SECURITY INTELLIGENCE
REVIEW COMMITTEE

Annual Report

1988-1989

Security Intelligence Review Committee
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.

Minister of Supply and Services Canada 1989
Cat. No. JS71-1/1989
ISBN 0-662-56937-7

September 30, 1989

The Honourable Pierre Blais, P.C., M.P., Q.C.
Solicitor General of Canada
House of Commons
Ottawa, Ontario
KIA OA6

Dear Mr. Blais:

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 1988-89, 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., Q.C.

What we call our future is the shadow
of our past, thrown onto the path ahead of us.

Marcel Proust

Contents

1. FIVE YEARS IN THE LIFE ...

This, our fifth annual report, comes at a key moment. After five years on the books, the *Canadian Security Intelligence Service Act* is due for review by Parliament. Many people with a professional or personal interest in security intelligence will propose amendments that they believe will improve the *Act*. Our own proposals can be found in Appendix A of the present report.*

In this introductory chapter, we review our work during the past five full and interesting years. We are not motivated by sentiment or nostalgia. We have a keen sense--expressed in our choice of epigraph for this report--of how much the future grows out of the past. By reviewing what we have done as Parliament's and the public's eye on the Service (CSIS), we hope to sketch in background that others may find helpful when they think through their position on how well the *Act* has met the goals sought by Parliament in 1984.

For our part, we continue to believe that the *Act* is fundamentally sound and that a civilian agency under well-defined political control and independent oversight is the appropriate model for security intelligence in Canada.

The Committee

A unique feature of the *CSIS Act* is the Security Intelligence Review Committee (SIRC) itself. In the United States and Australia, intelligence agencies are overseen by legislators. Oversight in the United Kingdom has essentially been bureaucratic. Here in Canada, SIRC is appointed by the Governor in Council after consultations by the Prime Minister with leaders of opposition parties in the House of Commons.

We believe that the tri-partisan nature of the Committee has been a strength. It reduces suspicion that the Committee is in the Government's pocket. Yet we found it easy to check our partisanship at the door. In our oversight role we have been able to reach our conclusions by consensus. We have been comfortable about delegating the supervision of investigations and hearings arising out of complaints to one or, occasionally, two or three among us.

The fact we work part-time on Committee business has also been a strength, we believe. It has permitted us to bring a broader perspective to the job at hand as we have all remained active in our professions and local communities and organizations in different regions of Canada. It has spared us the dangers of becoming part of the Ottawa "establishment". Yet, through a competent and aggressive staff in Ottawa, we have been able to say on top of things.

The *Act* gives us two roles--review and the investigation and hearing of complaints.

---

* The substance of Appendix A is reprinted from *Amending the CSIS Act*, which we prepared for the use of the special, all-party committee of the House of Commons reviewing that *Act* and the companion *Security Offences Act*, and of others who intend to contribute to that committee's work.

Review

Review, in turn, can be subdivided into three activities. We keep a watching brief on such things as ministerial directions and amendments to the Operational Manual, the use of warrants and agreements under which information is exchanged with other agencies in Canada and abroad. We look into specific incidents and situations that come to our attention. And, third, we have conducted a series of in-depth reviews of specific areas as the basis for chapters in our annual reports and special reports to the Solicitor General.

During our five years we have completed in-depth reviews of the major operational branches-Counter-intelligence, Counter-terrorism, counter-subversion (which has since been disbanded, as we recommended), and the Analysis and Production Branch. Within the limits set by national security, our conclusions on the Counter-intelligence Branch are reviewed in Chapter 4 of this Annual Report.

We also made special reports to the Solicitor General in a number of thematic areas. Two are reviewed in this Annual Report--science and technology (Chapter 6) and the peace movement (Chapter 5). There have also been special reports on bilingualism and staff relations; allegations that the Service had carried out improper surveillance within the labour movement; security screening in immigration matters; personnel recruitment, training and development; and two issues raised by complaints.*

As an oversight body, our mandate is limited to CSIS. But we have had to look beyond it, to understand its relations with the whole security intelligence community. In last year's Annual Report, we shared some of what we learned about the network of federal departments and agencies involved in security and intelligence matters. Our comments about CSIS in many contexts have had to take account of its relations with other players in this area.

Complaints

Our second role is to investigate and hear complaints that are made about the denial of security clearances in various settings--federal employment and contracts, immigration and citizenship--and about any activity by the Service.

A key outstanding issue is whether the recommendations we make to grant security clearances ought to be binding. A ruly by the Federal Court of Canada is expected in the fall of 1989, around the time when the present Annual Report is tabled in Parliament.

Our own view is that the *Act* should be amended to make SIRC recommendations binding. We discuss our thinking in Appendix A. But in reviewing the record, we believe it is worth

---

* The special report on bilingualism and staff relations was published in 1987 as *Closing the Gaps* and the special report on allegations that the Service had overstepped its mandate in surveillance of the labour movement in 1988 as *Section 54 Report to the Solicitor General on CSIS' Use of its Investigative Powers with Respect to the Labour Movement*. The special report on security screening in immigration matters was not published by the Solicitor General because of the highly classified material it contained. The same is true of the two reports prompted by complaints.

noting that immediately after our appointments we formulated comprehensive Rules and Procedures to ensure that our investigations and hearings balance fairness to the individual complainant, on the one hand, and protection of national security on the other. Our review of each case has been much more extensive and exhaustive than any conducted by the people who made the original decision to deny a clearance.

We also established, at the outset of our mandates, an independent panel of lawyers with security clearances that enable them to act as Committee counsel during investigations and hearings. This has allowed us to appoint counsel instantly when needed. We are grateful for the excellent professional help we have received and the procedural fairness to all parties that has resulted. A list of our counsel can be found in Appendix B.

Themes

Our observations in previous annual and special reports have centred on a number of key themes. At the heart of our approach is a necessary balance between effective protection of national security and respect for individual rights. In the first vein, we recommend, for example, provisions for emergency warrants that would let the Service respond instantly to sudden needs. With respect to the protection of individual rights, we have made a number of key recommendations, such as the use of a "devil's advocate" to argue the case against warrant applications, and limits on targeting. These recommendations have been acted on, at least in part. We have more to say about them in Appendix A.

We have also stressed the need to move from an investigative to a research approach by CSIS. Not, of course, that the Service can do entirely without investigation on classic police models--tracking the movements of suspected terrorists, listening in on conversations that may point to espionage, and so on. But it has seemed to us that the Service does not adequately exploit so-called open information--the mass media, scholarly works, research papers and other sources available on the public record.

The Service's dependence on allied foreign agencies as a source of information has also given us some concern in the past. Again, the exchange of information among agencies is important; it cannot be abandoned. But the Service is constantly in danger--and we found examples, despite efforts by the Service to avoid this pitfall--where the point of view of the foreign agency was adopted uncritically by the Service, without regard to Canadian foreign policy.

Both the stress on investigative techniques and reliance on foreign agencies have had an impact on the quality of assessment that CSIS provides. We have raised the possibility--and do so again in Appendix A--of a separate assessment agency, taking information from CSIS and all other available sources as a basis for advice to the Government.

Another recurring theme has been to encourage the Service to make itself more reflective of Canadian society. That was one of the themes of *Closing the Gaps*. While real progress is being made on bilingualism, we would like to see a speed-up in some other areas--notably to bring the representation of women and ethnic minorities in the operational staff closer to the balance found in Canadian society as a whole.

The Service's First Five Years

Much of our criticism of the Service over the years boils down to this: the Service was slow to make the necessary adjustments after it was split away from the RCMP. It seems clear in hindsight that the sheer mechanical difficulties of transition were underestimated, as were the resources required by the new Service. CSIS had to rely at the outset on the RCMP for a number of services and even for much of its accommodations. It also obtained its initial complement of intelligence officers from the RCMP.

But beyond this, we also detected a lack of commitment in the early stages to real change. Symbolic of this was the Service's reliance for a time on "direct entries", recruiting from police forces more aggressively than developing its own program for producing a new kind of intelligence officer with skills in research and analysis as well as investigation and factfinding.

Nothing happens without reason, of course, and reasons for these problems are easy to find. CSIS was naturally under pressure to keep important operations going, and this kept fundamental reform low on the priority list. And, no doubt, it was not easy for former RCMP officers to set aside the proud traditions of the Force. The sharpened focus on the counter-terrorism program also brought strains. Initially, the Service tried to meet the new needs by reallocating existing resources. But this brought real difficulties and eventually new resources had to be provided by the government.

There was an important turning point in 1987 after our critical report on the counter-subversion program, the report of the Independent Advisory Team appointed by the Solicitor General to follow up, and the collapse of an important terrorism case when it was revealed that unreliable information had crept into an application for a warrant. As a result, targeting procedures have been considerably tightened up and more emphasis has been put on administrative controls.

In our last annual report, we offered the hope that CSIS was "turning the corner" at last. While our position--given our statutory role--remains one of reasoned skepticism about the Service and its work, the experience of the past year gives us increased confidence that CSIS is on course.

Summing Up

Independent oversight of security and intelligence agencies is now a well-established idea. It was resisted at first, but it is coming to be seen as an advantage. Senior officials of both the FBI and CIA have told us that independent review has helped them focus their efforts more tightly and become more efficient and, in the long term, has helped them develop and maintain political and financial support for their work.

We believe that the review and complaints provisions of the *CSIS Act* have proved themselves. Indeed, we think that the time has come to extend review to other agencies in the security intelligence field. We discuss this matter in more detail in Appendix A.

When oversight was first proposed in Canada, there was a view that there should be separate oversight and complaints agencies. It was feared that if the review body had "executive authority", even to the extent of reviewing and recommending on appeals in security clearance cases, it might become part of the "establishment" and lose its frankness in reporting to Parliament and the public. There was also fear that the burden of investigating and hearing complaints would absorb so much attention that there would be no time for more general review of the Service's performance.

Neither of these fears has been realized. We hope others will agree with us that the complaints function has not prevented us from being forthright and as open as national security permits. We know there are people within the bureaucracy who wish we would say less than we do. And we have not been swamped with complaints at the expense of more general review.

But beyond this, we have found that the review and complaints roles have given each other strong mutual support. What we learn in the oversight function is often very helpful in understanding the background to complaints. And complaints bring to our attention some things that we might never, otherwise, find out. We believe that the complaints and oversight functions should be kept together.

Another problem that did not arise in a serious way is that of timing--whether we should wait until files are stone cold before we look at them. A few critics have made much of this issue, suggesting that by looking at ongoing operations we were trying to "direct" the Service, thus exceeding our statutory mandate. In our oversight function, we make observations and recommendations but we do not direct the Service, nor are we qualified to so do.

Unfinished Business

Effective review is a continuous process. Experience has shown that reviewing warrants must be a continuing priority. We further intend to launch a study designed to measure the real usefulness of information gained through such intrusive powers as wiretapping.

Some other areas where we see a need for more work include monitoring of information exchanged with provincial and foreign police forces and government agencies; the use of open sources; visa vetting by CSIS; unauthorized disclosure of classified information; further progress in destroying inappropriate materials on CSIS files; and the Service's role before and after the Air India and Narita Airport disasters.

2. OVERSIGHT

For obvious reasons, the Canadian Security Intelligence Service (CSIS) cannot reveal as much about its work as most public institutions do; both its sources and its product are secret. So the *CSIS Act* makes extensive arrangements for controls on the Service by the Federal Court, the Solicitor General, the Inspector General and the Security Intelligence Review Committee (SIRC).

SIRC's special role is to act as Parliament's and the public's eye on CSIS.* Through private and public comment, it seeks to ensure that CSIS is adequately protecting national security but--and this is crucial--that it is not acting illegally or making unreasonable or unnecessary use of its powers.

Investigating and hearing complaints is part of this process. We deal with complaints in Chapter 8. In this chapter and the five that follow we discuss what we have learned in our more general oversight activities. Chapters 4, 5 and 6 deal with specific topics--counterintelligence, CSIS involvement with the peace movement and the protection of scientific and technological secrets. Chapter 3 deals with CSIS operations in general and Chapter 7 with housekeeping matters. The present chapter reviews the elements of oversight spelled out explicitly in the *Act*.

Ministerial Direction

Under subsection 6(2) of the *CSIS Act*, the Solicitor General can give the Director of CSIS written directions with respect to the Service and a copy of such direction comes to us for review under subparagraph 38(a)(ii). We reviewed five new ministerial directions in 1988-89. They are listed in Appendix C. We also reviewed:

- six 1987-88 directions that arrived too late to be examined before the last annual report was prepared; and

- a package of older documents that the Service regarded as ministerial directions but the Ministry of the Solicitor General did not. These documents were identified in a review carried out to ensure that we were getting copies of all ministerial direction.

With one reservation, discussed later in this chapter in the section on disclosure, nothing we saw permits any unreasonable or unnecessary use of the Service's powers or unduly impinges on individual rights. We are pleased in particular with specific instructions to cleanse files of certain information on individuals, collected before and after July, 1984, under the counter-subversion program. Progress in this area is reviewed in detail in the next chapter.

---

* We call this role "oversight" or "review". Some of our critics would like us to limit ourselves to the term "review", apparently believing that "oversight" implies more extensive powers to direct CSIS. It is true that "review" is the term used in the *CSIS Act*, but, on the other hand, "oversight" is the word generally used in the Western intelligence community to describe this function. The debate seems unproductive, and we continue to use the two terms interchangeably. What matters is what we do. This includes commenting on the Service's performance, both in private and in public. It does not include giving direction to the Service.

As part of our review of ministerial direction, we now also examine amendments to the CSIS Operational Manual. During 1988-89 the Service completed major revisions to a number of chapters originally written for the RCMP Security Service, before the *CSIS Act* was adopted. In general, they tighten Headquarters control over investigations and clarify responsibility for regulating activities. We applaud, in particular, a shift away from a procedure-based, step-by-step approach and towards spelling out general principles that are to be respected in investigations.

Agreements with Governments in Canada

Subsection 13(2) and paragraph 17(l)(a) of the *Act* permit CSIS to enter into arrangements with other arms of the federal government and with provincial governments and their agencies (including police) for the purpose of performing its own duties and functions and to provide security assessments. Subparagraph 38(a)(iii) gives us a twin mandate to review these arrangements and to monitor the provision of information and intelligence made under them.

We received only one new agreement in 1988-89. It was with the Province of Manitoba and is similar to agreements with other provinces. Covering both the provincial government and police forces within the province, it allows for exchanges of information and the provision of assistance generally. It is not binding. CSIS now has agreements with all provinces except Quebec and Ontario and agreements covering major police forces in all provinces except Quebec.

There has been some criticism of provincial governments for entering into agreements with CSIS. We consider the agreements essential: the Service needs access to such provincial information as motor vehicle registrations, while provincially-controlled police and other agencies must get the information they need to assist in protecting public order and individual safety. The existence of agreements does not, in itself, threaten the privacy Canadians are entitled to. In fact, the existence of formal agreements is an element of control over exchanges of information that might otherwise take place on an unrestricted basis.

However, we believe that the exchanges of information that take place should be carefully monitored to ensure there are no abuses. During 1988-89, we developed a framework for monitoring and auditing all information exchanged under agreements with other governments, focusing initially on agreements with provinces. We now have a province-by-province count of recorded transfers of information in the three years from January, 1986, to December, 1988.

