were made to ensure that all applications for warrants noted evidence that did not support the use of intrusive powers as well as evidence that did (see page 9 of this report).

CSIS should maintain a complete and up-to-date index of individuals subject to investigative authorization, instead of the partial index that exists now.

Files on Individuals

Files are opened on targeted individuals and organizations. We were unable to determine the precise number of riles opened as a result of counter-subversion operations as they are not segregated from counter-intelligence and counter-terrorism files.

According to the best information we have been able to obtain, the Counter-Subversion Branch probably has more than 30,000 files on individuals--how many more, no one knows. This is a matter of some concern to us. We don't know and we can't find out without a manual examination of thousands of files.

Only a small proportion of the people with files are under active investigation.

To further place the 30,000 figure in context, CSIS as a whole holds more than 600,000 files on individuals.

(It opened 112,000 such files in 1986-87. These include administrative files on, for example, the Service's own employees, as well as security assessment and immigration-related files, which turn over rapidly.)

Despite efforts in the early 1980s to purge files with little or no intelligence value, the number of files on individuals in the counter-subversion area seems to have remained relatively constant compared with the number held by CSIS's predecessor, the RCMP Security Service.

Old Files. Many of the files now held were opened when security intelligence was the responsibility of the RCMP Security Service, before there was a statutory definition of "threats to the security of Canada" (section 2 of the *CSIS Act)* or the "strictly necessary" rule (section 12) was laid down.

We have already made it clear in this report (page 21) that we think CSIS should review its files on individuals and remove information that does not meet the standards of sections 2 and 12.

We also suggest that detailed criteria be developed for opening files on individuals and groups and that the implementation of these criteria be reviewed periodically.

Dissemination of Information

When we asked CSIS how much information was provided to Canadian and foreign government agencies, we were told that the management information system could not readily identify such items. Each file shows what information went to whom. But there is no coding that lets aggregate figures be determined without a file-by-file search.

This gap could make it more difficult for us to meet our oversight duties for sections 17 and 19 of the *CSIS Act*, which deal with the exchange of information.

We urge that the management information system be programmed to allow easy access to aggregate statistics on information transmitted to and from Canadian and foreign government agencies.

Further, a specific policy and auditing procedure should be developed for the release of any information on a Canadian resident.

Five Organizations

We reviewed operational files on five organizations representing different categories of counter-subversion targets, to determine whether investigation of these groups was warranted under sections 2 and 12 of the *CSIS Act*.

We compared the files with the relevant SERs and warrant affidavits, and we discussed our impressions with CSIS experts.

In making our own assessment of the Service's investigative effort against each of these targets, we considered the requirements of the *Act*, the magnitude and imminence of the threat as we saw it, and the extent of the resources CSIS was devoting to it.

We concluded that the Counter-Subversion Branch is primarily concerned with two things:

- The potential ability of foreign powers to manipulate Canadian policy through social institutions or legitimate protest groups.
- The possibility that certain groups might undermine Canadian institutions and bring about the violent overthrow of the state.

In both cases, there appeared to be an underlying belief that the Canadian public was only too liable to be duped.

We think that the Counter-Subversion Branch over-estimates the influence and persuasive power of these groups. From our own reading of the media and our own personal knowledge of people in every walk of life, we know that Canadians are generally mature enough to resist the blandishments of the groups concerned.

Over-estimated. We also believe that CSIS over-estimates the likelihood of violence by some groups.

One targeted group, for example, publishes a magazine that deals with a wide range of topics--the arts as well as social policy and other issues--from the perspective of the far left.

It is true that some members have advocated violent action by this group, but they were brushed aside by the others.

A good case could be made that the partisans of violence in this group rate investigation as individuals.

But we remain to be convinced that the group itself should be targeted for investigation. It opens the door to unnecessary intrusion on the freedoms and privacy of the most innocuous as well as of the most obnoxious members. It also carries the risk of harm to freedom of speech, one of our fundamental social values.

Summing up, it is possible that any targeted group could undertake terrorist acts at some point, but most are not, on the available evidence, likely to do so in the foreseeable future.

Two Paths

There are two paths running through the grey zone in which the Counter-Subversion Branch operates, corresponding to its two major concerns--undue foreign influence and the risk of violence.

As it happens, these are the concerns of two sister branches, Counter-Intelligence and Counter-Terrorism respectively.

We recommend that these two paths be followed to their conclusion. The counter-subversion role should be split between the other two branches; Counter-Intelligence would deal with undue foreign influence, Counter-Terrorism with the risk of violence.

Priorities could be set more rationally, and some of the targeted groups we have cited here might appear more clearly in their real light.

And good intelligence officers who may now feel isolated and ill-appreciated in the counter-subversion role would find themselves in more active environments where their talents would get full rein.

7. CSIS Itself

To end our review of oversight findings, we return to one of the questions we posed in Chapter 2: Is CSIS efficient--in terms of both management goals like financial integrity and policy goals like civilianization and official bilingualism? As the subject of a special inquiry, official bilingualism will be dealt with in the next chapter. This chapter focusses on other internal matters.

Resources and Administration

The obligation to spend public money wisely must always be a high priority, and it is doubly strong in times of restraint like these. All arms of government, including CSIS, are squeezed for funds.

But CSIS also has special problems all its own. It still faces one-time costs associated with "transition" as it creates facilities and services that were once the responsibility of the RCMP. These start-up cost have sometimes proved higher than expected.

The Service has also been asked to undertake new tasks without giving up old ones and, in some cases, without getting extra money or staff. In this connection, we welcomed the Government's decision to allocate a significant amount in 1986-87 for enhancement of the counter-terrorism program. We hope care will continue to be taken that CSIS is not forced to spread itself too thin.

Accommodations. Restraint has obstructed CSIS's program for providing all its staff with offices separate from the RCMP's. One effect, ironically, is to increase the ultimate costs, at least in current dollars, because of persistent-if- relatively mild--inflation. Where CSIS has been unable to move out of RCMP accommodations on schedule, this may be an element in chilly mutual relations.

Following a report by the Auditor General on delays and cost overruns in renovating premises in Montreal, CSIS is developing a written accommodations policy and guidelines of its own to replace the RCMP policy and guidelines it had been using. It hardly needs to be said that we welcome this.

PEMS. In last year's annual report, we complained of weaknesses in the Service's PEMS (Policy and Expenditure Management System) documents.

CSIS has taken some positive steps since then. In last autumn's MYOP (Multi-Year Operational Plan), it used sub-elements that conform more closely to operational outputs (although some of them cannot be linked with distinct organizational entities, making it difficult to know who the responsible manager is). It is also attempting to show the marginal impact of security expenditures when it asks for funds.

On the other hand, we find that, though CSIS is fully meeting Treasury Board requirements, more recent MYOPs convey less information than earlier ones did.

For our own analysis, we wanted to know more, and CSIS has provided further information that has allowed us to examine spending as thoroughly as we did in previous years. We will make it a practice to ask for this information in future.

Civilianization

A major criticism of the RCMP Security Service was that it brought a police approach to security intelligence work.

The differences are important. As one study has noted, security work "offers few of the social and legal certainties" that the police can find in "the comparatively unambiguous objectives of prevention and apprehension".* We have already noted, for example, our own suspicions about the effect of the case-by-case police approach on the CSIS research effort (page 13).

The object of security intelligence work is not primarily to put miscreants behind bars. The core mandate is set out in the *CSIS Act* itself, which says (section 12) that the Service:

> shall collect ... and analyse 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.