A limited spot check we made in one province indicated that most of the information involved is quite mundane--birth records, for example, to check against applications for security clearances. This need cause no concern. However, situations may arise when more sensitive information is exchanged. We need to be in a better position to monitor exchanges of such information. In particular we are concerned that:

- the Service does not distinguish between personal information and other information in the records that it keeps of exchanges;
- it does not tag the release or receipt of particularly sensitive personal information; and

- we do not know in all instances what departments or agencies are being accessed for information.

During the remaining months of this year, one of our major projects will be to audit the record keeping under all agreements--specifically the information exchanged with provinces and the quality of the Service's policies in this area. We have also started examining the information exchanged under other agreements.

Foreign Agreements

Eight agreements were concluded under paragraph 17(1)(b) of the *Act* with police or security agencies in other countries and the Service was also authorized to extend its agreements with 60 police and security organizations. These agreements as such do not give us any concerns. They close gaps that opened when--having been created to separate security intelligence from the police function in Canadian society--CSIS initially cut back its formal contacts with foreign police. It became apparent that CSIS needed these contacts to check criminal and other records in preparing recommendations on security clearances.

But we are still not satisfied that we are able to monitor the flow of sensitive personal information as well as we think necessary. As in its exchanges with provinces and provincially-controlled police forces, CSIS does not tag the information on individuals that it passes to foreign agencies in such a way that we can easily put a ringer on it. By checking any individual file, we can see whether information has been provided and what that information was. But there is no list of files from which such information has been provided.

Because regular searches of all files are not practical, we cannot keep track of the volume of information being provided by CSIS or of its nature. We continue to press CSIS to close this information gap and we expect it to be done when more powerful computers that the Service has been promised are installed.

Warrants

We do not have an explicit mandate to monitor individual warrants. The primary responsibility for them lies with the Federal Court of Canada. However, in the course of our in-depth reviews of CSIS programs we look with great care into affidavits sworn to justify warrant applications. In particular we verify that the affidavits accurately reflect the facts in the files they are based on. We also make it a practice to read all warrants.

In last year's annual report, we outlined significant changes in procedures in this area. They were intended to make identifiable individuals responsible for the accuracy of the facts provided to the Court in support of warrant applications. Procedures have continued to evolve. In particular, the Legal Branch is playing a larger role. Each drafting team consists of a lawyer and an analyst.

We naturally support tighter internal controls on the warrant application process. We believe that the intrusive powers authorized by warrants should be used only in cases of real necessity, when the information CSIS needs to safeguard the national interest cannot be secured elsewhere.

But we are also concerned that the new process is cumbersome. We do not, of course, suggest any relaxation of the rigour that the Service has started to bring to the process. But we are

reinforced in our view that there should be a procedure for emergency warrants. Our thinking and proposals are set out in Appendix A.

We were glad to find in 1988-89 that warrants continue to include protections for solicitor-client privilege. We have noted before now that, unlike the Criminal Code, the *CSIS Act* does not offer statutory protection to solicitor-client privilege. Our recommendation that the *CSIS Act* be amended to provide such protection is also set out in Appendix A.

We also have proposals in Appendix A for strengthening the role of the devil's advocate in the warrant application process. At present, the devil's advocate ensures that the information used to support a warrant application is accurate. This is much less than we intended when we first proposed the appointment of a devil's advocate. We recommend that this position be provided for in the *Act* and that the devil's advocate argue against each warrant before the Federal Court itself, as if appearing on behalf of the target (who does not, of course, even know that a warrant is being sought).

Disclosures in the Public Interest

Section 19 of the *CSIS Act* provides, among other things, that:

> (2) The Service may ... disclose ... such information [i.e., "information obtained in the performance of the duties and functions of the Service under this Act"] . . . *(d)* where, in the opinion of the Minister, disclosure of the information to any Minister of the Crown or person in the public service of Canada is essential in the public interest and that interest clearly outweighs any invasion of privacy that could result from the disclosure, to that Minister or person.
>
> (3) The Director shall, as soon as practical after a disclosure referred to in paragraph (2)(d) is made, submit a report to the Review Committee with respect to the disclosure.

While no such reports were received in 1988-89, we became aware of a loophole that has permitted the dissemination of CSIS information outside the framework of section 19. In one instance, the then Solicitor General asked CSIS to coordinate the preparation and delivery, together with the RCMP and the Department of External Affairs, of a briefing for elected officials. CSIS has no authority under the *Act* to disclose information obtained in its work to elected officials other than members of the Government. Recognizing this, the Minister directed that the information be disclosed by officials "acting as my agents".

Regardless of the merits of this briefing, we are concerned that by making CSIS officials the agents of the Minister, it may be possible to circumvent the principle of section 19 that we be advised of disclosures that take place outside the narrow range of assistance in law enforcement, the conduct of international affairs and the maintenance of national defence.

There is another principle at stake here. The Solicitor General and officials of the Ministry have access to all the information obtained by CSIS using any of its highly intrusive powers. The *Act* provides no limit on how they may use this information. Our recommendation, spelled out in Appendix A, is that disclosure by the Solicitor General and officials and exempt staff of the Ministry be made subject to the same limitations as disclosure by the Service itself is under section 19.

Operational Statistics

We have a mandate under subparagraph 38(a)(vii) of the *Act* to "compile and analyse statistics on the operational activities of the Service". Over the past year, we have developed the specifications for a comprehensive, computerized Oversight Information System covering intrusive powers, the number of targets subject to investigation, financial and staff resources, personnel, file retention and destruction, the use of open sources, intelligence production, information exchanged under agreements with Canadian and foreign organizations, operations undertaken with ministerial approval, and objective measures of threat levels.

We now have some data in all these areas. We have been standardizing it, normally on the basis of fiscal years, so that comparisons can be made easily, and centralizing it in a single data base.

The Service's level of cooperation in this exercise presents a mixed picture. For our part, to save expense and time, we have tried as much as possible to use information that the Service already collects for its own purposes. But while some data is provided by the Service quarterly, which allows us to be reasonably up to date in our analysis, some is provided only annually. In these cases the data is sometimes quite stale by the time we have processed it. Discussion of this problem continues with the Service.

We completed a number of statistical studies in 1988-89--on the use of intrusive powers, on the use of person years and, third, on the investigation of targets originally selected under the disbanded counter-subversion program, In Chapter 3 we report the encouraging findings of the third study.

Unlawful Acts

Under section 20 of the *Act*, the Director must advise the Solicitor General when there is reason to think a CSIS employee has acted unlawfully. We get a copy of the Director's report together with any comment made by the Solicitor General to the Attorney General.

One such report came to us in 1988-89. It involved an Intelligence Officer who passed himself off as a member of the RCMP in the course of arranging a surveillance operation. In this particular case, while the Intelligence Officer showed poor judgment, it does not appear that any real damage was done. The employee has been reprimanded.

In last year's annual report we noted that one report of illegal activity had been referred to provincial authorities, who decide whether to prosecute. The Attorney General of the province has decided not to prosecute in this case.

Special Reports

As part of our mandate under paragraph 38(a) of the *Act* to "review generally the performance by the Service of its duties and functions", coupled with our power under section 54 to make special reports to the Solicitor General, we have conducted a program of in-depth studies over the years.

In 1988-89, we completed studies of the Service's role in protecting Canada's scientific and technological secrets, the Service's involvement with the peace movement, and the Counter-intelligence Program. Reports are being submitted to the Solicitor General. Within the limits set by national security considerations, summaries of our findings are set out later in this annual report.

We also followed up the special study we made the year before on security screening in immigration. We have certain concerns about the effectiveness of the process and are sending a further report to the Solicitor General. A realignment of responsibilities between CSIS and the immigration authorities, now in progress, may go some way to meeting our concerns, freeing the Service from some routine so it can concentrate its efforts on identifying prospective immigrants who could present real threats to national security. We will monitor these changes.

Consultations and Inquiries

As in years past, we met on occasion with the Solicitor General, the Deputy Solicitor General, the Inspector General, and the Director of the Service. We also continued our practice of calling on regional offices of the Service. In 1988-89 we called on offices in Vancouver, Toronto, Montreal, Quebec City, Halifax and the regional office in Ottawa.

In general CSIS continued to be cooperative in meeting our formal requests for information. One difficulty in 1988-89, however, deserves to be noted because of the fundamental principle it raises. We asked to see files that had also been the subject of a complaint to the Privacy Commissioner and an application before the Federal Court of Canada under the *Privacy Act*. We wanted to assure ourselves that the Service had not unreasonably withheld anything from the Privacy Commissioner's examination.

CSIS delayed providing the information because it received legal advice that since the Privacy Commissioner was involved, SIRC may have been beyond its jurisdiction. We could not accept that. The *CSIS Act* says that we are to have access to everything CSIS has on file except cabinet confidences. This is an important principle, and the matter was eventually resolved to our satisfaction.

The question of the exclusion of cabinet confidences is one we have dealt with before. In previous reports we said we knew of no instance in which it impeded us in our work. However, one has now arisen: we were refused access to the Service's Multi-Year Operational Plan (MYOP) on the grounds that it was prepared for submission to Treasury Board, which is a committee of Cabinet.

A compromise has been reached in this instance: while the MYOP document is being withheld, we have been promised access to all the information it contains. However, this

points up the possibility that the exclusion of cabinet documents could sap the effectiveness of oversight. We recommend in Appendix A that subsection 39(3) of the *CSIS Act* be repealed so the Committee has access to all information under the control of the Service, regardless of its source.

Collection of Information on Foreign States and Persons

Under section 16 of the *Act*, the Minister of National Defence and the Secretary of State for External Affairs, subject to the consent of the Solicitor General, can ask CSIS to collect information within Canada about foreign states and non-Canadians, for use in defence and international affairs. Under subparagraph 38(a)(v), we have a duty to monitor any such requests. Again in 1988-89, we were advised of none.

The obvious usefulness of intelligence on other nations in defence planning and the conduct of international relations makes a striking contrast with the failure to make use of CSIS in this area. It suggests to us that section 16 is too restrictive.

In 1988-89 we commissioned a paper* from a well-known Canadian expert on security intelligence, Professor Peter H. Russell of the University of Toronto, on the advantages and disadvantages there would be in creating the kind of foreign intelligence agency that Australia, the United States and other countries have. We agree with his conclusion that Canada does not need such an agency at this time.

However, as discussed further in Appendix A, we also endorse his recommendation that the limiting words "within Canada" be removed from section 16. This may encourage the government to make more use of CSIS in this area. One benefit could be to make Canadian policy-makers less dependent on intelligence gathered by the agencies of other countries and shaped by their, rather than Canada's, needs.

Report of the Director and Certificate of the Inspector General

The 1988-89 Annual Report of the Director of CSIS to the Solicitor General has been received. As we completed work on our own annual report, the Inspector General was still developing his Certificate, indicating whether he was satisfied with the Director's report. Comment must await the Committee's next report.

In 1988-89 we received the Certificate of the Inspector General for the period of January 1, 1987, to March 31, 1988. It was a most useful supplement to our own thinking and research. We note that it gives good marks to changes in the way CSIS selects targets and decides how intensively to investigate them, confirming the view we expressed in the last annual report on the strength of our own research.

---

* This paper is available from Professor Russell.

Unauthorized Disclosures

Like all security intelligence agencies, CSIS has an internal security system to protect classified information from unauthorized disclosure, destruction, removal, modification or interruption. It is directed against penetration from outside and also against failure from within resulting in accidental or deliberate leaks.

In 1987 there were a number of public disclosures--including a news report revealing a highly sensitive intelligence gathering operation--that pointed strongly to the possibility of leaks from within the Service. As a result we asked the Inspector General under section 40 of the *CSIS Act* to conduct on our behalf a review of CSIS policy and practices relating to unauthorized disclosures of classified information. We also asked the Inspector General for his views on the role the RCMP should play in the investigation of suspected leaks.

We have now received the Inspector General's report and are considering its findings and conclusions. We will provide a section 54 report to the Solicitor General in due course.

3. CSIS OPERATIONS

While the *CSIS Act* spells out a number of specific tasks for us, it also gives us a broad mandate to review generally the performance by the Service of its duties and functions. Having disposed of the specific tasks in the preceding chapter, we now turn to a more general survey. Two principles underlie our approach--the effective protection of national security and respect for individual rights and freedoms.

Use of Warrants

The use of such intrusive techniques as electronic eavesdropping and mail-opening is allowed only under warrants from the Federal Court of Canada. As can be seen in Table 1, the total number of new and renewed warrants rose to 90 in 1988-89 from 75 in the previous year. This is a sharp rise, but it is more apparent than real; there was some catching up to do following delays in renewing warrants while a more rigorous process (see Chapter 2) for applying for warrants was put in place. The total number issued and renewed in 1988-89 remained below 1985 and 1986 figures.

We remain dissatisfied with the limited warrant statistics it has been possible to make public. This is territory we have covered extensively in past annual reports. The Service

Table 1. New and Renewed Warrants

	calendar years			fiscal years*	
	1985	1986	1987	1987-88	1988-89
New warrants	82	95**	71	67	55
Warrants renewed	27	11	5	8	35
Total	109	106	76	75	90
Average duration of warrants (days)	173.6	162.2	190.8	211.5	224.3

* We are reporting warrants statistics on a fiscal-year basis for the first time. In previous years we had reported numbers for the preceding calendar year. The change brings warrant statistics into line with the rest of the annual report, which covers the fiscal year. In order to permit comparisons with the previous year and to keep the record complete (otherwise warrants issued from January to March, 1988, would not be counted), we are also providing the 1987-88 figures.

**In past annual reports, by inadvertent error, we reported 94 new warrants in 1986.

Source: CSIS

believes that greater disclosure could compromise national security but we note that Canadians get less precise information now than they did before 1984, when security intelligence warrants were issued under the *Official Secrets Act.*

Therefore, in Appendix A we spell out a proposal that the *Act* explicitly authorize the publication of statistics showing the number of Canadians--citizens and landed immigrants who have been under surveillance. We think this is something that Canadians are entitled to know and that provides a meaningful measure of the level of CSIS activity.

Access to CPIC

CSIS is within sight of much improved access to CPIC (Canadian Police Information Centre), the computer-based, radio-linked network that gives police instant access to data banks on vehicle registrations, outstanding arrest warrants and other information.

Initially, CSIS could get information from CPIC only through the RCMP. Later it got direct access, but only for counter-terrorism purposes and with terminals only at Headquarters and in two of the six regions. This was plainly insufficient. As we pointed out in our 1986-87 Annual Report:

> ... 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 were puzzled and disappointed that it was taking so long to resolve this problem.

CSIS and the CPIC authorities are now considering a draft agreement that would give the Service access for all purposes to two of the three data banks--Identification Records and Motor Vehicle Records. The exclusion of the third data bank from the draft agreement on access does not trouble us. It includes information on open police investigations.

However, we are dismayed by the exclusion of Quebec motor vehicle records from the agreement. This means, for example, that CSIS cannot readily identify the owner of a car with Quebec plates used by a suspected terrorist.

The Quebec authorities have decided that they will not negotiate an umbrella agreement for cooperation with CSIS until they have first reached an agreement with the RCMP for cooperation with respect to the *Security Offences Act.* CSIS already has umbrella agreements with police in all other provinces.

This exclusion mars an otherwise important step forward in giving CSIS the tools it needs to do its job. We share the Service's hope that an umbrella agreement can be reached soon with Quebec.

Security Screening

The persistent problem of delays in processing security clearances has eased considerably. A number of factors made this possible. One was prompt and effective action on the recommendations of an expert called in from Treasury Board to see how the system could be streamlined. Another was an important change in the way citizenship screening is handled. Instead of making a report on each applicant for citizenship, CSIS now reports only when checks on an applicant reveal problems.

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

Analysis and Production

A number of welcome changes have taken place in the work of the Analysis and Production Branch since we reviewed its activities in 1987-88.

Our fundamental criticism was a marked stress on short-term current analysis, which focuses on events as they unfold and alerts the authorities to potential problems, at the expense of long-term basic analysis, providing in-depth data designed to help the government in policy development and strategic decision-making.

Behind this imbalance lay a number of structural factors. We found, for example, an institutional bias in favour of information gathering by operational programs--counter-intelligence and counter-terrorism--rather than advice to government. So the work of the Branch seemed to be driven by what the operational branches made available rather than by what the ultimate users of intelligence needed. We concluded that this could be explained in part by the fact there was no clear direction from the government on its needs for basic intelligence.

A strategic plan for intelligence requirements and priorities for production has now been prepared for consideration by the Government. It arises out of a forecast of threats prepared by the Analysis and Production Branch itself on the basis of a canvass of departments that use intelligence. It is expected that the decisions flowing from it will give the Branch its first overall guidance from the government on the intelligence that is needed. In addition, the executive-level Intelligence Production Committee within CSIS, which is primarily involved in strategic planning, has become more active.

The Service is also turning away from the bias we found in favour of generalists over specialists. A number of steps have been taken that will increase the level of expertise in the Branch. Its work has been reorganized along geographic lines; analysts are now assigned to specific parts of the world rather than to particular kinds of threat to national security. This gives them a real incentive to become familiar with the cultures in which the majority

of terrorist and espionage threats have their sources. The number of analysts will also double.

At the most mundane level, it is also helpful that analysts have been relocated out of the operational branches and now--albeit in excessively crowded quarters--are near their own chiefs.

An effort is being made to bring Security Liaison Officers into the Branch after they have ended their tours of duty abroad. We had seen this as a source of ready-made expertise that was being overlooked. The first officer has already arrived in the Branch in a senior position.

Perhaps the most striking development is that the Service is now looking beyond its own ranks for expertise. Steps are being taken to recruit academics and other specialists on contract to conduct basic analysis in their fields of expertise under the aegis of a new Strategic Analysis Group. Ready access to the academic world was one of the things that most impressed us about Australia's Office of National Assessments.

A welcome change has also taken place in the focus of the Intelligence Production Committee within the Branch. It is now mandated to ensure that intelligence reports provide sufficient analysis, including forecasting, and that the "implications for Canada" sections are adequate. One fault in past reports was that they sometimes did not stray far beyond a mere description of issues. We were also concerned that foreign sources of information were sometime relied upon too uncritically.

CSIS has taken important steps to correct the shortcomings identified by us and by the Independent Advisory Group in 1987. But we continue to believe that the creation of a separate agency to analyse intelligence from all sources--not only CSIS--deserves further study. We discuss this matter in Appendix A.

Counter-terrorism Program

The year under review passed without a serious incident of terrorism, and the Counter-terrorism Branch deserves some of the credit. The greatest challenge that the Branch faced--if only because any incident would have echoed worldwide--was last year's Economic Summit in Toronto. CSIS issued a number of threat assessments and developed a video presentation to inform other agencies of what they should be alert to. The success of the video can be measured by the fact that a number of other governments asked for copies.

CSIS has been actively involved in the development of government-wide policies and procedures for responding to terrorist incidents. During exercises designed to ascertain the readiness of various departments and agencies, the Counter-terrorism Branch has shown that it can swing into action rapidly.*

---

* It had a real-life occasion to do so soon after the end of the fiscal year under review when a Montreal-New York bus was hijacked and driven to Parliament Hill. At this stage, dealing with the hijacking was essentially a police operation. But, for example, it was through CSIS contacts that the identity of the hijacker was determined before the incident came to its peaceful end.

In last year's Annual Report, we mentioned the targeting of a Latin American group whose contribution to conflict abroad, we said, had dwindled to the point of insignificance. The scope of this investigation has been reduced.

There has been progress in another area we went into. Instructions have gone out to field investigators making it clear that they may stay in regular touch with people in ethnic communities that include some groups that resort to political violence related to disputes in their homelands. This is in line with a recommendation we made. We are satisfied with guidelines that have been written into the Operational Manual for such community relations. Guidelines are necessary because of the chilling effect that CSIS operations can have on legitimate political activities in ethnic groups.

While it is not, of course, possible to go into details here, the Service also seems to have had some success in significantly reducing meddling in ethnic communities by foreign agents over the past year. We also noted in our special report last year on the counter-terrorism program that the agents of some governments are known to give CSIS inaccurate information designed to make the Service do things that are useful to them. CSIS is aware of this and we found that it had done a good job in separating fact from fiction.

The Service has been considering splitting the research and briefing functions within the Counter-terrorism Branch. This was our recommendation and we encourage it to proceed. We had concerns that research was being short-changed as the unit met frequent and urgent demands to prepare briefings. A separate research unit will be better able to focus on consolidating operational intelligence and thus determining patterns and trends in global terms so the Branch is ready for new threats.

One rising threat seen by some commentators is "narco-terrorism" or trade in illicit drugs to support political violence. While this is a major problem in some places, notably some Latin American countries, CSIS believes that narco-terrorism is not significant in Canada at this time. The RCMP agrees. CSIS believes that Canada's drug trade is run by criminals of the traditional sort, motivated by their own greed rather than service to a political cause; there may be isolated instances of individuals who mix terrorism with drug dealing, but they are small-timers, operating on their own account.

Air India and Narita

After very careful consideration, we decided in December, 1988, that we could and should undertake an inquiry into CSIS actions or lack of action before and after the Air India and Narita disasters in June, 1985, both involving flights originating in Canada. While the RCMP is responsible for the investigations, questions have been raised about whether CSIS could have done more to prevent these disasters and whether it has been sufficiently helpful in the police investigation afterwards. We believed that a carefully limited but thorough inquiry would be most useful and would not affect either the judicial process or the police investigation that is still underway.

Early in 1989 we drew up terms of reference with care, recognizing that a false step might prejudice Canada's ability to bring any culprits to justice. We asked the Director of CSIS for comment on the terms of reference and he offered his full cooperation.

Since any inquiry would require the cooperation of other agencies, the Chairman also consulted with the Deputy Solicitor General and the Deputy Attorney General of Canada. Strongly supported by the Commissioner of the RCMP, they took the position that any inquiry at this critical time, even one as precisely focused as we planned, could hinder the police investigation and could also hinder the course of justice. With some reluctance, we accepted the request of the Deputy Attorney General that we not proceed with our inquiry at this time.*

However, we advised him that we would continue to require CSIS to provide us with updates on the investigation, and we reserved the right to commence the inquiry at any time. We have assurances that CSIS is now keeping tapes of tapped conversations that could be relevant, to permit a thorough inquiry when the time is right.

CSIS and Native Peoples

The Service made inquiries across Canada in 1988-89 about the potential for foreign influence and violence among native peoples. The inquiries were based on a rash of statements by native leaders suggesting that there could be violence if there were no accommodation to native demands. The inquiries were completed in March, 1989, and CSIS provided the Government with its assessment.

We have been asked about interviews in which the Service sought information relating to protests by the Innu people of Labrador against low-level training flights by NATO aircraft over the land they occupy. As a result, we are going into this in some depth. This process is continuing as we complete work on this Annual Report. We will report our findings and conclusions to the Solicitor General when our inquiries are completed, with recommendations for public release if appropriate.

Counter-subversion

CSIS has continued to narrow its focus on individuals and groups originally targeted under the counter-subversion program. A statistical study we carried out in 1988-89 showed a dramatic decline in the number of targets and in the use of intrusive powers and human sources.

When the counter-subversion program was disbanded, some of its targeted individuals and groups were reassigned to the Counter-terrorism Branch, some to the Counter-intelligence Branch and some to the Analysis and Production Branch. Most targets were simply dropped.

The use of intrusive techniques under Federal Court warrants is significantly reduced. There are no ministerial authorizations for the use of intrusive techniques to investigate solely on

---

* The text of the relevant correspondence between the Chairman of SIRC and the Deputy Attorney General can be found in the *Minutes of Proceedings and Evidence of the Standing Committee of the House of Commons on Justice and Solicitor General*, Issue 3 (May 30, 1989), pages 3:8 and 3:9.

the basis of the definition of a threat to the security of Canada found in paragraph 2(d) of the *CSIS Act.*

Considerable work is being done to weed the files, both paper and electronic, removing information that is not strictly required. All material that falls outside the CSIS mandate or was of no intelligence value is being segregated so as not to be available for normal operational purposes. The residue has been set aside pending consultations with the National Archives on whether it should be destroyed or kept under lock and key for future historical research.

Cleaning the Files

CSIS is making progress towards ensuring that its files conform with section 12 of the *Act*, which sets out its basic mandate to collect and retain information, and with section 2's definition of threats to the security of Canada. This has been necessary because CSIS inherited so many files from the RCMP Security Service, which was not under the same statutory restrictions.

Files are being assessed by a special unit within the Records Branch in consultation with operational branches. From March 15, 1988, to March 31, 1989, more than 115,000 files were destroyed and a further 3,508 were packed for transfer to the National Archives as soon as the room where they will be stored has been made secure. All files on individuals and groups in the labour movement have either been destroyed or, because of their historical interest, packed for the Archives.

Access to another 57,473 files has been restricted while they await review. These include files opened under the disbanded counter-subversion program that have not already been either destroyed or packed for the Archives. They can be consulted only with the approval of the Deputy Director General, Records.

Corresponding material in the computerized information system has been placed in a separate data bank pending review by a special unit within the records branch. Material still under review can be consulted by intelligence officers only if they have a valid operational reason and the approval of the Deputy Director General, Records.

When Intelligence Officers want to use restricted information, it is reviewed on a priority basis. Material that meets the requirements of the *CSIS Act* is restored to the general filing system or data banks for use. Material that does not is deleted.

4. COUNTER-INTELLIGENCE OPERATIONS

On February 9, 1989, Stephen Ratkai was sentenced by the Supreme Court of Newfoundland to nine years in prison for violating the *Official Secrets Act* in gathering classified information for Soviet interests on the U.S. Navy base at Argentina. It was a reminder to Canadians that espionage within our borders is a real and continuing threat.

No fewer than two dozen states are known or suspected by CSIS to be engaged in activities prejudicial to national or allied interests and security, in or against Canada. In some cases, they want secrets relating directly to defence and other national interests. Stephen Ratkai, for example, offered a substantial amount of money for information that would allow the Soviet Union to develop countermeasures against the Canadian and allied systems for tracking the movement of foreign submarines.

A second kind of threat involves attempts by foreign countries--some of them widely perceived as friendly--to turn policy and events in Canada to their own purposes. For example, some countries covertly use "disinformation" and other means in hopes of building support for policies that serve their interests rather than Canada's. Some ethnic communities are the targets of foreign agents who want to undermine enemies of the regime in the homelands.

Meeting the threats of espionage or sabotage and of covert foreign influence that misuses Canada's free and democratic political system is the task of the Counter-intelligence (CI) Branch of CSIS.

Counter-intelligence in Canada is older than Confederation. Over the years, its targets have included Fenians, radical labour and communist groups that preached revolution, Nazis and Fascists. Since the end of the Second World War the principal--but not the only--interest has been the intelligence activities of the Soviet Union and its friends.

This is an area where Canada has had a good reputation in the global intelligence community. In his best-selling *Spycatcher,** for example, Peter Wright credits Canada with innovating "many of the ideas which later played a major role in British and American thinking, such as computerized logging of the movements of Russian diplomats in the West".

During 1988-89, we completed three studies relating to the CI program at CSIS. One on CSIS investigations in the peace movement is reviewed in Chapter 5 of this Annual Report and one on the protection of scientific and technological secrets in Chapter 6.

The present chapter reports on a study we made of the CI Branch generally. A full report is going to the Solicitor General for his information and whatever action he deems appropriate. Because the full report contains a great deal of classified information, the review in this chapter is necessarily limited. However, we feel it is important to raise the curtain of secrecy wherever and as much as we can.

---

* *Spycatcher,* by Peter Wright (Stoddart Publishing Co. Ltd., Toronto, 1987).

Our Study

Our study followed two parallel lines. We undertook, first, an audit of the use of investigative powers, using an increasingly structured and standardized approach to answer the question, “Is anyone being investigated illegally or unreasonably or unnecessarily?” The
second line was an evaluation of investigations, aimed at answering the question, "Is Canada well protected?"

The ultimate measuring stick is the *CSIS Act*. At the heart of the Service's mandate is section 12, which directs it to collect information, to the extent strictly necessary, on threats to the security of Canada, to analyse and retain such information, and to report to and advise the Government. Adherence to ministerial direction and the CSIS Operational Manual are also tests we apply.

Threats to the security of Canada are defined in section 2 of the *Act*. The CI Branch deals with threats defined in two paragraphs of this section. Paragraph 2(a) covers espionage and sabotage. This is quite straightforward; it is impossible to imagine any argument that espionage and sabotage can be tolerated.

Paragraph 2(b) deals with foreign influence, and it presents a more difficult picture. Under paragraph 2(b), an activity threatens the security of Canada if it meets all four of the following conditions: it is foreign influenced; it is detrimental to the interests of Canada; it is within or related to Canada; and it is clandestine or deceptive or involves a threat to any person. We believe that paragraph 2(b) should be revised to narrow the possibility that investigations spread into purely lawful advocacy, protest or dissent, which are specifically excluded in section 2 from the Service's purview. In Appendix A of this annual report we propose an amendment and set out the rationale for it.

In the course of our study, we conducted in-depth examinations of some specific cases chosen at random, seeing how they unfolded at every step. Our purpose is partly to understand how CSIS operates and partly to serve as a spot check for any illegal activities by the Service or any unnecessary or unreasonable use of its powers. We also followed our usual practice of consulting with CSIS field investigators in the regions as well as with Headquarters officials.

Targeting

The targets of intrusive investigation by the CI Branch are mostly foreign nationals. Overall about 16 per cent are Canadian citizens or landed immigrants.

In a report two years ago, we said the counter-subversion branch had cast its net too widely and was investigating many Canadians without reference to the actual threat, if any, that they posed to national security. So we took an especially close look at targets investigated solely under the foreign influence mandate, which were inherited by the CI Branch when the counter-subversion branch was dismantled. We wanted to know what had happened to them.