The McDonald Commission, like the Mackenzie Commission a decade or so before, recommended the creation of a civilian security intelligence agency, separate from the RCMP. "Civilianization" became one of the policy objectives underlying the *CSIS Act* adopted by Parliament in 1984.

Dedicated Service. For many reasons, CSIS will continue for many years to show its police origins. Most significantly, the RCMP Security Service had the only large pool of trained personnel it could draw on.

No exception can be taken to the fact that many CSIS intelligence officers (IOs) come from the Security Service; civilianization is something to work for today and tomorrow, not a reflection on invaluable work being done by dedicated men and women who got their start in the Security Service. In addition, it made sense for CSIS to rely on some RCMP accommodations and services. It would be unrealistic to expect anything different.

Nonetheless, we see a real need to keep prodding CSIS along the civilianization path. Table 2, opposite, shows the distance to be travelled.

CSIS seems to see the figures as an effective response to those who say it is just the RCMP without the Musical Ride; fewer than half its employees were once uniformed members of the RCMP, it points out.

We look at it another way: More than 80 per cent of the people at CSIS brought the memories and habits of work of the RCMP with them. While we have not yet obtained

---

* Richard French and André Bé1iveau, *The RCMP and the Management of National Security* (Montreal, Institute for Research on Public Policy, 1979), page 4

exact figures from CSIS, there is not the slightest doubt that the proportion is even higher in the key 10 category and in middle management.

And this is after the "bridgeback" process was completed. In the two years ending July 16, 1986, former members of the RCMP had a right to return to the Force, and 75 did so--a relatively low proportion of those with bridgeback rights.

Table 2. Composition of All CSIS Staff

Former uniformed members of the RCMP	46%
Former civilian members of the RCMP	15%
Former public servants employed by the RCMP	21%
Not formerly employed by the RCMP	17%

(Source: as reported on December 3, 1986, by CSIS)

Who is Recruited

Recruitment from outside at all levels is the way to turn this situation around. We are seriously concerned by the reliance that CSIS has shown so far in its recruitment on "direct entries", as shown by Table 3.

Table 3. Sources of New IOs, January, 1985, to December, 1986

Public recruitment	51%
Direct entry (mainly from police forces)	34%
Conversions from within CSIS	15%

(Source: compiled from CSIS Figures)

Very nearly half the new IOs hired in 1985 and 1986 had police backgrounds. Direct entries are people with experience in police forces, the military and elsewhere, who are given IO status without going through basic training at the Service's own Sir William Stephenson Academy. The conversions are former surveillants who began their careers as RCMP "special constables".

The "not formerly employed by the RCMP" category in Table 2 includes some ex-policeofficers from other forces, as can be seen, along with some other pertinent detail, in Table 4.

Apart from the fact that, as a good employer, CSIS should continue to make room in the IO category for surveillants and other employees with the requisite qualities, we think that the emphasis in recruitment should be on factors other than police experience.

Collecting information is only part of the job. The kind of information CSIS deals with is only as good as the analysis that's done on it and the advice that the government gets as a result. The emphasis belongs on solid training in scholarly research and the social sciences.

Table 4. IO Recruits Exempt from Training at the Sir William Stephenson Academy, January, 1985, to December, 1986

Source	Sex		Mother Tongue		Entry Level	
	M	F	Fr	Eng	IO-2	IO-3
RCMP	33	6	6	33		39
DND	2			2		2
PCO	1			1		1
CEIC		1		1		1
Other Police	5		1	4	1	4
Total	41	7	7	41	1	47

(Source: CSIS)

We also found that the appointment of direct entries at the "journeyman" IO-3 level is a source of resentment to graduates of the Academy, who start work at the lower IO-1 level (see page 45).

Time Out at the Academy

For a few short weeks, we felt reassured by the Service's written statements, in response to one of our formal queries, that it did not expect further direct entries at the IO-2 and IO-3 levels and that all new IOs--except some who are already on the payroll in other jobs--would go through the Academy.

But we were subsequently stunned to learn that CSIS had hired 16 former police officers in the last quarter of 1986 and left no positions open for new recruits from the universities or civilian employment.

As a result, the Academy has been closed down for a year, and further civilianization of the Service has stalled.

We understand that plans are being formulated to re-open the Academy in 1988. We strongly recommend that greater attention be given to civilianization and that, to that end, no direct entries be taken from police forces so a new class of civilian recruits can be made up as soon as possible.

Bilingualism and Equitable Participation

The 1987-88 class was to be the one in which, for the first time--CSIS management had solemnly decided some months ago--every member would be bilingual, as we have recommended.

It also offered the Service an opportunity to act on our repeated recommendations that it take steps to increase the representation of women and Francophones to levels closer to their representation in the labour pool.

Table 5 clearly shows why these recommendations need to be repeated and why the loss of the 1987-88 class will be so deeply felt.

Table 5. Selected Characteristics of CSIS Recruits in the First Three Classes at the Sir William Stephenson Academy (Percentages)

	January 1986	June 1986	February 1987
Bilingual (English-French)*	9	10	10
Women	25	20	10
First Official Language French	3	10	10

(Source: CSIS)

* CSIS reported that a further third of the first class, the entire remainder of the second class, and nearly a third of the latest class were composed of Anglophones with "some French".

The First Class

In our last annual report, we discussed our report entitled *Eighteen Months After: The Canadian Security Intelligence Service Recruitment, Training and Development Programs.* In the course of the research, we interviewed the first civilian recruits, who were then training at the Academy. We found that they generally had positive impressions of the training program.

Following up in 1986-87, we arranged new interviews with nearly half of the graduates of the first class. Except as noted below, morale remained high.

Overall, members of the first class enjoyed their work, found it challenging, and said they were pleased with their duties and ongoing development. On a scale of five, they gave an average rating of four to their feelings about CSIS. Most indicated that they expected to make a career within CSIS and rated their career opportunities as four on a scale of five.

Direct Entry. The one sour note, expressed by almost all those we interviewed, was that preferential treatment had been given to direct entries--that is, intelligence officers who have been recruited directly into CSIS because they have previous police experience.

The direct entry recruits are not required to take the introductory course at the Academy and they are generally hired at the IO-3 level (see Table 4 above), while civilian recruits are hired at the lower IO-1 level.

This represents a pay difference of about $10,000 a year, although the duties of an IO-3 and an IO-1 are broadly the same. The difference in level is based on the supposition that IO-3s are seasoned veterans who can be relied on to work more on their own and even to help IO- 1s along.

This is frustrating to the 10-Is--so much so that we had some concern that valuable people might resign because they felt their career aspirations were blighted in this way from the start.

At another level, the advantage given to direct entries seems to perpetuate the domination of the Service by people who developed their corporate culture in police organizations.

These are both reasons to welcome new arrangements that will let superior IO-1s (usually civilian graduates of the Academy) reach the first level of management (IO-4) in as little as seven years--not the 11 years originally projected. But this is still much longer than the two years in which an IO-3 (ex-police direct entries) can hope to become an IO-4.

Training. Looking back from the vantage point of day-to-day work, the first class had varying comments on the training they got at the Academy. Overall, the basic suggestion was that training should concentrate more on everyday needs like source-handling, interviewing and report-writing.

Building Morale

We see value in a public relations campaign designed to foster an appreciation among Canadians of CSIS and its role. We think this could have a significant effect on morale, giving CSIS employees a positive corporate image to back up their own sense of personal contribution to the security of Canada.

A strong and positive image for CSIS could also overcome any gap between the corporate culture of ex-police-officers and that of employees who got their first taste of security intelligence work in the more civilian atmosphere of CSIS itself.

Polygraph Examinations

Another issue related to recruitment is the use of polygraph examinations. Despite one scrap of good news, we are disappointed with inaction at both CSIS and the Ministry of the Solicitor General on this issue.

In our last annual report, we set out in detail our grave doubts about the Service's use of the polygraph (popularly, though incorrectly, known as the "lie detector") in screening potential employees and in testing the loyalty of serving employees.

Testifying before the Standing Committee of the House of Commons on Justice and Solicitor General,* the Director said he was not satisfied that the opinion expressed by us and others was "sufficiently strong at this stage to warrant not proceeding with that particular investigative tool". He noted in particular that the polygraph examination is only one of 21 steps in the recruitment process and that any concerns raised by this test are pursued by investigation afterwards.

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

False Appearance. We think we met that argument last year when we said we could not believe that CSIS policy against making polygraph examinations the sole determinant of security clearances and employment could be made to stick. Because of their false appearance of scientific rigour, the results of polygraph examinations would more often than not be accepted at face value. There would be a strong temptation to discount a contrary result from investigation, because it was subject to "human fallibility".

Highlighting other arguments we made last year:

- There are no generally accepted scientific studies that establish the validity of polygraph examinations in mass employment and security screening (although we recognize that there may be a place for the polygraph as one of many tools in a criminal investigation).

- Even the defenders of polygraph examinations admit that the results are sometimes wrong-10 per cent of the time or more. Anyone who made spelling mistakes at that rate would be unemployable in a job that called for much writing, yet polygraph readings with less than 90 per cent reliability are wrapped in the cloak of "science" and can cost Canadians their careers and savage their reputations. Indeed, because of errors, polygraph examinations cannot even be defended as an airtight bulwark against penetration of the Service by disloyal and dishonest people.

- While polygraph examinations for serving members of CSIS were not mandatory, we did not believe they could be truly voluntary, as the Service claimed. Anyone who showed reluctance to be examined would inevitably be suspected of having something to hide, so the pressure to take a polygraph examination would be irresistible for all but the hardiest souls.

- Finally, we were concerned that as polygraph examinations became routine within CSIS, their use would spread throughout the government, bringing in their wake fear and mistrust--shabby values to encourage in a country like ours.

The good news since then is that CSIS has suspended its "voluntary" testing of employees already on the job. This disposes of one of the objections we made in our last annual report.

---

* House of Commons, *Minutes of Proceedings and Evidence of the Standing Committee on Justice and Solicitor General*, December 11, 1986

But the rest of our doubts remain unanswered by either CSIS or the Ministry of the Solicitor General.

A Disguise. New recruits were still put through polygraph examinations, covering both lifestyle and loyalty, as a condition of employment. CSIS tried to dress its program up in a lab coat by calling it a pilot project, but this is merely a disguise.

The term "pilot project" suggests a trial run, carefully planned and equally carefully evaluated. This program has neither terms of reference nor evaluation methodology developed in advance of testing. In short, there is no "pilot project"--just the same old polygraph examinations continuing as usual under a new label.

Meanwhile, the issue has not been actively pursued by the Ministry of the Solicitor General.

Ministry staff told us they were awaiting the results of two studies taking place in other countries. Interested in these studies ourselves, we made inquiries and found that one had. been cancelled and the second had been completed without yielding any useful results. We brought the Ministry up to date on these developments.

The Ministry, following the advice of an interdepartmental committee, contented itself with getting a legal opinion, which held that polygraph examinations could be considered a legal condition of employment.

Essential Flaw. This did little to resolve the issue of the essential flaw of polygraph examinations--their lack of reliability and the injustices that can flow from errors in reading their results.

We have heard reports that CSIS may be under some pressure from friendly security and intelligence agencies abroad to use polygraph examinations in security screening. We believe that these pressures should be resisted in the absence of conclusive evidence that polygraph examinations are more reliable than generally believed.

Indeed, we believe that well-designed, rigorous employment and security screening investigations would make the use of the polygraph superfluous in any case.

And we once again urge, as we did in our last annual report, that the use of polygraph examinations for employment and security screening be stopped and that a thorough and objective study be carried out so the Solicitor General and the Government can decide for themselves whether such methods are compatible with the values of our free and democratic society.

8. Closing the Gaps

Like civilianization, discussed in the last chapter, official bilingualism is a major policy goal for all federal agencies--and especially for CSIS, which has a lot of ground to make up.

At the request of the Solicitor General, we conducted an extensive inquiry in 1986-87 into official bilingualism and staff relations in CSIS, focussing on the Quebec Region, the Ottawa Region and Headquarters, where tensions seemed to be highest.

Culture and Communications. Our report, submitted to the Solicitor General in March, 1987, highlights gaps in culture and communications and makes a total of 48 detailed recommendations for bridging them. CSIS management has undertaken to make a conscious and sustained effort to close these gaps. To provide an overall framework, we recommended that:

- A Deputy Director, Special Projects, be appointed for a two-year period to oversee implementation of a special official languages plan and of our recommendations for better staff relations.
- A consultative committee of experts--from Treasury Board, the Department of the Secretary of State and the private sector, perhaps--be created to assist in implementing the official languages plan.

We prepared an abridgement of the report to permit broad distribution. We are now informed that it will be made public.* As we say in our preface to the abridgement: "We hope this signals the Service's determination to lay the ghosts of past problems and get on with the tasks of giving both official languages their due and opening up channels of communications in staff relations".

We will continue to follow the official languages and staff relations issues closely.

In this chapter, we review some of our most important findings and list other major recommendations.

Official Languages

We found in our special study that, despite good intentions at the top, there had not been enough real commitment among some key players to the government's official languages policies and not enough understanding of the Francophone culture that shapes the thinking of one in four Canadians.

CSIS was taking steps to improve the situation. During our inquiry it:

- Lifted a moratorium on language training and on the usual obligation that a unilingual government employee faces to learn the second language within two years of appointment to a bilingual position.
- Hired a Chief, Official Languages, who immediately went to work drafting key policies.

---

* *Closing the Gaps: Official Languages and Staff Relations in the Canadian Security Intelligence Service* (Ottawa, 1987)

We welcome these initiatives. But our optimism is clouded by lapses that continue to take place.

Indeed, it has since become difficult to resist a tinge of cynicism as a result of a mismatched pair of decisions about the Sir William Stephenson Academy, where training is provided to new intelligence officers.

During our inquiry, management decided that henceforth all recruits admitted to the Academy would have to be bilingual and courses would be given in both official languages. Later (see page 44 of this annual report), it undermined its credibility by suspending classes at the Academy for a year.

One lapse during the inquiry itself was the publication of a Directive Writers' Guide in English only--despite the basic principle that employees whose working language is French are entitled to the same assistance in carrying out their duties as those whose working language is English.

Culture gap. This is a small but telling example of what we meant by the "culture gap"--the expectation some Anglophones seem to have that Francophone needs can be dealt with as an afterthought. We want to make it clear that this approach was not universal, but we caught whiffs of it far too often for our liking.

Complaints about messages to the Quebec Region in English only or in English first with a French translation later, sometimes much later, were among the issues that led to our inquiry. Yet such messages remained a problem at least as late as October, 1986--seven months after our inquiry began.

English-only messages from Headquarters clearly contravened government-wide official languages policy. Officially designated a bilingual office with French as its primary working language, the Quebec Region is entitled to get communications from Headquarters either in English and French simultaneously or in French alone.