We found that investigations in this area have been reined in drastically, both in numbers and in scope. However, some concerns emerged from our study of investigations in the peace movement, and they are discussed in the next chapter of this Annual Report.

Another issue concerns information thresholds. We noted that CI targeting, even with reference to espionage investigations, is often based on very little information. We recognize that this is unavoidable. For example, when a secret document is photocopied and then put back where it belongs, there is no visible evidence of loss. Furthermore, professional spies are trained to avoid detection, and it is not to be expected that they will make their illicit activities obvious. The use of known techniques to evade CSIS surveillants is not in itself a threat to the security of Canada. But it has to be presumed that a foreigner who uses these techniques has something to hide, and we acknowledge that it may be grounds for targeting.

While the evidence is often skimpy, we did not rind any case where we felt there was no basis for targeting. We raised concerns, however, in one case. Here the initial targeting decision seemed correct to us. But a lengthy investigation has not turned up much information.

This points to a basic issue in targeting. While espionage is a long-term activity, in which the cat may wait years before pouncing, CSIS controls on targeting procedures are designed for the short-term. Targeting decisions are reviewed annually and, if intrusive techniques are used, warrants must be renewed no less than once a year. Yet there may not be any payoff over a one-year period to make the need for renewal obvious. This could be a problem for the CI program if impossibly high standards were set for targeting in this area.

But so far this has not happened. It was the contrary tendency we noted in some cases--an inclination to renew targeting over many years despite the failure to uncover any information clearly demonstrating a threat to the security of Canada. But, in accordance with its new targeting procedures, CSIS has recently stopped some investigations that fit this description. We encourage it to keep a critical eye on non-productive investigations.

Another issue is the ability of field investigators to maintain contacts with people who are not themselves targets of investigation or sources of information about targets, keeping an ear open for tips or hints of significant developments. There was some concern that tighter controls on targeting, instituted in 1987-88 in line with recommendations we made, limited such community relations. What we say on page 19 of this Annual Report, with reference to the same concern in counter-terrorism, applies here as well. Field investigators should have considerable freedom to maintain community relations and we note that this freedom is being provided. At the same time, we are pleased that precise guidelines have been established because of the chill that attention from CSIS can put on legitimate political activities.

Investigations

The open literature on counter-intelligence describes two types of operations. One can be called passive. Human and technical surveillance is mounted to determine the source and nature of threats. Vulnerable assets are also identified and personnel in government and

sensitive industries are alerted to potential threats. The second type of operations can be labelled active. It involves taking steps to neutralize threats.

CSIS is directly engaged in passive operations through the collection, retention and analysis of information, as provided for by section 12 of the *Act*. But the *Act* does not provide a mandate for active operations. Responsibility for neutralizing threats falls on the Government, which can take such steps as laying charges, refusing visas and expelling diplomats
who have engaged in spying or illicit interference in Canadian affairs. CSIS does have a mandate under section 12 to give information to the Government and advise it.

The CI program includes the identification and surveillance of suspected foreign agents, to build files that can ultimately be used by the Government to take appropriate action, vetting visa applications by visitors, and providing security briefings.

We found that CSIS takes a methodical and logical approach to collecting information and assessing it. Following recent reforms, Headquarters maintains very tight control over the use of intrusive powers. A review of warrant applications, prompted by the Atwal case, turned up a large number of errors in applications originating in the CI Branch and elsewhere. Although CSIS notified the Federal Court of these errors, the Court took no action. While the granting of warrants is a matter for the Court, we believe that none of the errors alone was significant enough to bring into question the need for the warrant.

We examined changes that have taken place in the Human Sources Branch and were impressed on the whole by a new approach that stresses the principles to be followed rather than detailed rules. We believe that sound general principles, well understood by both sources and their handlers, are a stronger bulwark against unnecessary and unreasonable investigation than step-by-step rules are. In general we feel that sources are well managed.

Headquarters also exercises a moderating role with respect to some of the analyses developed by regional offices. The study reinforced our view that it is of vital importance for Headquarters to have experienced officers providing analysis to their counterparts in regional offices. This capability is critical if limited resources are to be focused on the targets who most merit attention.

Generally speaking, we have few complaints about the procedures CSIS uses to identify individuals suspected of working for foreign intelligence agencies. A key program in this area is the collation of reports that Canadian officials abroad make on their contacts with officials of specified foreign governments and the analysis of reports on the debriefing of Canadian officials on their return home. As a result of CSIS initiatives, cooperation by the Department of External Affairs and the Department of National Defence in this area seems to have improved dramatically over the past year.

Historically, prime targets for all security intelligence agencies are "illegals"--foreign agents who enter the target country with false documentation and try to melt into the general population, posing as ordinary people. The recent CSIS decision to reorganize the functions of its resources in this area should improve its efficiency.

We have some concern about the influence that allies may have in the CI Branch's activities. With little ability to collect foreign intelligence on its own, CSIS has no alternative but to look to other agencies. This underscores the importance of having a first-class analytical capacity to help the Service separate the wheat from the chaff. We dealt with this issue in last year's Annual Report and return to it in Appendix A.

We also see a need for the reconstitution of an operational research unit within the CI Branch. The Counter-terrorism Branch has such a unit in operation and so did the CI Branch at one time. While the analysts now working in the CI Branch have their attentions unavoidably--and properly--glued to particular investigations and sets of investigations, a research unit could use information culled from all the case histories, covert human sources and defectors, public documentation ("open sources") and other intelligence agencies to pinpoint unsuspected problems and emerging threats.

A research unit may be even more important in the CI Branch than in the Counter-terrorism Branch, because hostile intelligence agencies are generally more sophisticated than terrorist groups, using more advanced technology and having greater resources of all kinds. A research unit would also be a pool of experienced professionals who could step outside the high pressure environment of particular investigations in order to obtain an overview --a centre for building up and maintaining the collective experience within the Branch. Our secret report to the Solicitor General elaborates on this issue.

CSIS can and does cooperate with allied intelligence services, sometimes in Canada and sometimes abroad. Such operations are not common and each one requires written authorization by the Solicitor General.

Our examination of these operations centred on whether Canada retained control over all activities within its borders, whether the mandate of section 12 was respected and whether there was a benefit to Canada. In the case of activities abroad, we were also concerned that they not be perceived as offensive information gathering by Canada. While we flagged some concerns, we found that the Service stayed within its statutory mandate and was generally successful in meeting the policy goals cited above.

CSIS has been instrumental in helping a small number of defectors and political refugees who have sought asylum in Canada. To a large extent, the success of such operations depends on the cooperation of police and other agencies of government, federal and provincial. We have been informed of two cases in which police did not consult with CSIS at an appropriate moment in such operations. While the Service has already taken steps to make itself known to police across the country, we urge it to continue these efforts until every responsible police desk understands CSIS' role.

Conclusion

At the outset of this chapter, we posed two questions. In answer to the first, we found that, with the reservations discussed in Chapter 5, we have few quarrels with the choice of targets for Cl Branch investigations. As was to be expected, the overwhelming majority of targets under intrusive investigation are foreign nationals.

In answer to the second question, we believe that the CI Branch proceeds in a methodical, logical way to protect national security. However, we believe that the Government and senior CSIS management, after focusing strongly on the counter-terrorism program for the past few years, should give more attention to the policy and resource requirements of the CI program.

We see a number of areas where additional resources might be put to good use. Without going into a long list, we believe, for example, that the program for identifying hostile agents through contact reports by Canadians abroad and debriefing may merit more attention as evidence mounts that approaches are increasing in third countries--that is, countries other than Canada and the homelands of the agents. Further resources could also be used in the development of new investigative tools and computer capacity.

5. CSIS AND THE PEACE MOVEMENT

In early 1989, as promised in last year's Annual Report and in Part III of the estimates, we completed an investigation into CSIS activities associated with the peace movement in Canada.* A classified report containing our detailed observations, conclusions and recommendations is being sent to the Solicitor General and the Director of CSIS. This chapter sets out our thinking on the subject and provides as much information as can be made public on the substance of the report.

Our Study

Because we are limited in what we can say publicly, it is perhaps important to say something about our methodology so that readers can assess our thoroughness.

We conducted an extensive study of the activities of both CSIS and the predecessor Security Service of the RCMP in relation to the peace movement. We adopted this approach so as to put current CSIS activities in perspective. Naturally we have focused on what CSIS is doing now.

Our research included meetings with officials at CSIS Headquarters and key regional offices, and we reviewed relevant CSIS reports for an understanding of the kind of information the Service provides to its consumers. However, we relied principally on a review of scores of operational files (some running to dozens of folders) while focusing on a detailed review of five organizations and ten individuals active in the peace movement.

Throughout the investigation, the questions we sought to answer were:

- to what extent, if any, has the Canadian peace movement been monitored by CSIS; and
- if there were monitoring activities, were or are these activities justified under the *CSIS Act?*

Our concern extends beyond the strict legality of CSIS operations. In accordance with section 40 of the *Act*, we also have a duty to determine whether the Service makes "unreasonable or unnecessary" use of its legal powers.

This is an important distinction. Because the risk of investigation as a security threat can discourage Canadians from using their constitutional right to speak out on sensitive issues, CSIS must be prudent as well as strictly lawful in its choice and investigation of targets. It should act only where there is a clear and manifest threat to the security of Canada. The "strictly necessary" provision of section 12 reinforces section 40 in making this clear.

---

* The basic research was conducted for us by Jacques J.M. Shore, a lawyer with the Montreal law firm of Heenan Blaikie, who was our Director of Research until June, 1987. He was assisted by two members of our staff.

Peace--The Context

International peace is a goal that everyone can accept unreservedly. But, despite that apparent unanimity, the range of opinions about what constitutes “peace” and how it can be attained or preserved is greater than on almost any other issue.

Most nations assert that their military strength is necessary to preserve peace. Yet one nation's strength is often seen as a threat to its neighbours and competitors. It is also true that a nation's military weakness has often precipitated war or has, at least, been perceived as the cause of war. Every country, therefore, tries to match or exceed the strength of its neighbours, leading to an arms race somewhere in the world in every generation since records were kept, all in the name of peace.

Avowals of peaceful intentions by militarily powerful states are treated with suspicion because history provides innumerable examples of nations that advocate peace but build threatening military machines and then attempt to subjugate their neighbours, and of nations whose verbal devotion to the cause of peace is unassailable but which constantly attempt to weaken or undermine the strength of others.

Within the living memory of many Canadians is the Neville Chamberlain declamation "Peace in our times", ceding the Sudetenland to the Third Reich and emboldening Hitler in his quest for European domination. One can only question the intelligence made available to that British Prime Minister prior to his meeting.

Peace is not, therefore, a simple concept. It is a complex idea that raises many questions, Peace with whom? On what terms? With what degree of assurance? With what guarantees of security? For how long?

It has always been a function of national security intelligence agencies together with other intelligence agencies to assist in answering those very questions.

During the more than forty years since the end of the Second World War, much of the industrialized world has been divided into two armed camps. The situation can be evoked in a few well-known phrases--iron curtain, cold war, McCarthyism, Berlin Wall, Prague Spring .... Through a succession of thaws and chills, the cold war has been a central reality of world affairs.

Perhaps the Soviet Union's fear of being attacked a third time this century was underesti- mated, and so to some extent the Kremlin's motivation was misunderstood, but the reality that had to be faced by the West was that of a powerful military machine at the service of an expansionist ideology. When the Warsaw Pact or the Kremlin spoke of peace, the West was suspicious because of military intervention in places like Czechoslovakia, Hungary and Afghanistan.

Many people began to fear for the future of civilization and even of the human race unless the hostility could be ended and the arms race wound down. A powerful peace movement arose in the West long before society's leaders in either East or West changed the attitudes they had developed during the cold war. A tiny public movement for peace grew in the East Bloc too, but was either suppressed or taken over by government.

The new and infinitely larger peace movements in the democratic countries of the Western Alliance were widely suspected by the allied intelligence agencies, at least initially, of trying to weaken the NATO Alliance and, thus, of acting wittingly or unwittingly as the ally of the militarily threatening Communist Bloc. It was also observed that some of these peace organizations became favourite haunts for active senior members of the Communist Party of the country in which the peace movement was active.

The motivation of the Security Service of the RCMP was perhaps made unique among the allied services by the "Gouzenko Affair". In 1945 a Soviet cypher clerk, Igor Gouzenko, defected in Ottawa and revealed an elaborate spy ring implicating a number of Canadians, including civil servants and a member of Parliament, in the passing of secret information to the Russians.

The Taschereau-Kellock Royal Commission was charged with conducting a full enquiry and its recommendations in 1946 zeroed in on the failure of the Canadian public administration to keep its secrets and the need to improve the security system. A major recommendation was to tighten the security clearance process to prevent "access to sensitive government posts by persons likely to commit the type of acts mentioned in this report". It is evident that the targets of this new policy were to be primarily communists, and their fronts.

It was in this atmosphere that the Security Service of the RCMP, together with police and security intelligence agencies in every member country of the NATO alliance, started to accumulate files on foreign influence within their respective peace movements. Western intelligence agencies worked together very closely on this issue.

Very soon after we started our investigation we saw that monitoring of the peace movement fell into two distinct phases with a major turning point coming in 1988.

Until 1988

We found that, prior to 1984, the Security Service of the RCMP, by targeting peace groups, had collected an enormous amount of information and opened a very large number of files on groups and individuals connected with the peace movement. Essentially, any contact whatsoever with members of the Communist Party of Canada, provincial Communist Parties, Soviet officials or any one of the array of organizations labelled as "Soviet fronts"* brought a group or individual under suspicion of "subversive" activity, and information was collected on them. The result was that very many of the files on ordinary Canadians arose as a consequence of their belonging to a peace organization which the Security Service of the RCMP believed had been infiltrated by members of the Canadian Communist Party.

---

* A front group is defined as "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". Membership in a front group should not, however, be construed as knowledge of, agreement with, support of or adherence to the organization's covert objectives.

Although much of what was done then could be illegal now or, at the very least, "unreasonable or unnecessary" under the *CSIS Act* today, this activity was within the law at that time.

In order to collect such a great volume of information, the Security Service had many methods, but the most productive was the use of a large number of human sources within the peace movement. Though the avowed aim was always to monitor the activities of known Communists or Communist sympathizers (a very elastic term), the practical result was the accumulation of thousands of files on Canadians and groups of Canadians from all walks of life whose only common denominator was a link with the peace movement. Many of them simply wished to end the arms race or, at least, to prevent nuclear war.

Once this accumulation of information was underway, the process continued. Almost no evaluation or assessment was made of the information collected. Volumes of information were accumulated on Canadians whose motives did not seem to be suspect even to the Security Service itself. Apart from all other considerations, much of this activity was a clear waste of the RCMP's, and the nation's, resources.

The data became part of the large Security Service data base on counter-subversion. It was utilized whenever the Service prepared analyses relating to Soviet activity in Canada and security clearance assessments. Unfortunately that data base contained information on individuals who were of absolutely no security interest. Often, the analysis conducted was aimed more at justifying the continuation of surveillance of the peace groups than at providing meaningful intelligence. On the rare occasions when an evaluation of what was going on occurred, it was superficial and, in effect, a rationalization designed to justify continued activity along the same lines.