Spirit of Bilingualism. Frequent English-only messages from one Ottawa Region unit to the Quebec Region were, strictly speaking, admissible under official languages policies Designated a bilingual office itself, Ottawa Region is entitled to communicate with all other CSIS offices in either or both official languages.

However, we consider that this particular unit is in a special position because it provides a national service to all branches of CSIS, coast to coast, and the spirit of official bilingualism calls for more than the strict minimum.

We were often confronted with the "urgency" argument--that translation into French would impose unacceptable delays. We found that there was usually less to this argument than met the eye. In many cases, for example, material in a foreign language was translated into English; why could it not be translated into French at the same time?

Other Issues. Among other issues were a very modest level of bilingualism required in some Headquarters positions, the advertisement of positions before the language requirements had been approved by the Chief, Official Languages, and failure to consider

equitable representation in the selection of the first class at the Sir William Stephenson Academy with the result that only one recruit was Francophone ("We goofed", one highly-placed source admitted to us).

Anglophone Concerns. At the same time, we noted concerns among unilingual Anglophone employees that strict adherence to the government's language policies could stall their careers.

We believe that stepped-up language training is the way to make it clear that there is equal opportunity in CSIS for all qualified people, regardless--to borrow the wording of the *Canadian Charter of Rights and Freedoms*--of race or national or ethnic origin.

Recommendations. Among our major recommendations for dealing with official languages issues were that:

- A special, two-year official languages plan be implemented to make up for lost time.
- CSIS give priority to expanding its facilities for translation into French so that operational efficiency ("urgency") could no longer be offered as an excuse for English unilingualism in written communications.
- As a matter of policy, the Ottawa Region unit mentioned above communicate in French with French-language offices and bilingual offices where French is officially designated as the primary working language.
- A French-language equivalent to the Directive Writers' Guide and any other guides or manuals now available in English only be published in 1987.
- Steps be taken to ensure that management positions are designated bilingual on the same basis as this is done throughout the government and that no job competition be held until the Chief, Official Languages has established official languages requirements for the position concerned.
- Language training be scheduled by the end of the Special Plan for all unilingual employees in bilingual positions and that CSIS officially decide by July 31, 1987, how it will deal with unilingual employees in bilingual positions who (a) are not eligible for second-language training, (b) refuse or fail to enrol in such training, (c) fail such training or (d) lose their ability to work in the second language.
- Continued emphasis be placed on bilingualism as a recruitment criterion and that CSIS structure its hiring and staffing procedures to ensure adequate Francophone recruitment.
- The bilingualism bonus be paid in accordance with Treasury Board rules.

Haig-Brown. Because there have been reports in the media on the so-called Haig-Brown Report, it may be worth briefly saying what we found in the course of our inquiry.

This report, a collection of memoranda by two Army officers seconded to the RCMP during the Second World War to advise on the organization of personnel selection, perpetuated unacceptable stereotypes about certain ethnic groups.

We were not entirely convinced by protests that the Haig-Brown Report was irrelevant in its day, but, in the final analysis, we agreed that its present interest is historical; there is no evidence that it ever guided personnel selection in CSIS.

OCOL. We should also say for the record that we conducted our inquiry in cooperation with the Office of the Commissioner of Official Languages (OCOL), which was simultaneously engaged in its own audit of official languages practices at CSIS. OCOL was issuing its own report.

Staff Relations

We found that real problems in staff relations had been amplified by a communications gap in which management and some employees came to suspect the worst of each other.

The problems and the communications gap could both be traced in part to transition, as CSIS took shape out of the former RCMP Security Service. CSIS managers themselves acknowledge that in the hectic early days, many decisions were founded more on intuition and experience than on planning or policy. It is hardly surprising that such decisions sometimes seemed arbitrary and lent credibility to whispering about discrimination and favouritism.

Another factor was nostalgia for the RCMP. Managers who learned their craft in the hierarchical RCMP tended to expect swift and silent obedience, not questions about their decisions.

Finally, there was the value attached to the need-to-know principle in any security and intelligence agency. This principle is, of course, essential in security matters. But it should not spill over into routine administrative matters. CSIS had not made known, for example, its policy governing transfers.

Personnel Manual. As in official languages, CSIS was taking steps to deal with its staff relations problems. We were especially reassured to find that it was preparing a formal Personnel Administration Manual. By clarifying the rules, this Manual can prevent much misunderstanding and suspicion.

CSIS is also proposing that the Public Service Staff Relations Board (PSSRB) be empowered to adjudicate grievances by non-unionized employees like intelligence officers, surveillants and analysts. At present the Director makes the final decision on these grievances which places him in the awkward position of being both judge and party.

Our only concern is to ensure that the amendment sought to the *Public Service Staff Relations Act* actually does give the PSSRB an adequate mandate to deal with CSIS grievances.

Conversion. One of the major controversies that led to our inquiry had to do with "conversion", when surveillants (former "special constables" in the RCMP, the people who tail targets) were given an opportunity to compete for positions as intelligence officers (IOs).

This was an opportunity of great significance to the surveillants. Their jobs lead nowhere; the reward for diligent and skillful surveillance is the chance to do more surveillance. An IO, on the other hand, is on the first rung of the career ladder that leads to the director's office.

Communications problems, unfortunately, turned conversion into a battlefield. In the first place, surveillants interviewed in the course of our inquiry believed that the distinction between them and IOs would be completely erased; all would be on the same career path. At least some surveillants in Montreal believed that they were being offered absolute priority to try for IO positions before any outsiders were considered.

Both these hopes were dashed. CSIS management interprets the promises it made much more narrowly. It believes that it kept its promise by letting the surveillants apply for jobs as IOs without holding university degrees (which few surveillants have) or going through basic training at the Sir William Stephenson Academy.

Mobility Agreement. The Montreal surveillants also believed that a mobility agreement presented to them as a condition of conversion was an attempt to frighten them off. This agreement raised the possibility of transfer, and the surveillants lived up to the conventional wisdom that Francophone Montrealers in all fields prefer to make their careers in Montreal.

In a serious departure from good official languages practice, CSIS first offered psychological testing in English only, then made those who insisted on French tests wait for six months. Only the "culture gap" we referred to under the official languages heading above can explain this kind of unequal treatment of Francophone and Anglophone candidates for conversion and failure to anticipate the reaction.

Then came the announcement of a second conversion competition before the first one was completed in Montreal. The Montreal surveillants were apparently not told that the first competition was over in the rest of the country, and they were quick to conclude--understandably if, as best we could determine, wrongly--that this was a dirty trick of some kind.

Other Problems. Our findings on the grievance procedure are obvious from what we have already said and from the recommendations described below.

We also found that the prospect of ill-explained lateral transfers was a serious source of insecurity among employees, that there was a widespread belief that competitions for promotions concealed rather than prevented favouritism, and that CSIS employees (who are not, legally speaking, public servants) feel trapped because they cannot enter internal competitions for Public Service jobs.

Recommendations. Among our major recommendations for dealing with staff relations issues were that:

- The *Public Service Staff Relations Act* be amended in such a way that grievances by non-unionized CSIS employees can be adjudicated by a member of the Public Service Staff Relations Board with suitable security clearance.

- Since non-unionized employees do not have a collective agreement, they be allowed to grieve on the basis of the Personnel Administration Manual.

- The Director's reply to a grievance always include reasons for the decision.