In 1984 the *CSIS Act* came into force, and these files were inherited by CSIS. They became part of the Service's "counter-subversion" holdings. CSIS reviewed all counter-subversion targets in an attempt to ensure that no groups or individuals continued to be targets unless they came within the specific provisions of the *Act*. But, it concluded that nearly all of the RCMP Security Service's targets fitted within what it saw as its mandate under the new *Act*.

Once again, the justification for collecting information remained the suspicion of foreign influence exerted either by Communists, Communist sympathizers or the many domestic or international groups identified by the Service or allied agencies, rightly or wrongly, as Soviet fronts. For nearly all targets, most of the information continued to come from human sources.

The only clear difference between the activities of the RCMP Security Service before July, 1984, and the CSIS approach under the new law was a diminution in the amount of material gathered. It is not evident that this was a conscious goal. It could have been due to the much increased emphasis on counter-terrorism and a consequent reduction in the resources available to the counter-subversion program. Whatever the reason, there was a welcome, if insufficient, reduction in the amount of information placed on files concerning the peace movement.

We have made our views clear before now, in our report on the counter-subversion program in CSIS, reviewed in our 1986-87 Annual Report. We pointed out that entire categories of persons were targeted without reference to the actual threats, if any, that they personally posed to the security of Canada. CSIS cast its counter-subversion net too widely, in our view. Insufficient account was taken of the harm that monitoring could do to the fundamental values of personal freedom and privacy.

A Change in 1988

As a result of our study on the counter-subversion program and consistent with the corrective action designed by the Independent Advisory Team headed by Gordon Osbaldeston and specific directives given by the then Solicitor General, the Honourable James Kelleher, significant changes were made early in 1988 in the approach CSIS took to files that had been under the Counter-subversion Branch, including peace movement files.

The branch was disbanded. Active investigation of most of its targets ceased and a few were reassigned to other branches. Remaining targets in the peace movement, coming within paragraph 2(b) of the *Act*, are now the responsibility of the Counter-intelligence Branch. A great many-investigative resources have been suspended or have been redirected to other targets. Tens of thousands of files have been cleansed, destroyed or segregated.

In early 1987, files held under the "counter-subversion" rubric numbered in the tens of thousands. About 2,400 were active at that time. Among them were files relating to the peace movement. By March, 1988, the number of active files was down to less than 100, of which fewer than half were in any way associated with the peace movement.

The criteria for an approved investigation involving foreign interference in or manipulation of peace groups or individuals have become infinitely more rigorous. The new rules require CSIS to look at targets associated with the peace movement through a keyhole rather than through the door that used to be wide open.

We believe that CSIS has made substantial and praiseworthy progress, albeit tardily, towards limiting its investigative activities to those which are clearly supportable under the mandate laid down by the *CSIS Act*. CSIS asserts that it is now attempting to limit its investigative activities to those persons who are Soviet conduits and who conduct covert activities within Canada on behalf of Moscow or who are witting agents of the Communist Party of the Soviet Union, carrying out Soviet policy initiatives in Canada.

At the direction of the Solicitor General, two explanatory telexes were sent by the Director to all CSIS regions in May and September of 1988 to clarify the essential elements of this much more limited approach. It appears that CSIS management is now making a determined effort to act reasonably as well as to stay strictly within the limits of the *Act*. We have no criticism on that score.

Yet we still have concerns about the practical results obtained from even the present, more limited, program. Our concern is that even though CSIS now looks through a keyhole rather than through an open door, it is still looking into the same room and in that room there are many Canadians who are not "Moscow dupes".

This unavoidable fact of life is compounded by the attitudes of some CSIS investigators, who have expressed to us concerns relating to the disappearance of the Counter-subversion Branch. They maintain that the new, much more restrictive, guidelines preclude them from collecting information which they still sincerely believe pertains to threats to the security of Canada. In particular, many CSIS officers believe that the new guidelines could deprive them of the data bank that until now has been used in investigations of security clearances.

This attitude stems in large part from a reluctance to change past practices in place since the Taschereau-Kellock Commission recommendations in 1946, but it is also a product of the lack of precision in the definition of a threat to the security of Canada found in paragraph 2(b) of the *CSIS Act*, which we address in Appendix A of the present annual report. This is the paragraph that is the basis for CSIS targeting in the peace movement. As we say in Appendix A, paragraph 2(b) is worded imprecisely. But it is also true that neither the Government nor the Service itself have yet made the intellectual effort necessary to clearly define exactly what this paragraph allows CSIS to do or forbids it from doing.

Many investigators still honestly believe that espousing the views of the Soviet Union, particularly if it is done in an apparently covert way, is *automatically* detrimental to Canadian interests and, therefore, targetable. It is by no means self-evident that every policy position taken by the Soviet Union, if adopted, would be detrimental to the interests of Canada. Some Soviet policies, obviously, would be detrimental to Canada. Others equally obviously, would not.

In the view of these investigators, however, anything that can be construed as reflecting Communist influence is, in itself, dangerous to the security of Canada. They believe that, depending on the shifting goals of Soviet foreign policy, Communists slip in and out of alliances with democratic movements. Even when these alliances appear least threatening,
these investigators are convinced that they are only manoeuvres designed to further the goals of their Soviet masters.

It is plain that more effort should be devoted to clarifying the meaning of paragraph 2(b) or to amending it if targets are to be limited to those which most Canadians could accept as being entirely reasonable. We make such recommendations in Appendix A.

We are concerned that this mindset on the part of some CSIS investigators may have been reflected in CSIS reports and evaluations which have been sent to other federal agencies.

In our 1987-88 Annual Report and in Chapter 3 of this report we dealt with the need for CSIS to improve its analysis and evaluation capability so as to deal with information in a well informed and intellectually rigorous manner. This requirement certainly applies in particular to its past and current reports on the peace movement. Through the Solicitor General we have urged that an internal CSIS review of current reports on peace groups take place with an objective appraisal of their continuing validity.

Our study raised another issue that has implications reaching beyond the peace movement to embrace the whole CSIS program. Despite the massive reduction in the number of authorized targets (active files) since March, 1988, information is still collected on Canadians who come into contact by accident or design with approved targets. This cannot be avoided. Information

on these Canadians is no longer put on files bearing their names. No files may now be opened by CSIS unless the subject of the file is designated as a target under the new stringent guidelines.

In the paper world of yesterday this would be sufficient. But in the electronic world of today, information gathered on Canadians in the process of investigating approved targets can be extracted from computer data banks at the touch of a few keys. In effect, the modern electronic world allows for the instant retrieval of a complete set of references to persons who are not, and who never were, targets. Although CSIS has some safeguards built into the system, this situation causes us serious concern.

We do not suggest that all this information should be erased from computer files. It is, after all, important to know whom a foreign agent, or a person acting on behalf of a foreign power, is contacting, how often, and why. However, we believe that the Solicitor General should direct CSIS to have its experts develop proposals for programming its computer system to exclude any possibility of information on non-targets being recovered from electronic files except under two specific conditions:

- when the person concerned becomes a target pursuant to the provisions of the *CSIS Act*; or
- when the person requires a security clearance from the government of Canada and, therefore, signs a consent form authorizing CSIS to conduct a full security assessment.

In all other circumstances, information gathered on non-targets should be unconditionally unobtainable by any person. These rules apply to information in the FBI's computer system in the United States. It should be possible to do the same thing in Canada.

Conclusions and Recommendations

Our inquiry has revealed that the Security Service of the RCMP cast far too wide a net with far too small a mesh in an attempt to catch "subversives", including members of the peace movement. It collected a great deal of information with little evaluation or analysis. Because its aim was vague and unfocused, enormous amounts of irrelevant information was accumulated on Canadians.

CSIS, in 1984, made a superficial and ineffective attempt to bring its procedures into line with the *CSIS Act*. At that time, it clearly did not succeed.

Finally, beginning in late 1987, all this started to change. Thousands of files were cleansed or destroyed, human sources were discontinued and the number of approved targets was drastically reduced to fewer than a tenth of the previous number.

But the process needs refinement. It is still true, and will always be unavoidably true, that some information on innocent Canadians will be collected during investigations of approved targets, no matter how few and how rigorously selected. We recommend that special, absolutely watertight, procedures be instituted by CSIS, upon the direction of the Solicitor General, to keep this information from being used except in the particular circumstances described earlier.

We also recommend that a special effort be made by the Government to clearly define what constitutes a "threat to the security of Canada" in the context of the peace movement. Clear guidelines should be provided to CSIS as soon as possible.

6. SCIENCE AND TECHNOLOGY

One of CSIS' responsibilities is to provide intelligence on clandestine, illegal transfers of goods and information to other countries. To the extent that such transfers are carried out by foreign intelligence officers, they can constitute "espionage" under section 2 of the *CSIS Act*.

Our interest as a Committee in the protection of scientific and technological assets is rooted in our ongoing oversight responsibilities. But it quickly became apparent in our inquiries that CSIS could not be assessed in isolation; it is only one of many agencies involved, so we inevitably had to delve into its relationships with other parts of the security intelligence community.

Canada is among the world's most technologically advanced nations. Spending over $7 billion a year on research and development, we have and use state-of-the-art technology in such areas as information processing, food production, the generation and transmission of power, transportation and the development of natural resources. We also benefit from the latest technology developed in friendly countries, notably the United States.

We share our know-how widely. Articles written by Canadian scientists on their latest discoveries are read worldwide. Canadian companies carry out remote sensing projects that help third-world countries exploit their mineral wealth. Canada exchanges students and researchers with many countries.

At the same time, we need to protect key scientific and technological secrets from the agents of foreign countries and from "technobandits"--freebooters, some of them Canadian, who are prepared to smuggle restricted goods out of the country for a quick buck.

In our inquiries we reviewed the system for safeguarding scientific and technological assets in Canada, relying primarily on structured interviews with federal officials involved in this area. We met with people from the Privy Council Office, Revenue Canada (Customs), the Department of External Affairs, the Royal Canadian Mounted Police, the Department of National Defence and Supply and Services Canada as well as with CSIS officials.

A Crowded Field

One of the first discoveries of the inquiry was that there is no central apparatus charged with all aspects of safeguarding Canada's scientific and technological assets, including both the enforcement and the intelligence production functions. What boundaries there are seem to be defined by the departments and agencies involved and COCOM (the Coordinating Committee for Multilateral Export Controls), described below.

Departments in this area function largely through coordinating committees of senior managers--the Intelligence Advisory Committee (IAC), chaired by the Deputy Clerk, Security and Intelligence, and Counsel (PCO), and the Security Advisory Committee (SAC) chaired by the Deputy Solicitor General.

Science and technology matters, like all others considered by the IAC, are first discussed by one of its several sub-committees. These sub-committees, known as Specialized Assessment Review Groups, are divided according to geographic region and thematic concerns.

One of them is devoted to S&T matters, producing reports written and considered by experts from the concerned departments.

The Canadian government "system" for protecting assets is limited to three components:

- Export control.
- The Visitors Panel and visa restrictions.
- Protection of classified facilities.

To some degree, CSIS activities support all three components of this system.

Two basic functions have been identified in the area of science and technology security. There is enforcement, which is largely the domain of Revenue Canada (Customs), the Department of External Affairs and the RCMP. They are responsible for physical protection and investigation.

The second function is intelligence production--estimating the threat to which science and technology assets are subjected so as to allow the appropriate government agencies to identify the goods, knowledge and installations that need protection and so as to assist in the detection of illicit efforts to acquire Canadian secrets. Not only CSIS but almost every government agency with an interest in science and technology gathers information and produces intelligence that could be relevant.

The System

COCOM is the Coordinating Committee for Multilateral Export Controls, which brings together 16 nations* to limit exports of sensitive goods to certain countries. Canadian exports regulated under the *Export and Import Permits Act*, administered by the Department of External Affairs. Revenue Canada (Customs) monitors exports. The RCMP and Customs investigate suspected offences.

Exchanges of students and researchers is one way that scientific and technological information crosses international boundaries. Nearly 3,000 students, scientists and delegates came to Canada in the first eight months of 1986 from the Soviet Union and East Bloc nations alone. The Visitors Panel is a committee of deputy ministers whose secretariat vets invitations from government and government-funded bodies to communist bloc students and scientists. The Panel itself is largely inactive.

As for the protection of classified installations, Supply and Services Canada, as well as the Department of National Defence and its Communications Security Establishment, work with industries that carry out classified contracts on behalf of the federal government, setting the security standards that must be met.

---

* Members are Belgium, Canada, Denmark, France, West Germany, Greece, Italy, Japan, the Netherlands, Norway, Portugal, Spain, Turkey, Luxembourg, the United Kingdom and the United States.

CSIS Operations

CSIS plays a role in all the activities we have described. It is a member of the Canadian delegation to COCOM and, with the RCMP and others, it contributes to the data base that Customs uses to monitor exports of sensitive goods. CSIS is advised through Employment and Immigration Canada's visa vetting system as well as by the secretariat of the Visitors Panel when students and researchers from some communist countries apply to come to Canada. It does security checks on employees of private sector firms carrying out secret work for the government.

But its principal activity in this area is to monitor the activities of foreign intelligence officers. Its mandate derives from the definition of "espionage" as a threat to the security of Canada (paragraph 2(a) of the *CSIS Act).*

The Threat

No one doubts that strenuous efforts are being made by some countries to close the technological gap, military and non-military, between themselves and countries of the Western alliance. Instances are known in which foreign intelligence officers have approached researchers at facilities where secret work was being done in Canada, and where pressure has been put on immigrants by the authorities in their countries of origin to obtain restricted technical manuals, where attempts have been made to smuggle restricted goods out of the country.

The United States itself, not Canada, is seen as the major target of foreign intelligence agencies that want secret American technology. However, Canada may become a more attractive target as the result of major defence projects such as the Canadian Patrol Frigate project. Then, too, there is Canadian participation in American high tech projects such as the space station program for which Canada is to provide the mobile servicing system.

We saw in our study that the government has access to a great deal of the information that it needs to safeguard the nation's scientific and technological secrets. For example, CSIS has records of every Level II and Level III (formerly known as SECRET or TOP SECRET) security clearance in industry, which allows it to identify installations where SECRET and TOP SECRET work is being done on a federal contract--or, to put it another way, prime espionage targets.

Recommendations

For security reasons, we will not comment publicly on our assessment of the present arrangements for safeguarding Canadian science and technology. This is a high-stakes area where any information is more helpful to foreign governments than it is to Canadians. However, we betray no secrets when we say that the present system can be improved. In April, 1989, we provided a report to the Solicitor General under section 54 of the *CSIS Act.* In the report, we recommended mechanisms for greater coordination over S&T related investigations within the Service, and among participating agencies. We further recommended that CSIS seek from the government a mandate to assign a higher priority to protection of S&T assets, and if necessary, seek additional resources. Lastly, we suggested that the government strengthen "intelligence analysis, research and policy development" in this area, perhaps by the creation of an organizational entity dedicated solely to these tasks.

7. INSIDE CSIS

The foregoing chapters have dealt with operations. In this chapter we turn to the Service's internal affairs.

Recruitment

After graduating just one class of new Intelligence Officers (IOs) from its Academy in 1988, CSIS made plans for three classes in 1989-90. This is a welcome sign that the Service is now fully committed to the idea that it is not enough to get IOs “off the sheif”, as it once seemed to want to do, by recruiting from police forces.

The credentials of the 1988 recruits and those chosen during the year under review for the first class of 1989-90 are impressive. Twenty-one of the 25 hold postgraduate degrees. Among their disciplines are law, political science, business administration, international affairs, philosophy, geography and modern languages. Six know at least one language besides French and English. Ranging in age up to 38, with an average of 30 in 1988 and 28 in the first class of 1989-90, some of the recruits have, as well, valuable experience of life that will enhance their contribution to the Service.

We are also pleased that room is being made at the Academy for "conversions"--that is, people entering the IO category from other jobs within CSIS. Knowing this door to advancement is open is a plus for staff morale.

That being said, we continue to stress the Service's need to recruit from the widest possible public. Relying on unsolicited applications leaves out many talented people who have perhaps never thought of a career in security intelligence. We are pleased that the Service now searches the Public Service Commission's professional inventory as well as its own "in-basket" for potential recruits. CSIS is planning newspaper advertising. We urge that it also join other government agencies and the corporations in sending recruiters to the university campuses.

Equitable Representation

In recruitment among groups that have long been underrepresented in the security intelligence community, the picture is mixed. With respect to people whose first official language is French, Table 2 shows that the Service continues to move in the right direction.

However, the trend is not so clearly encouraging with respect to women. We applauded last year when we learned that the 1988 class was half men, half women. In the first class of 1989-90, not quite a third are women. The Service's stated objective is to have equal or greater representation of women in each class, so we will be watching trends in this area.

Because of the well-known difficulties in assembling relevant statistics, we do not know how many Intelligence Officers are from native and "ethnic" communities. CSIS assures us that "recent initiatives have placed emphasis on the identification of candidates representative of the Canadian mosaic". In this it has our full support because of our belief that CSIS must be representative of the country in order to do its job effectively and sensitively.

Table 2. Composition of Classes at the CSIS Academy						
	Sex		First Official Language		Source*	
Year	Male	Female	English	French	Conversion	Outside
1986	50	17	58	9	14	53
1987	23	4	17	10	7	20
1988	4	8	6	6	3	9
1989**	9	4	6	7	2	11

* "Conversion" refers to recruitment of Intelligence Officers from other positions within CSIS while "outside" refers to recruitment of newcomers to the Service.

** Statistics reported here are for the first of three classes planned in 1989-90; the other two classes remained to be selected at the time of writing.

Source: CSIS

Bilingualism

The composition of the 1988 class and the first class of 1989 at the Academy shows encouraging evidence of a commitment to official bilingualism. All in these classes are bilingual at the B or C levels. None are unilingual or at the basic A level in their second official language.

Looking at official languages programs as a whole, we are pleased with the strides that CSIS has made. There are still weaknesses, of course. For example, as noted by the Commissioner of Official Languages in his latest annual report,* a spate of early retirements brought the proportion of managers whose first official language is French down to 18 per cent in 1988 from 23 per cent.

But--and the Commissioner recognizes this in his report--progress is continuing. The number of employees taking language training doubled from 1987 to 1988, reaching a level of 430. The percentage of bilingual investigators in the Ottawa Region rose to 42 per cent in 1988 from 33 per cent in 1987. A plan has been adopted to give the Ottawa Region office the capacity to operate fully in both languages within three years.

* From Act to Action: Annual Report 1988, the Commissioner of Official Languages (Ottawa, 1989), page 132.

It is a hopeful sign that the Commissioner received only 11 complaints against the Service in 1988--a very sharp drop from the 63 recorded in 1987 and the hundreds that sparked our own special study of official languages matters in the Service in 1986-87.

Staff Relations

We noted some positive moves towards better staff relations in 1988-89. One was the launch of an employee newsletter. In addition, wide circulation was given within the Service to a comprehensive Human Resources Management Plan. Both these developments are in the spirit of recommendations we made in *Closing the Gaps*, our special report on official languages and staff relations, issued in 1987. Since problems in staff relations are never entirely resolved we will continue to monitor problems as they are brought to our attention.

Polygraph Testing

Over the years, the Service's use of the polygraph in screening its own personnel has narrowed. By 1986-87, employees already on staff were no longer tested, even voluntarily. Then the "lifestyle" questions were dropped, so new applicants for Intelligence Officer positions are now tested only on "loyalty".

But the polygraph is still a long way from where we would like to see it--on the scrap heap. After continuing reviews of the available literature, we continue to oppose the use of polygraph testing as a tool in security screening, essentially because we do not think the acknowledged one-in-10 error rate is acceptable in light of the damage a negative result can do to individual reputations and careers.

We note that Prime Minister Thatcher announced on December 8, 1988, that the United Kingdom would not use the polygraph in security screening. She cited a study commissioned by her Government, which found "that the polygraph is probably incapable of achieving a high level of accuracy and reliability when used for screening purposes and, moreover, that individuals trained in the use of countermeasures would have a good chance of escaping detection".

Here in Canada, 1988-89 was a year of much activity but little action in government-wide consideration of the polygraph issue. Polygraph policy was discussed repeatedly but no final decisions were reached. It is now in the hands of the Security Advisory Committee (SAC), a subcommittee of the Interdepartmental Committee on Security and Intelligence. SAC has given a working group a mandate to draft standards covering who should be tested and how and what protections should be provided for individual rights.

Meanwhile, it has been agreed at the highest level of officials that the CSIS polygraph program should continue as a pilot project. This is the same language that was being used two years ago; we were told then that the polygraph program was a "pilot project". In the absence of any terms of reference for an objective study and of a methodology for evaluating results, our conclusion then was that CSIS was just trying to disguise its usual program by dressing it up in a lab coat. This time there are some signs that the Service intends to collect

and evaluate data in a serious way. Preliminary steps have been taken to engage an outside consultant to make a report in the next year. The use of an independent consultant could help reassure skeptics that the study is thorough and objective.

We stand by the recommendation we first made in our 1985-86 Annual Report and have repeated ever since: "that the use of polygraph examinations for employment and security clearance screening stop, at least until a thorough and objective study has been carried out and the Solicitor General and the Government have been able to reach conclusions about whether the use of such methods is compatible with the values of a free and democratic society".

Accommodations

With the move of the Montreal Region office at the end of 1988-89 into more efficient quarters of its own, separate from the RCMP's, the next priority is construction of a proper Headquarters building in Ottawa. Five years after the Service was created, Headquarters are still scattered over a number of buildings in Ottawa, adding to the difficulties that any large and complex organization faces at the best of times with internal communications. We are informed that a site has been chosen, architects selected and funds committed. We encourage the Government to proceed as quickly as possible with a good functional building.

Public Relations

We believe that CSIS deserves the respect of Canadians for the important work that it does. We have commented often on the difficult public relations problem that CSIS faces, unable for national security reasons to say much about its successes and faced with an array of critics, both official critics like ourselves and unofficial ones, at every sign of a problem.

So we are glad to see that the Director of CSIS is accepting a higher profile, meeting with the editorial boards of major newspapers and making some public appearances. We believe that the better CSIS is known, the more it will gain the respect that it needs to help it recruit the best and to secure the cooperation of Canadians in its important work.

8. COMPLAINTS

The last six chapters have dealt with our oversight role. Our other role is the investigation and bearing of complaints, and we now turn to it. Complaints can be broken down into two categories. First there are complaints about the denial of security clearances. This covers federal government employment and contracts under section 42 of the *CSIS Act*, immigration under sections 39 and 81 of the *Immigration Act, 1976*, and citizenship applications under section 19 of the *Citizenship Act*. Second, there are complaints that anyone can make under section 41 of the *CSIS Act* "with respect to any act or thing done by the Service" except those that can be dealt with under the staff grievance procedure.

In Chart 1 (page 48) we briefly sketch the process for section 41 complaints and in Chart 2 (page 49) the process for complaints about security clearances. There are a few significant differences. We always hold formal hearings on complaints about security clearances, but hearings are often dispensed with in section 41 complaints--when the facts emerge clearly from interviews with the people involved and the relevant documents. In addition, complainants cannot come to us under section 41 until they have taken up the matter with the Director of the Service.

The question of whether departments have the power to reject a SIRC recommendation on a security clearance under section 42 is still before the Federal Court of Appeal, in the Thomson case. Our view is that the *CSIS Act* should be amended to make SIRC recommendations binding. We also believe that where substantive rights are at stake, SIRC recommendations on section 41 complaints should be subject to judicial review by the Federal Court of Appeal. Both these points are discussed in Appendix A.

Complaints in 1988-89

We took in 55 new complaints in 1988-89, up from 38 in the previous year. While the number of citizenship and immigration reports fell to zero from one and two respectively in 1987-88, complaints under section 41 rose sharply to 44 from 34 and complaints about security clearances jumped to 11 from one in 1987-88.

The Department of National Defence accounts for nine of the new complaints about clearances. A large proportion of the new complaints under section 41 are about delays--six to 12 months in many cases and sometimes more--in immigration and citizenship proceedings. We can say that CSIS is not generally responsible for these delays. The Service's role in vetting citizenship applications is minimal in any case. Nor have we found unreasonable delays by CSIS in security checks on people coming into Canada although, as we note in Chapter 3 above, when checks with foreign services are required the Service is unable to control the timing.

We closed 44 cases in 1988-89. There were formal, written decisions in 14, and case histories can be found in Appendix D. In 30 cases there was no need for formal investigation and hearing because the issues raised were clearly beyond our jurisdiction or the complainants had not provided a strong enough factual base for us to conduct a full investigation.

Table 3. The Complaints Record, 1988-1989*				
	New complaints	**Carried over from 1987-88**	**Closed in 1988-89**	**Carried over to 1989-90**
Security clearances	11	1	6	6
CSIS	2	0	0	2
DND	9	1	6	4
Citizenship	0	4	1	3
Immigration	0	4	3	1
Section 41	44	4	34	14
Total	55	13	44	24

* This table covers the period to the end of June, 1989

CSIS Presentations

In security clearance cases, CSIS presentations at our hearings were far better in 1988-89 than ever before. The Service is involving its Legal Branch much more in the preparation of evidence and argument, so we are hearing fewer guesses and assumptions and more hard facts and logic.

We have also found it easier to come to agreements with CSIS on the amount of information that can be released to complainants. Our policy, based on sections 46 and 48 of the *CSIS Act,* is to let complainants know as much as possible about the evidence so they can attempt to meet the cases against them, but at the same time to protect national security. In past annual reports we have complained that CSIS was excessively secretive. We cannot, of course, promise that the Committee will never make the same complaint again. But we want to record that in 1988-89, at least, we have no occasion to.

Defence Department Clearances

Hearings during 1988-89 renewed concerns we have expressed before about the way the Department of National Defence (DND) carries out security clearance investigations and responds to complaints brought to us when clearances are denied.

DND is sometimes still too prone to act on unsubstantiated statements and half-truths. The facts uncovered in clearance investigations are often cast in the worst possible light. In one case, when a complainant asked a sergeant what he could do to improve the report on his security clearance, it was assumed that a bribe was being offered. We think this was a far-fetched inference.

Furthermore, the Department does not seem to recognize that people mature. Many young men and women find in the Forces a sturdy framework for well-ordered lives and productive careers. It seems unreasonable in these cases when they are denied security clearances because of youthful indiscretions that they have left behind. An example can be found in the case summaries in Appendix D (number 4).

It is a commonplace in the military that "the welfare of the rank and file comes first", but this was not always apparent at our hearings. It is dismaying to see a young member of the Forces at one of our hearings, unable to afford counsel, matching wits with the best that the Forces' legal and security machine can muster.

We have been urging since 1986 that departments ensure that their employees have appropriate assistance at our hearings. DND has taken no action, and we again urge it to act on our suggestion. Denial of a security clearance has most of the implications of conviction by a court martial in terms of future prospects. For this reason, we believe that the Judge Advocate should assign an officer to assist the complainant, just as must happen at courts martial.

Chart 1: Complaints Process under Section 41 of the CSIS Act

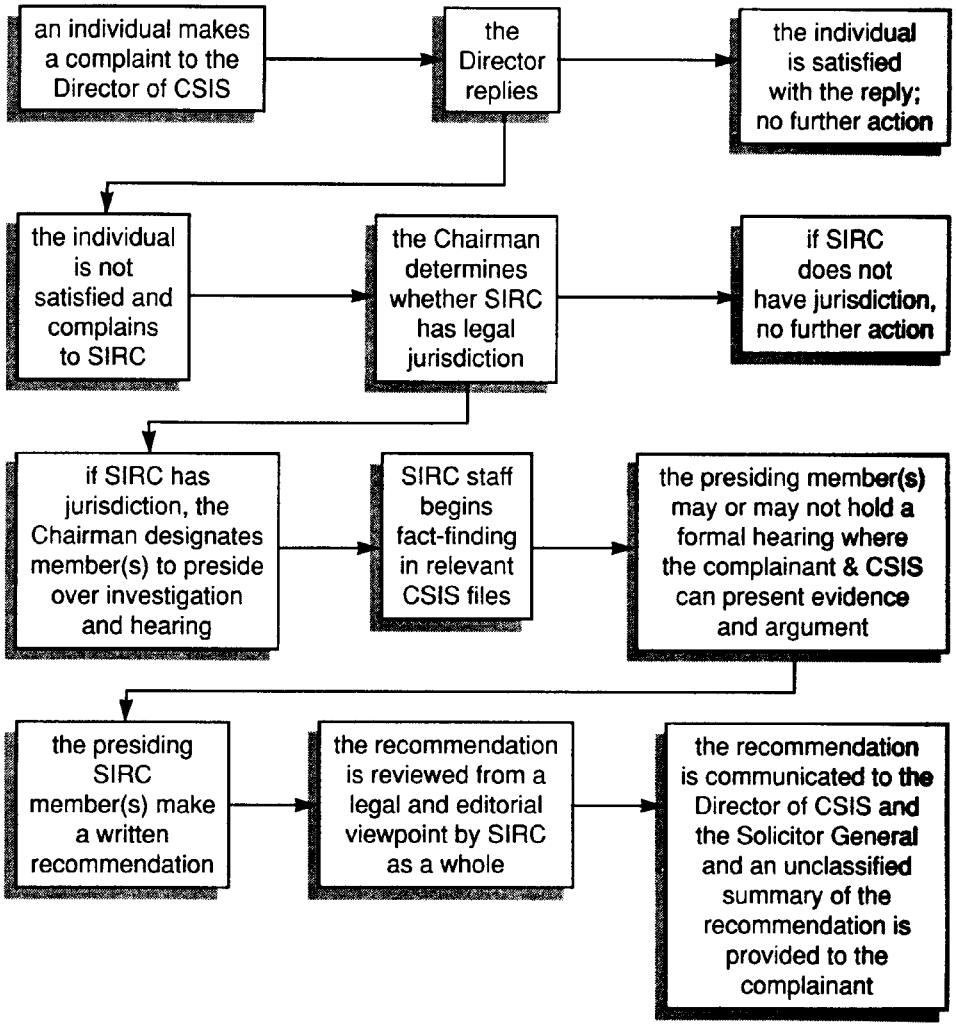
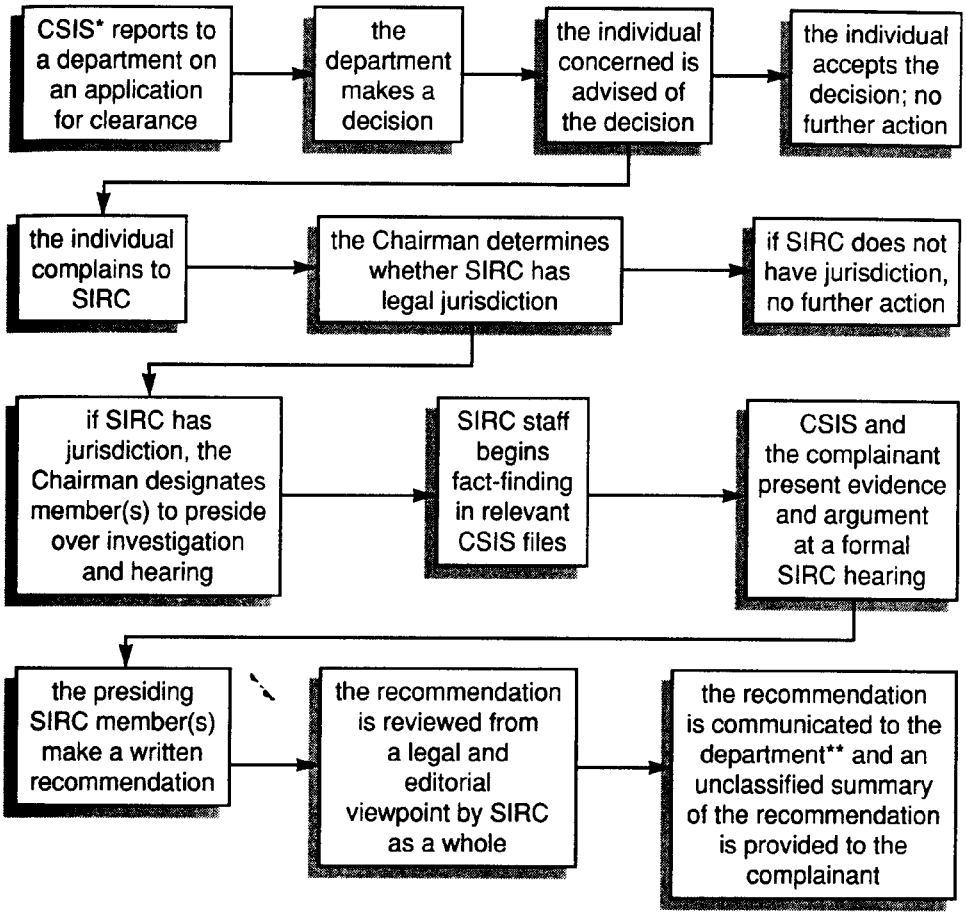