- Arrangements be made for paycheque deductions to provide the Association of CSIS Employees with funds to pay the costs of adjudication if the Association decided to accept a role in such proceedings. The amount of the checkoff would be determined by a majority vote of Association members.

- CSIS issue a policy statement describing career paths open to its employees, especially those outside the IO category, and setting out the rules for conversion from one path to another.

- CSIS issue a policy statement specifying the conditions under which lateral transfers will be made.

- In staffing, selection boards be composed of the supervisor to whom the position reports, a supervisor of equal rank from another branch of the Service and an officer, with appropriate security clearance, of the Public Service Commission.

- CSIS explore avenues for permitting its employees to compete for Public Service jobs.

9. Complaints

Citizenship and immigration cases gave us most of our work on complaints in 1986-87.

This was not merely a matter of numbers. Compared with security clearance cases, those dealing with citizenship and immigration are complex and difficult, usually involving large numbers of reports and documents accumulated over many years. And the stakes are high. An adverse report by us could well result in the Governor in Council's deciding to deny citizenship or direct the commencement of deportation proceedings.

Meanwhile, the number of new complaints about security clearances plunged.

Kudos for Defence

New screening procedures at the Department of National Defence (DND) appear to go a long way to explaining the drop in security clearance complaints.

In our last annual report, we objected in strong terms to the way DND had carried out clearance investigations.

We are pleased this year to say publicly what we have already said privately--that DND showed some real sensitivity to individual dignity by radically revising its security clearance procedures.

Of the 44 people whose cases we asked DND to reconsider in 1986, fully 39 were granted clearances. The other five withdrew their complaints on promises that their cases would be re-examined at a later date.

New complaints against DND in 1986-87 totalled zero. We hope that this Department maintains the high standard it has set for itself. As insurance, we have asked it to tell us every year how many security clearances it has denied. If the number is high, yet complaints are low, we will ask why.

Security Clearances

The number of new complaints arising out of security clearances denied by other departments also shrank; there was only one in 1986-87, compared with 14 the year before.

We like to think that this reflects greater care being taken as the people responsible for security--in departments and agencies as well as in CSIS--learn about the complaints process and the criteria that are taking shape as we deal with specific cases.

A new security classification and screening system was introduced by the Government in 1986. It does not come directly under our oversight mandate. But it is an important element in complaints that we hear as well as in CSIS's workload, so we say something about it later in this chapter.

Mandates. Under the *CSIS Act* (section 42), a complaint can be made to us by:

- A person refused federal employment solely because a security clearance has been denied.

- A federal employee who is dismissed, demoted or transferred or denied a promotion or transfer for the same reason.

- Anyone refused a contract to supply goods and services to the government for the same reason.

The Department of National Defence carries out its own security screening.* In other departments and agencies, decisions to grant or withhold clearances are made by the deputy head after a security assessment is submitted by CSIS.

Anyone denied a clearance must be notified and told that a formal complaint can be lodged with us. After investigation and *in camera* hearings by one or more members of our Committee, we report our findings and any recommendations to the Solicitor General, the Director of CSIS, the deputy head concerned and the complainant.

Investigations and Recommendations. This year, hearings have been completed and recommendations made in two cases. In one we recommended that clearance be granted, and this was done. In the other we supported CSIS's recommendation against clearance. Summary case histories can be found in Appendix B. One complaint of this kind was still under investigation at year-end.

Complaints against CSIS

Mandate. The *CSIS Act* directs us to investigate complaints about "any act or thing done by the Service" (section 41).

There are two principal limitations. A complaint must first be made to the Director of CSIS. We can then accept the complaint if the Director has not responded within a period that we consider reasonable or if the complainant is not satisfied with the Director's response.

Second, we may not investigate a complaint that can be channeled through another grievance procedure under the *CSIS Act* or the *Public Service Staff Relations Act.*

Complaints by Employees. Both we and the Commissioner of Official Languages received 1,776 complaints in 1986-87 about the Service's official languages practices, all from CSIS employees. This is about three times the number of language complaints in the previous year.

We held these complaints in abeyance while the Office of the Commissioner made a detailed audit of official bilingualism in the Service and while we conducted the inquiry reviewed in Chapter 8.

Complaints from the Public. We had 13 complaints from members of the public, pared with four in the previous year. Twelve, mostly from disappointed candidates for

---

* So does the RCMP.

employment by CSIS, were outside our jurisdiction and one was under investigation at year-end.

Immigration and Citizenship

We had 13 citizenship cases and one immigration case on hand as 1986-87 began. Five more immigration cases came to us during the year, but there were no new citizenship cases.*

Mandates. Under the *Citizenship Act*, the Secretary of State reports to us when he is of the opinion that citizenship should be denied because there are reasonable grounds to believe that the applicant is either a threat to the security of Canada or is involved in organized crime.

Similarly under the *Immigration Act, 1976,* a report is made to us when the Minister of Employment and Immigration and the Solicitor General believe that the applicant for admission to Canada will engage in activities inimical to Canada's interests in various specified ways.

in both cases, the subject of the report must be notified. We investigate as we would in the case of a complaint by an individual and make recommendations to the Governor in Council.

Investigations and Recommendations. One immigration case was disposed of. We agreed that admission to Canada should be denied. Investigation was continuing on four immigration cases and a fifth was being reopened by consent of all parties.

Six citizenship cases were closed. In two, we recommended that citizenship be granted. One citizenship case ended when the applicant died. In addition, CSIS withdrew its objections in three citizenship cases during investigation. Summary case histories of citizenship and immigration cases can also be found in Appendix B.

One report on a citizenship case was being prepared at year-end, and investigation was continuing in six cases.

The first case involving the criminality provisions of the *Immigration Act, 1976,* came to us at the close of the year. There was reason to expect more early in 1987-88.

Quality of Investigations

We have already dealt with the striking improvement in the quality of investigations by the Department of National Defence.

---

* Readers who enjoy statistical analysis may want to know that: (a) one of the immigration cases and one of the citizenship cases involve the same person, and (b) one of the new immigration cases is identical with one of the immigration cases carried over from the previous year; it is being re-opened with the consent of all parties.

CSIS Security Assessments. Over the last three years, we have seen many security screening reports prepared by CSIS for other departments and agencies, and, for the most part, they were well done.

However, in the cases we saw this year, some conclusions were inferred from insufficient evidence and what could have been perfectly innocent activities were sometimes viewed in the worst possible light without adequate reason. Case reports highlighted these weaknesses.

Immigration and Citizenship. We were especially disappointed in the quality of CSIS reports and of the evidence it presented to us in citizenship and immigration cases.

For example, the Service sometimes took weeks to respond to straightforward questions that we posed during the preliminary investigation, and it sometimes came to hearings with evidence that had not been seen by the minister or ministers to whom the initial recommendation had been made.

Neither the delays nor the after-the-fact accumulation of evidence speaks well of the care taken with recommendations on which the rest of a person's life may depend.

Special Report. We have made a special report to the Solicitor General, under section 54 of the *CSIS Act,* to share with him our concerns about both security assessments and the handling of citizenship and immigration cases by CSIS.

A special report was necessary because CSIS does not accept our concerns. In fact, CSIS seems to blame the process required under the Act--or our interpretation of the process.

To bring about better controls, we recommended that:

- The Director (or, in his absence, a deputy director) of CSIS personally have sole authority to recommend that, for security reasons, citizenship be denied, a potential immigrant or visitor be refused entry or a permanent resident be deported.