Chart 2: Process for Dealing With Complaints Respecting Security Clearances



* Complaints about Department of National Defence and RCMP clearances follow essentially the same process.

** As noted in the text, whether a SIRC recommendation can be rejected is being considered by the Federal Court of Appeal and we recommend that these recommendations be binding.

9. INSIDE SIRC

This chapter reviews activities that fall outside our core mandate of oversight and the investigation and hearing of complaints. Some are routine--matters of internal administration. Others involve our responsibility, within the boundaries set by national security considerations, to give Parliament and the public a window on security intelligence in Canada and to foster informed debate of security intelligence issues.

Reporting to Parliament

We appeared before the Standing Committee of the House of Commons on Justice and Solicitor General on April 14, 1988, at the very beginning of the year under review, to answer questions on our Annual Report for 1986-87.

Because of the autumn 1988 election campaign, our 1987-88 Annual Report was not tabled in Parliament until December 13, 1988 (although it was, of course, in the hands of the then Solicitor General by September 30, as required by the *CSIS Act).* Following the close of the 1988-89 fiscal year, we appeared before the Standing Committee on Justice and Solicitor General on May 30, 1989, to answer questions on our 1987-88 Annual Report and on our 1989-90 spending estimates.

We also held meetings in May, 1989, with the chairman of that Committee and with opposition party representatives on that Committee to discuss proposed arrangements for the five-year review of the *Act.*

Outreach

While Parliament is our principal audience, we address other publics as well. Through frequent contacts with the media and in speaking engagements, we try to make sure the *CSIS Act* and our role are well understood. Among speaking engagements:

- Ronald G. Atkey, the Chairman, participated in the 1989 Cambridge Lectures, sponsored by the Canadian Institute for Advanced Legal Studies, presenting a paper on the limitations that national security can place on freedom of expression.
- Mr. Atkey was a panellist when Phillip Knightley, author of *The Second Oldest Profession* and other works on security intelligence, was the guest of the Habourfront Authors Series in Toronto in the spring of 1989.
- Jean Jacques Blais addressed the 1988 annual conference of the Canadian Association for Security and Intelligence Studies (CASIS) on "The Political Accountability of Intelligence Agencies--Canada".
- Paule Gauthier addressed the 1988 Ditchley Foundation conference in England on "Oversight--the Canadian Experience". Mr. Atkey also took part in the discussions at the Ditchley Foundation conference.
- Saul M. Cherniack addressed the annual conference of the Canadian Rights and Liberties Federation in Regina on SIRC's role.

Like many others, we were also preoccupied in 1988-89 with preparations for the five-year review of the *Act*, due to begin in the second half of 1989. A number of scholars and lawyers generously--we paid no fees--responded to our invitation to meet with us in a seminar to help us fine-tune our thinking. They are listed in Appendix E. We want to say publicly what we have already told them privately--that we are very grateful for their help.

During 1988-89 we also made a commitment to help fund a CASIS conference in September, 1989, on the five-year review process.

The proceedings of a February, 1988, conference on "Advocacy, Protest and Dissent"--held at Queen's University and sponsored jointly by us and the Office of the Inspector General--have now been published.*

Administration

Our 1988-89 budget is set out in Table 4.

Table 4. SIRC Budget 1988-1989

Personnel		**$640,000**
Salaries and wages	$554,000	
Contributions to employee benefit plans	$86,000	
Goods and services		**$657,000**
Professional and special services	$503,000	
Other	$154,000	
Total operating expenditures		$1,297,000
Capital expenditures		$9,000
TOTAL		$1,306,000

Source: 1989-90 Estimates, Part III, figure 5

Our staff numbered 13 in 1988-89. It is headed by the executive secretary who directs day-to-day operations. Other members of the staff were the research director, two research officers and a research assistant, a senior complaints officer, an executive assistant who supports both the research and complaints functions, an administration officer who is also registrar of our investigations and hearings and coordinates our responsibilities under the *Access to Information Act and Privacy Act*, a records officer, a records clerk and two secretaries. One secretarial position was vacant at year's end.

* *Dissent and the State*, C.E.S. Franks, ed. (Oxford University Press, 1989).

As the year came to a close, we were making plans for a reorganization of the research branch, with a senior research officer assigned to counter-intelligence operations and a senior research officer assigned to counter-terrorism operations, both reporting directly to the executive secretary. The staff directory in Appendix F reflects the new scheme.

APPENDIX A

Amending the Act

A special eight-member committee of the House of Commons under the chairmanship of Blaine Thacker, M.P., has now been established to review the *CSIS Act* and also the *Security Offences Act.* The mandate of this all-party committee is very comprehensive. Through our proposals for amendments and our appearance before the committee we hope to contribute to its deliberations.

SIRC is Parliament's "watchdog" committee. In this appendix* we specify those areas of the *CSIS Act* which we think could be improved. Some of our suggestions have already been mentioned in last year's Annual Report. But this year we make specific recommendations for Parliamentary consideration.

Generally, we believe that the *CSIS Act* has worked quite well. Under its authority, the new security intelligence agency came into being in July, 1984. As we said in our 1987-88 Annual Report, we continue to believe that the appropriate model for Canada is the following:

> A civilian agency whose mandate is spelled out in law rather than by executive order, with clear political and judicial control, and with independent review.

That is, of course, exactly what the *CSIS Act* was designed to create. The following suggestions are meant to improve the working of the *Act*, not to modify its basic design.

The CSIS Mandate: "Threats to the Security of Canada"

Everything in the *CSIS Act* turns on the definition of "threats to the security of Canada" contained in section 2. During our term, we have become concerned about the scope and the wording of this provision.

Threats to the Security of Canada: paragraph 2(d) (Domestic Subversion)

In testimony to the Justice and Solicitor General Committee on December 17, 1987, the Chairman of SIRC, Ronald G. Atkey, speaking on our behalf, stated that the so-called counter-subversion mandate in paragraph 2(d) of the *CSIS Act* applied "regardless of how unlikely [the activities in question] are to lead to violent revolution". He added that "most of the investigations carried out by the [then] counter-subversion branch were authorized either because of the suspected involvement of hostile foreign intelligence services or because of a danger of politically motivated violence". In urging that the Counter-subversion Branch be disbanded, he indicated that the problem was one of proportionality.

---

* The substance of this appendix is reprinted from *Amending the CSIS Act*, the summary of proposals we prepared for use by the special committee and by others who intend to contribute to its work. We include it here for the convenience of readers of the Annual Report.

With the closing of this branch, and the decision of the Solicitor General that active investigations in the field of counter-subversion would require his personal authorization, we believe that it is now time to urge that this part of the mandate be reassessed. It is our conclusion, in light of the evolving experience with paragraph 2(d), that it should now be repealed. Such a repeal would, of course, involve repeal of paragraph 21(5)(a), which deals with paragraph 2(d) warrants, as a consequence. We realise that there can be a real threat to security posed in any democracy from domestic sources. But we believe that other parts of the mandate offer adequate protection to the security of Canada.

Additionally:

a) The present *CSIS Act* already distinguishes between paragraph 2(d) and other aspects of the mandate in providing a maximum time period of 60 days for judicial warrants granted under authority of this provision (paragraph 21(5)(a)). Therefore, the *Act* already recognizes that activities under paragraph 2(d) require special restrictions.

b) In our 1986-87 Annual Report (page 36), we noted that in counter-subversion, groups are targeted most often under the criteria of undue foreign influence or politically motivated violence. These fears are the concerns of other paragraphs in the section 2 mandate.

c) In 1987, the Solicitor General announced that the Counter-subversion Branch would be disbanded and that any retained files were to be transferred to the operational branches of the Service addressing the concerns noted in paragraph (b).

d) We note that last year there were no groups that were subject to investigation solely under paragraph 2(d) (1987-88 Annual Report, page 13).

e) The counter-subversion mandate has probably been criticized more than any other provision in the *CSIS Act*.

1. *We recommend*, therefore, that paragraphs 2(d) and 2](5)(a) be repealed.

Threats to the Security of Canada: paragraph 2(b) (Foreign Influenced Activities)

Paragraph 2(b) of the *CSIS Act* defines the following threat to the security of Canada:

> 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.

Before any activities fall within that definition, certain key characteristics must be present, four in Group A and four in Group B. They must be:

Group A

- foreign influenced;
- within or relating to Canada;
- clandestine or deceptive; and
- detrimental to the interests of Canada; or

Group B

- foreign influenced;
- within or relating to Canada;
- detrimental to the interests of Canada; and
- involve a threat to any person.

These requirements are conjunctive: all of them in Group A or Group B must be met before the Service can get involved. A final requirement must also be met, although it is expressed in the negative. As with the threats defined in paragraphs 2(a), (c), and (d), the Service can get involved with any "foreign influenced activities" that include "lawful advocacy, protest, or dissent" only if they are carried on in conjunction with any of the activities referred to in paragraphs (a) to (d). The key requirements listed above that help define the mandate of the Service are most ambiguous. They are not found in other Canadian legislation, and their use in the *ASIO Act* of Australia has also given rise to considerable controversy. We have had a great deal of experience with the mandate presently contained in paragraph 2(b), and we have concluded that it should be revised. The key requirements will be addressed in order.

Foreign Influenced. The phrase "foreign influenced" would cover foreign interest groups, political organizations, individuals, associations and corporations: any such groups or individuals are arguably "foreign" simply because they are not Canadian. The verb "influenced" was used rather than the narrower "directed" employed in the Cabinet Directive defining the mandate of the Security Service of the RCMP.

Within or Relating to Canada. At present, whether the activities are actually carried on in Canada, are directed from Canada, or are conducted or directed outside Canada, they need only be said to be "related" to Canada for the Service to satisfy the second requirement in paragraph 2(b). There are no criteria set out in the *Act* to help determine how much any particular activity must "relate" to Canada before CSIS can take jurisdiction. So long as there is some "reasonable connection" between the activity in question and Canada or its interests, this part of the requirement will be too easily met.

Clandestine or Deceptive. The basic notion of this characteristic relates to secrecy, concealment or threat. The precise meaning of the term "clandestine" is uncertain. It may connote an element of underhandedness or *male fides*, but some dictionary definitions would support an interpretation that merely "secret" activities may be "clandestine". To avoid any uncertainty, we propose that the term "clandestine" be repealed and replaced with a word like "surreptitious", which more clearly connotes some element of underbanded behaviour. The meaning of "deceptive" is clear; it seems to connote dishonesty in the sense that the person who is deceiving knows what he is doing or saying is false or intends to mislead by such falsehood. Where a foreign power "surreptitiously" or "deceptively" intrudes into Canadian national activities, the interference may be every bit as objectionable as espionage. The Service should be amply equipped to address this kind of interference in our national affairs.

Detrimental to the Interests of Canada. The most problematic part of paragraph 2(b) is the phrase "detrimental to the interests of Canada". It is not found in any other Canadian enactment. It is almost wholly subjective: no criteria are provided to offer any standard for determining what

is "detrimental". Although it is true that Canadian statutes routinely employ such phrases as "the national interest" or "the public interest", such formulations are deliberately used by Parliament when it wishes to confer maximum discretion upon some decision-maker. But this is hardly the kind of broad discretion that Parliament wished to grant to a security service which was required to maintain the principle of a "delicate balance" between the need to acquire information and an individual's right to privacy. The recent national debate on the merits of the Free Trade Agreement illustrates that even well-intentioned, patriotic citizens can differ strongly on what is in "the interests of Canada". We propose that the phrase "detrimental to the interests of Canada" be defined in the *Act.*

Involve a Threat to Any Person. There are fewer difficulties with this phrase, connoting as it does a genuine fear or apprehension of physical or psychological violence. Therefore, we propose only that the term "threat" be modified by an adjective like "serious". This was the step taken by Parliament in response to similar concerns voiced in the context of the mandate contained in paragraph 2(c), relating to politically motivated violence.

2. *We recommend* that paragraph 2(b) of the *CSIS Act* be repealed and replaced by the following:

"foreign directed activities within or directly relating to Canada that are surreptitious or deceptive and that are detrimental to the interests of Canada or involve a serious threat to any person".