- These recommendations be made to the Solicitor General who, if he agreed, would then, in citizenship matters, authorize the report being forwarded to the Secretary of State or, in immigration cases, would forward the report himself, with his own comments, to the Minister of Employment and Immigration.

- Similarly, the Commissioner of the RCMP (or, in his absence, the Deputy Commissioner) personally be the only one with authority to make recommendations to do Solicitor General regarding deportation under the criminality provisions of the *Immigration Act, 1976.*

- Only the Director of CSIS (or, in his absence, a deputy director) have the authority to recommend that a security clearance be denied to a Canadian seeking federal government employment.

We look forward to discussing this issue in detail with CSIS, and we hope next year to report that more effective procedures have been developed for maintaining the delicate balance between protection of the security of Canada and protection of individual rights.

Immigration Act Study

In a report on June 17, 1986, the Standing Committee of the House of Commons on Labour, Employment and Immigration made two recommendations regarding security screening, as follows:

> 32. The Solicitor General should ask the Security Intelligence Review Committee to investigate and report on whether Canada's *Immigration Act* is adequately protecting Canada and any recommended legislative changes should be introduced to Parliament as soon as possible.
>
> 34. The Solicitor General should ask the Security Intelligence Review Committee to review the criminality provisions of the *Immigration Act.*

On September 26, 1986, the Solicitor General officially asked us to investigate and report on the effectiveness of the relevant provisions of the *CSIS Act.* Under Section 40 of this *Act,* we have asked the Inspector General to undertake some fact-finding for us. Our work on this was continuing at year-end.

We have also been invited to take part in the Interdepartmental Working Group formed by the Minister of State (Immigration) to develop the Government's response to the Standing Committee's report. We are represented by the Executive Secretary.

In neither of these activities do we play an executive role. But our experience with immigration and the virtually identical citizenship cases has given us a particular perspective that we feel should be put at the Government's disposal as it considers amendments to the *Immigration Act, 1976.*

We regard it as preventive action. Better to offer our advice now in hopes of warding off problems than waiting for problems to emerge and then carping from the sidelines.

The New Security Policy

On June 18, 1986, the then Solicitor General introduced a new security policy and operational guidelines for classifying information and screening personnel.

The previous policy had its origins in a 1956 PCO document called Security of Information in the Public Service of Canada, supplemented by Cabinet Document (CD) 35, which dates from 1963. It is generally recognized that too much information was being classified and security clearances were being sought for too many people under these arrangements.

Costs are a factor in limiting the scope of security policy. The average cost of a Top Secret clearance has been reported as $1,425 and of Confidential and Secret clearances as $13.62--figures that we believe are, if anything, serious underestimates, as we explained in last year's annual report.

Speeding up the screening process for individuals by reducing the demand was another reason for reform. As matters stood, CSIS was snowed under by a growing backlog of clearance investigations in progress. This situation, too, we described in last year's annual report.

Demand. The new measures were to bring about a reduction in the demand for security clearances by requiring that requests be justifiable, equitable and effective. It established as objectives that:

- Only information whose protection from unauthorized disclosure is essential to the national interest be classified.

- Departments and agencies reduce the number of positions that require employee to be security cleared.

- The rights of individuals affected by the government's administrative security system be improved.

- The security of Canada be upgraded by more effective management of the resources dedicated to the security screening and information classification and protection programs.

Under the new policy, information is to be classified only if it falls into one of six categories--national defence, international affairs, national security (including hostile and subversive activities and threats to the security of Canada), Cabinet confidences, federal-provincial affairs, and selected economic interests of Canada.

Deputy heads are held accountable for security in their departments and agencies. Among other things, they identify employees who need security clearance and ensure that, as a condition of employment, these employees are screened.

Except, as explained above, in the case of DND and the RCMP, a "security assessment" is provided by CSIS. But the ultimate decision to grant or withhold clearance lies with the deputy head.

Rejection Criteria. Under the new policy, no one can be refused security clearance for disloyalty unless there are reasonable grounds to believe that he or she engages in or may engage in activities that fall within the definition of "threats to the security of Canada" in the *CSIS Act* (section 2).

Under CD 35, a person could be rejected for "unreliability", not merely for outright disloyalty. This remains true, but there must be reasonable grounds to believe that the individual may disclose (through careless talk, for example) or may be induced to disclose (under the threat of blackmail, for example), or may cause to be disclosed (through habitual carelessness, for example) classified information.

Treasury Board, which is responsible for the overall management of the new policies, is assisting each department with implementation of the program and monitoring compliance with the new policy.

On September 12, 1986, the Solicitor General issued a formal directive to CSIS governing the provision of security assessments.

Redress. Announcing the new security policy, the then Solicitor General reaffirmed that the Government was committed to a fair and equitable review procedure for those denied security clearances. He said:

> Members will know that the SIRC is made up of five Privy Councillors representing all three parties in the House. It has an independent mandate to review all complaints concerning security clearances requested by the government, with full authority to require the production of evidence and witnesses from the Service and the department that has denied the security clearance.
>
> The SIRC has demonstrated its value as a review mechanism by the careful, thorough and fair manner in which it has investigated and reported upon those cases which have so far come before it and the way in which it has brought the principles of natural justice into play in these cases.*

Impact on CSIS. We have not conducted a full review of the new security policy's impact on CSIS. However, we are mindful of three elements that will add to its workload, as follows:

- CSIS will establish and maintain a central index for all security clearances.
- For criminal records and credit checks, it will be the sole entry point for all agencies except DND and the RCMP on security screening.
- As a pilot project, personal interviews are to be conducted with persons requiring Secret clearance, whereas interviews were previously conducted only for cause. Personal interviews are now always required for Top Secret clearance.

No Let-Up. Six months after the announcement of the new policy, our research showed no let-up in requests for security assessments. As a matter of fact, while requests for field investigations--more or less synonymous with requests for Top Secret clearances--were down, total numbers increased after the new policy was in place. Table 6 sets out the figures for the last six months of 1985 and of 1986.

Table 6. Requests for Security Assessments

	security clearance requests	field investigation requests
second half, 1985	31,797	2,005
second half, 1986	35,061	1,425

(Source: CSIS)

* *House of Commons Debates*, June 18, 1986

These numbers include all three levels of clearance--Confidential, Secret and Top Secret.

The Solicitor General has taken a number of steps to deal with this situation.

At a mundane but practical level, he directed the Security Screening Branch at CSIS to get the temporary secretarial help it needs to clear the backlog of about a thousand cases that had been wrapped up by the investigators but remained piled up in the typing pool In basket.

He also directed the Service in December, 1986, to send outstanding requests back to the departments for reconsideration under the new policy.

Finally, he asked the Intelligence and Security Co-ordinator at the Privy Council Office to speak personally with deputy heads in departments that may be asking for Top Secret clearances that cannot be justified under the new policy.

10. Tidying Up

Our work in oversight and complaints is no mystery to readers of the foregoing chapters. But some of our activities do not fit under either of these rubrics. We describe them here.

Answering to Parliament

We appeared twice in 1986 before the Standing Committee of the House of Commons on Justice and Solicitor General--on June 3 to answer questions on our 1984-85 annual report and on November 20 to answer questions on our 1985-86 annual report. Issues raised with us on those occasions have been dealt with in this report.

As the year under review ended, we looked forward to an appearance before the Special Senate Committee on Terrorism and the Public Safety on April 3, 1987.

Outreach

As part of our accountability to Parliament, we see ourselves as accountable to Canadians at large.

Accepting a responsibility to foster public knowledge and awareness of security and intelligence matters, we are as forthright as security considerations let us be with the hundreds of individuals who ask us about security clearance procedures and about specific incidents or general issues.

Mass Media. We are as open as possible with the mass media. After our second Annual Report was tabled in Parliament in June, 1986, we held a news conference, and our Chairman, the Honourable Ronald G. Atkey, as well as other members and staff have been interviewed many times over the year. We believe that in a healthy democracy there can and should be a degree of informed public discussion on national security issues.

There are also occasions when it would be inappropriate for CSIS to make issues public but it is appropriate for us to do so. On such occasions we are able to put matters in perspective, to the benefit of all concerned.

Meetings and Conferences

Academic researchers and students also interview the Chairman and staff. We keep our lines open to academic and professional specialists in security intelligence, not only out of a duty to share our own insights widely but for what we can learn from them.

In the past year, the Chairman:

- Was a panelist at the National Forum on Access to Information and Privacy staged by the Department of Justice and Treasury Board March 7, 1986.
- Presented a paper entitled "The Security Intelligence Review Committee: Legislative Oversight and Government Policy in Canada Today" at a conference on Intelligence and Policy sponsored by the Defence Intelligence College in Washington, D.C., August 26-28, 1986.

- Spoke on "Accountability of the Security Intelligence Committee" at a seminar organized by Professors Clifford Shearing and Stuart Farson at the Centre of Criminology in the University of Toronto, February 24, 1987.

- Spoke to Osgoode Hall Law School students at York University enrolled in a course on security and intelligence, March 11, 1987, and participated in discussion afterwards. The session was organized by Professor Peter Hanks, a visiting professor from Australia.

Two members, the Honourable Jean Jacques Blais and the Honourable Frank McGee, attended the National Conference on Law in Relationship to Terrorism, sponsored by the American Bar Association in Washington, D.C., June 5-7, 1986.

Our Executive Secretary and a research officer participated in a conference on The Psychology of Terrorism in Washington, D.C., at the Woodrow Wilson Center, International Security Studies Program, March 16-17, 1987.

In addition to attending the August 26-28, 1986, conference on Intelligence and Policy sponsored by the Defence Intelligence College in Washington, D.C., with the Chairman, the Director of Research attended the second annual conference of the Canadian Association of Security and Intelligence Studies at the University of Manitoba in Winnipeg, June 7, 1986.

The Executive Assistant and the Senior Complaints Officer met twice with U.S. Defence Department officials to study personnel security policy and exchange ideas--first at the Pentagon on November 14, 1986, and then at the Personnel Security Research and Education Center in Monterey, California, on January 15 and 16, 1987. At the Research and Education Center, the Executive Assistant made a presentation on the development of the security screening process in the government of Canada.

A research officer attended a symposium on Present and Future Strategies for Employment Testing on June 21, 1986, at the annual conference of the Canadian Psychological Association.

Personnel

Our office remains as lean as it was at the end of last year; throughout 1986-87, we still had just 13 employees, despite a mushrooming workload.

They are headed by an executive secretary who directs all day-to-day operations. Other employees are a research director, two researchers and a research assistant, a senior complaints officer, an executive assistant who supports the research and complaints functions, an administrative officer who is also the registrar for our hearings and coordinator of our response to requests under the *Access to Information Act* and the *Privacy Act*, and five support staff. A complete list with telephone numbers can be found in Appendix C.

Financial Report

Our 1986-87 budget is set out in Table 7. We originally budgeted $344,000 for goods and services in 1986-87, but found that this amount had to be nearly doubled through supple-

mentary estimates to meet needs that could not be foreseen when the main estimates were drawn up in 1985--notably:

- Conducting, at the request of the Solicitor General, a special study of official languages and staff relations problems in CSIS (see Chapter 8, page 49 of this annual report).

- Meeting legal fees associated with the complaints process.

Table 7. SIRC Budget, 1986-87

Personnel		$545,000
Salaries and wages	$475,000	
Contributions to employee benefit plans	$70,000	
Goods and services		$677,000
Professional services	$519,000	
Other	$158,000	
Total operating expenditures		$1,222,000
Capital expenditures		9,000
TOTAL		$1,231,000

(Source: 1987-88 Estimates, Part III)

11. Looking Ahead

Among our priorities for 1987-88, we number CSIS's counter-terrorism program, its intelligence analysis and production process, and the protection of scientific and technical secrets.

Our work on the protection of scientific and technical secrets has already begun, and we might say a word about it here, to set the scene.

Science and Technology. Traditional military secrets are no longer the only targets of espionage. Scientific and technical knowledge must also be protected. Being a member of the Western scientific community as well as of Western military alliances, Canada has a duty to safeguard borrowed as well as home-grown science and technology.

We are looking into a number of issues that arise out of these considerations, including:

- CSIS's part in developing policies to protect scientific and technical assets--ours and our allies'.

- What intelligence CSIS provides to federal departments involved in export controls and other protections for secret scientific and technical knowledge.

- The priority CSIS gives to collecting intelligence on the theft of science and technology and what resources it devotes to this task.

- Whether the government's identification of potential targets is adequate.

- What provisions are made for security screening personnel in high-technology firms that have access to secret scientific and technical knowledge.

We have had briefings from CSIS on these matters and are pursuing our inquiry.

Five-Year Review

But our overriding preoccupation in the coming year will be to draw up a full list of issues that Parliament may want to address when it conducts the five-year review of the *CSIS Act* in 1989.

We intend to consult with interested individuals, with relevant interest groups and with experts in the universities, government and elsewhere. This will allow us both to test the conclusions we have drawn from our experience and to provide them with an early forum for insights we may profit from.

Scattered throughout this report are issues that have suggested themselves in our routine review activities--for example, the protection of solicitor-client privilege (page 19) and the adequacy of raw warrant statistics (page 11).

The Extent of Oversight

Another issue we can already see on the horizon is the oversight function itself. The *CSIS Act* broke new ground when it created this Committee to monitor the Service. But there

are other major players in the Canadian security and intelligence community and they are not in the purview of any independent oversight.

Canadian Security and Intelligence Directory. Indeed, one of the surprises we got when we took up our duties in 1984 was that we could not even find a comprehensive directory of federal government agencies engaged in security and intelligence work.

We felt it was important to know something about CSIS's sister agencies. For one thing, we would better understand CSIS's mandate if we knew the mandates of the others and CSIS's relationships with them. We were particularly interested in committees that disseminate security and intelligence information and that make decisions based on this information. Knowing the needs of such committees would improve our appreciation of CSIS's operational objectives and its relationships, real and potential.

Unable to find a complete directory, we decided to prepare one ourselves, and this task was completed in 1986-87.

We recognize, with regret, that we cannot make the directory public. Some of the material it contains--notably descriptions of the roles played by certain agencies--would be of far too much interest to the enemies of our country. We also promised to limit circulation in order to gain the cooperation of certain agencies that had no legal responsibility to provide us with information.

However, we have made copies available within the Canadian security and intelligence community itself and have been pleased with the very favourable reactions. Apparently we were not alone in feeling that it is useful to know just who does what.

Because of these reactions, we intend to revise and distribute the directory yearly, both to keep our own understanding up to date and to serve the security and intelligence community within Canada.

Cabinet Confidences. Another limit on our present powers is that we are not entitled to be told Cabinet confidences. We have not felt this as a severe limitation to date but, of course, we cannot really assess how much we are missing. We have been concerned that it could be a problem if a Cabinet spread the mantle of confidentiality too widely in future.

We note that the Standing Committee of the House of Commons on Justice and Solicitor General has recommended tightening the definition of Cabinet confidence for purposes of the *Access to Information Act* and the *Privacy Act*,* and we await the Government's response before taking a more precise position of our own.

---

* House of Commons, *Open and Shut: Enhancing the Right to Know and the Right to Privacy*, Report of the Standing Committee on Justice and Solicitor General on the review of the *Access to Information Act* and the *Privacy Act*, March, 1987

A Last Word

At the middle of our five-year mandate, we look back with some satisfaction on what we have been able to do--and forward with not a little apprehension to how much more we have to do.

Yet in reflecting on our work to date, we continue to value two important features of our mandate. The first is our appointment as part-timers, active on other matters in the community and in private life. This has permitted us to remain somewhat more objective and detached from the day-to-day intrigue of security intelligence matters specifically and government affairs generally. Hopefully it has sharpened our analysis and judgement.

Second, we have had the good fortune to attract competent and hard-working professionals as members of our permanent staff and panel of outside consultants and lawyers. All of these Canadians, after achieving the appropriate level of security clearance, have thrown themselves into the task at hand with dedication, energy, and a strong sense of commitment. Treasury Board has responded positively with a level of resources which is limited but nevertheless appropriate. The Committee and hence Canadians are well served by this group of "watchdog" professionals who work long and lonely hours mostly without public recognition--except that which it is our pleasure to provide in this report.

Appendix A

Ministerial Directives and Directions to CSIS, 1986-87

CSIS-RCMP Cooperation Regarding Counter-Terrorism

The Provision of Security Assessments

Notification of the Minister Concerning Certain Types of Operations

Investigative Activity

Use of Confidential Sources

Protection of Canadian Citizens

Protection of Foreign Citizens in Canada

Policy on Reporting Incidents to the Minister

Arrangements for RCMP Assistance

Appendix B

Summary Case Histories of Security Complaints Dealt With by the Security Intelligence Review Committee, 1986-87

Security Clearances

1. A person complained that a Top Secret clearance was denied on the basis of alleged dishonesty in (a) citing false past job titles on a personal history form, (b) misappropriating the employer's property in a past job and (c) having been involved in the sale of stolen goods.

At the hearing, CSIS cited reports from its sources in support of all three allegations. A CSIS investigator answered detailed questions about the reliability of these reports.

The complainant denied all allegations, noting that employer statements confirmed the accuracy of the job titles and arguing that personal animosities lay behind the other allegations. The complainant further argued that the allegation about the sale of stolen goods involved mistaken identity.

The Presiding Committee Member found that the job titles had not been misrepresented, but sustained the other allegations.

The Presiding Committee Member recommended that the denial of a Top Secret clearance be upheld.

2. An individual was denied the Top Secret clearance required for transfer to a special unit. Denial was based on alleged dishonesty, indiscretion, and financial indebtedness.

The allegation of dishonesty turned out to be based on a minor, isolated incident that did not justify continuing concern, and the indiscretion issue proved to be groundless.

But the heavy indebtedness was real, and CSIS held that the resulting financial pressure could tempt the complainant to offer favours to clients in return for cash. It could also tempt knowledgable clients to offer financial inducements.

However, CSIS acknowledged that there was nothing to indicate that the complainant could not overcome the indebtedness by honest means; indeed, it agreed that the complainant deserved credit for positive efforts to deal with the problem.

An official of the employing department testified that, after interviewing the complainant, he was satisfied with the explanation provided for the indebtedness.

Finding that the complainant had the indebtedness under control and that all other allegations were groundless or minor, the Presiding Committee Member recommended that Top Security clearance be granted.

Citizenship

3. Citizenship was denied to a landed immigrant, 14 years in Canada, when CSIS said there were reasonable grounds to believe that this individual would engage in activities constituting a threat to the security of Canada.

At the hearing, evidence was heard from CSIS to the effect that the activities of this individual were in keeping with those of an agent of a foreign government.

The Presiding Committee Member proposed to disclose certain allegations to the applicant and counsel so a reasonable defence could be mounted. The Presiding Committee Member did not seek to disclose facts prejudicial to national security but insisted on appropriate disclosure as required by law.

CSIS then informed the Secretary of State that it wished to withdraw its objection to citizenship for this individual.

The Presiding Committee Member ended the investigation as there was no longer any basis for continuing.

4. An individual who found refuge in Canada after a military coup and later landed immigrant status was denied citizenship when CSIS said this individual was a sympathizer of a terrorist organization in the country of origin.

Paragraph 2(c) of the *CSIS Act* provides that "threats to the security of Canada" include

> activities within ... 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*. (emphasis added)

Both the applicant and CSIS were assisted by counsel at the hearings, and both presented evidence. The Presiding Committee Member also called an expert witness to fill in the background about terrorist organizations in the country of the applicant's origin.

The Presiding Committee Member concluded that this individual did not threaten the security of Canada, and recommended that citizenship be granted.

At the time of writing, the report of the Presiding Committee Member had not yet been acted upon by the Governor in Council.

5. This case, while it was the subject of a separate report, involves the spouse of the applicant dealt with in the preceding case history. The facts and the recommendation are the same. At the time of writing, the report of the Presiding Committee Member had not yet been acted upon by the Governor in Council.

6. Citizenship was denied to a landed immigrant, in Canada since 1966, because CSIS believed that this individual was a threat to the security of Canada. Before the Committee began its investigation, CSIS withdrew its recommendation against granting citizenship.

7. An individual who entered Canada as a refugee and was granted landed immigrant status more than a decade ago was refused citizenship when CSIS alleged that this individual was an agent of influence for a foreign intelligence service. CSIS withdrew its objections to citizenship for this individual before the Committee completed its investigation.

Immigration

8. Upon entering Canada, an individual was detained by immigration authorities, then released the following day after an appearance before an immigration adjudicator.

The Solicitor General and the Minister of Employment and Immigration subsequently reported to the Committee that this individual met the criteria for deportation under the *Immigration Act, 1976*. The specific allegations were to the effect that this person had a close and active association with a terrorist organization and was known to have engaged in terrorist acts.

At the hearing, CSIS supported these allegations. Evidence by the applicant and by witnesses in support of the applicant lacked credibility.

The Presiding Committee Member concluded that that there were reasonable grounds to believe that this person would instigate the subversion by force of the democratic government of another country while in Canada, and recommended that deportation proceedings be instituted.

At the time of writing, the Presiding Committee Member's report had not yet been acted upon by the Governor in Council but the applicant left the country.

Appendix C

SIRC Staff on April 1, 1987

Maurice Archdeacon, Executive Secretary	990-6839
Yvette Collins, Senior Secretary	990-8442
Danielle Blache, Secretary	991-9112
Annie Demirjian, Executive Assistant	990-6319
Shirley Heafey, Senior Complaints Officer	993-4263
Arthur Graham, Director of Research*	990-8051
Maurice M. Klein, Research Officer	990-8445
John M. Smith, Research Officer	991-9111
Joan Keane, Research Assistant	990-8443
Madeleine DeCarufel, Administration Officer and Registrar	990-8052
John Caron, Records Officer	990-6838
Roger MacDow, Records Clerk	998-5258
Diane Marion, Receptionist-Secretary	990-8441

* Throughout 1986-87, the Director of Research was Jacques J.M. Shore, who resigned on March 31, 1987, to practice law in Montreal. We wish to record our gratitude for he contribution he made in the two years he was with us.