Although this formulation of paragraph 2(b) is narrower, we believe that it will provide an adequate mandate for the Service. There is no attempt to limit the mandate to interference by "unfriendly nations" only. Nor does this formulation require that the interference occur in Canada--activities occurring in our embassies abroad would be covered, for example, so long as they are "directly" related to Canada. There is an implicit recognition in the proposal that foreign states may act through ostensible business organizations; consequently, the mandate would not be limited to actions conducted by foreign governments.

"Unwitting" agents of influence, if such agents in fact exist, could not be targeted by the Service under this paragraph. However, foreigners who attempt to "direct" such interference would clearly be subject to CSIS scrutiny. The addition of the modifier "serious" to threat is designed to limit the definition while still recognizing that the threat could occur either in Canada or abroad (such as a threat to a relative in one's homeland).

We believe most emphatically that the phrase "lawful advocacy, protest or dissent" must continue to limit this aspect of the Service's mandate as well as the entire definition of "threats to the security of Canada".

3. *We also recommend* that as precise a definition as possible of "detrimental to the interests of Canada" be included in the amended *CSIS Act.*

Drafting legal definitions is an arcane art and so we will not attempt to suggest a precise definition of the phrase "detrimental to the interests of Canada". We will, however, offer wording which could form the basis for discussion by individuals representing all points of view during the forthcoming Parliamentary hearings, as follows:

"detrimental to the interests of Canada" means activities which are foreign directed, are

surreptitious or deceptive, and are directed toward:

a) diminishing the sovereignty or territorial integrity of Canada,

b) weakening Canada's military defences,

c) harming Canada's international relations with any nation or organization,

d) seriously endangering the lives, health or safety of Canadians,

e) obtaining, illegally, or without proper authorization, any information or thing classified in the national interest by the Government of Canada, or

f) the bribery, coercion, or corruption of Canadians in respect of activities falling within paragraphs a), b), c), d) or e).

Overcoming Isolation

We note that the Independent Advisory Team which investigated the Service in 1987 (the Osbaldeston Committee) recommended that "the career paths of CSIS staff should provide for movement within both the security intelligence community and the public service" (page 17).

We believe that the Service's Analysis and Production Branch in particular would profit considerably if public servants from elsewhere in government, academics, or others with special expertise, could work with it. CSIS officers engaged in analysis and assessment also benefit by their ability to work in related agencies of government or universities.

Although we recognize that there would be a cost incurred in acquiring the extensive security clearances required by those who would rotate through the Service, we believe that the benefits would far outweigh the costs. CSIS believes that it already has the capacity to institute staff exchanges with the public service.

4. However, for greater certainty, *we recommend* that the *CSIS Act* be amended specifically to provide for the rotations by public servants and others with special qualifications through CSIS, subject to provisions that would safeguard the identity of employees engaged in the covert operational activities of the Service.

Grievance Procedures

Under the *CSIS Act*, SIRC cannot deal with complaints that are subject to grievance procedures set out in the *CSIS Act* or the *Public Service Staff Relations Act*. The *CSIS Act* contemplates that grievances might be adjudicated by members of the Public Service Staff Relations Board (PSSRB). In some cases, for example those involving salary matters and the like, SIRC would have little interest or particular competence in a dispute before the PSSRB. However, in many other situations, SIRC might be vitally interested. For example, a grievance involving alleged insubordination could arise if a member of the Service were to disagree strongly with how the Service was complying with a ministerial direction in a sensitive area.

5. Therefore, *we recommend* that CSIS be required to give timely notice to SIRC in advance of all grievance hearings that are conducted pursuant to subsection 8(3) of *the CSIS Act*.

SIRC should be entitled to be briefed in advance by the Service and to attend any grievance hearing. In this way, SIRC may better determine whether issues arising in a labour relations context merit independent investigation in the discharge of SIRC's separate responsibilities.

Warrants

The *CSIS Act* does not give SIRC any specific authority with respect to warrants. However, we have reported on warrants pursuant to our general duty to ensure that there is no "unreasonable or unnecessary use by the Service of any of its powers" (section 40) and our responsibility to "compile and analyze statistics on the operational activities of the Service" (subparagraph 38(a)(vii)).

In testimony to the Justice and Solicitor General Committee on November 20, 1986, Mr. Atkey discussed the fact that there was less statistical information concerning warrants available under the *CSIS Act* than had been available under the *Official Secrets Act*. He indicated his belief that parliamentarians are entitled to more of such information. Another member of the Committee, Jean Jacques Blais, noted that since it was the role of the Committee to review warrant affidavits and their concordance with the materials upon which they were based, SIRC will be in a position, eventually, to give broad assurances to Canadians that the *Act* is being followed. In our three most recent Annual Reports (1985-86, page 18-19; 1986-87, page 11, and 1987-88, pages 19 and 59) we have expressed our concerns about this matter.

Under the *Official Secrets Act*, generally, each warrant authorized only one covert technique against only one target, whereas one warrant under the *CSIS Act* can authorize the use of many powers against many targets. We do not think that aggregate warrant statistics under the present legislation are very helpful. Serious concerns about Canadians' privacy rights under the *Canadian Charter of Rights and Freedoms* prompt the following recommendation.

6. *We recommend* that the *Act* be amended to provide specifically that SIRC have the responsibility to compile and analyze warrant statistics and that SIRC be required to publish annually statistics containing the number of Canadian citizens or landed immigrants who have been affected by surveillance powers granted to the Service under judicial warrants.

We have often raised the issue of emergency warrants (1985-86 Annual Report, page 44; 1986-87 Annual Report, page 12; 1987-88 Annual Report, page 57). The elaborate procedures for obtaining a warrant that are currently in place offer important safeguards. But we are concerned that it might take too long in an emergency to obtain a warrant if the regular procedures are followed. Under the *Official Secrets Act*, warrants could be obtained within about three hours.

7. *We recommend* that section 21 of the *CSIS Act* be amended so as to permit the Director of the Service, with the agreement of the Solicitor General in each case, to issue a short-term, non-renewable warrant that would require an application to the Federal Court within 96 hours. There should also be the stipulation that SIRC must be notified within one week of the application.

Still in the area of warrants, we have also raised the issue of solicitor-client communications (1986-87 Annual Report, pages 19-20; 1987-88 Annual Report, page 58). Such communications are being protected by warrant conditions prohibiting interception of communications at the office or residence of the lawyer, or at any other place normally used by the lawyer to consult with clients. Furthermore, the interception of calls between a target and his or her lawyer are limited to calls that the Director or a regional director general have determined relate to the threat specified in the warrant.

We are pleased that such conditions are routinely included in warrants, but would prefer that such safeguards be enshrined in legislation. The *Criminal Code,* for example, explicitly protects solicitor-client communications. Of course, we recognize that terrorists or other groups whose activities constitute threats to the security of Canada may include lawyers in their number. Our concern is limited to communications with lawyers that fall clearly within the solicitor-client description. Our proposals would pertain solely to lawyers who are acting in their capacity as legal counsel.

8. *We recommend* that a section be added to Part II of the *CSIS Act* to provide statutory protection to solicitor-client communications.

9. Further, *we recommend* that another section be added to Part II of the *CSIS Act* listing warrant limitations that shall be considered by Federal Court judges.

Devil's Advocate (Amicus Curiae)

Since 1987, a Department of Justice lawyer, responsible to the Deputy Solicitor General, has appeared at the Warrant Review Committee as "devil's advocate".* But this official is exercising a more limited mandate than we intended when we first proposed a devil's advocate, in our 1986-87 Annual Report (page 9).

At present, the devil's advocate does no more than ensure that the information CSIS intends to cite in a warrant application is accurate. We had in mind, rather, someone who would challenge the need for a warrant at all--someone to make the case that the proposed target (who does not, of course, even know a warrant is being sought) might make.

We are also concerned about the location of the devil's advocate's intervention in the process. Sitting on the Service's internal Warrant Review Committee, the devil's advocate can too easily be perceived as a mere token at best, an insider at worst. We believe that the devil's advocate should appear before the Federal Court itself.

Therefore, although the warrant application system seems to be working much better than before, we believe that considerations involving the appearance as well as the substance of natural justice prompt reform in this context.

9. *We recommend* that Part II of the *CSIS Act* be amended to add a section requiring that a "devil's advocate", appointed by the Court, appear at each Federal Court hearing at which a judicial warrant is sought.

---

* By devil's advocate we mean an official appointed to argue a point of view, with which he or she may or may not personally agree, for the purpose of ensuring that all aspects of a matter are fully considered.

10. *We further recommend* that where possible this lawyer not be a government lawyer, but be drawn from a list of security-cleared outside counsel.

For example, SIRC has a roster of such lawyers (see Appendix B of this Report). To avoid any conflicts of interest, these lawyers could be appointed in alphabetical order or on some other random basis. The total number of new warrants and renewed warrants each year has fallen significantly, so this practice would not appear to represent a serious drain on resources.

Cabinet Decisions

Our current inability to see Cabinet decisions that affect CSIS has proved to be a problem in one instance we know of. During 1988-89, we were refused access to the Service's Multi-Year Operational Plan (MYOP) because it is prepared for submission to Treasury Board, a committee of Cabinet. In this instance, a compromise was reached: while the MYOP document itself was withheld, we were given the information it contains.

We have received assurances from the Ministry of the Solicitor General that cabinet decisions will be re-written and passed to CSIS as ministerial direction, which we automatically receive pursuant to subsection 6(2) of the *CSIS Act*. However, we have no way of knowing whether this procedure is foolproof or whether future Solicitors General would agree to continue the practice.

As we stated in our 1987-88 Annual Report, those of us who have been members of cabinets cannot understand why the statute would preclude the Committee from seeing cabinet decisions relating to CSIS operations. In our view, current arrangements create unnecessary public suspicion.

We recognize, of course, that we should not have access to records which would reveal the cabinet's decision making process. However, cabinet decisions are the executive authority used by all departments and agencies to justify their activities. It is essential that SIRC have access to cabinet documents directed or related to CSIS if it is to be in a position to review CSIS' performance of its duties and functions. Therefore, we believe that any cabinet decisions in CSIS' possession which relate to its duties, functions, or resources should be available to the Committee. Similarly, any memoranda to cabinet prepared by or about the Service should be available. Obviously, members of the Review Committee would be enjoined from revealing the content of confidences of cabinet to third parties; they are Privy Councillors and are bound by the same oath as are all past and present members of cabinet.

10. *We recommend* that subsection 39(3) of the *CSIS Act* be repealed, thereby permitting the Security Intelligence Review Committee to have access to all information under the control of the Service, regardless of its source.

Parliament might also consider amending subsection 31(2) so as to allow the Inspector General access to all information under the control of the Service, including confidences of cabinet.

Financial Review

In the past, the Auditor General audited the Security Service of the RCMP and, since he has a responsibility to verify how all money derived from the Consolidated Revenue Fund is spent, he has a statutory duty to audit CSIS as well. His auditors all have the requisite degree of security clearance to do the job. Now that the recommendations of the Osbaldeston Committee have been implemented, we think that it would be timely for a system audit of the Service to be conducted. We think it highly desirable for the Committee to have an element of responsibility for such an audit, given its understanding of the operational aspects of the Service's mandate.

Under section 38 of the *CSIS Act*, no specific authority is conferred upon SIRC to assess the Service's financial performance; however, the Committee may "review generally the performance by the Service of its duties and functions". The Committee believes that this power is technically sufficient to enable it to assess the Service's financial management.

11. Nevertheless, and out of an abundance of caution, *we recommend* that a subparagraph be added to section 38 of the *Act* to indicate clearly that the Security Intelligence Review Committee has the authority to undertake financial reviews of the Service in cooperation with the Auditor General.

"Whistleblowers"

Many governments have recently attempted to remove potential obstacles to public officials who wish to expose activities that they think are wrong. There is a so-called "Whistleblowers' Protection Act" in the United States *(Civil Service Reform Act, 1978,* 5 U.S.C. s.7701 *et seq.).* Similar reform is proposed in Ontario, and protection for "whistleblowers" is found in such recent federal legislation as the *Canadian Environmental Protection Act* (s.58(4) of that *Act,* being S.C. 1988, c.22). As we noted in our 1987-88 Annual Report (page 59), in the United Kingdom, a special official takes "leaks" from members of M15, who are not required to identify themselves.

Under the *CSIS Act,* there is no protection from disciplinary measures provided to employees of the Service who expose perceived wrongdoing to the Committee. Indeed, complainants must first make their concerns known to the Director, who may be precisely the person that the employee wishes to avoid.

14. Accordingly, *we recommend* that the *CSIS Act* be amended by adding subsection (3) to section 41 to guarantee anonymity to CSIS employees who complain to SIRC, and to guarantee that if such complainants are eventually identified, they will not face any disciplinary measures solely by reason of making such complaints.

Complaints Hearings

Under the *CSIS Act,* SIRC hearings must be conducted in private. Under subsection 48(2) of the *Act,* no one is entitled as of right to be present when representations are made to the Committee by any other person. In 1985, the Committee adopted quite elaborate rules of procedure in relation to the investigation of complaints made to it. Separate procedures have been prepared for complaints involving the denial of security clearances in employment, and in immigration and citizenship matters. These procedures were adopted by the Committee pursuant to its right to do so under subsection 39(l) of the *Act.* The extensive procedural safeguards that

the Committee has generated and distributed to the public are in marked contrast to the often abbreviated process that applies, for example, before a deputy head of a government institution reaches a decision to deny a security clearance. SIRC's investigations typically are very extensive and the hearing that is often held usually resembles a formal adjudication held by an administrative tribunal exercising quasi-judicial powers.

When public knowledge of evidence about to be adduced might be injurious to national security, perhaps because it would reveal sources or otherwise constitute a "threat to the security of Canada", complainants and their counsel are excluded while the evidence is heard by the Committee. There have been several challenges initiated in the Federal Court questioning the Committee's procedures in hearing complaints. So far, none of these challenges has succeeded and SIRC's rules of procedures and underlying practices have "passed muster" when measured against the *Charter of Rights and Freedoms* and the requirements of procedural fairness. Obviously, SIRC must abide by the outcome of any litigation that is not yet completed.

In oral hearings, it is in the discretion of the member hearing the case to determine whether or not a party should be excluded while testimony is given by another party. SIRC has evolved a procedure by which the counsel and the excluded party (usually the complainant) are then brought back into the room and given the gist of the evidence, without disclosing the national security information. They are then allowed to ask questions, and, where possible, cross-examine, on the basis of this summary.

We believe that the role now played by counsel to the Committee under our rules of procedure has proven to be quite fair and effective in this context. During complaint hearings when parties are excluded, Committee counsel is specifically instructed to ask Service witnesses the kinds of questions that one would expect the complainant's counsel to ask and to cross-examine with equal vigour. The summary of evidence that is later provided to the excluded party is usually negotiated by counsel for CSIS and SIRC under the supervision of the presiding member. What flows to complainants and their counsel is sufficient information to enable them to be as fully informed as possible of the case against them.

Only one problem has arisen with the present wording of the *Act* respecting investigations. Subsection 48(2) states:

> 48(2) In the course of an investigation of a complaint under this Part by the Review Committee, the complainant, deputy head concerned and the Director shall be given an opportunity to make representations to the Review Committee, to present evidence and to be heard personally or by counsel, but no one is entitled as of right to or present during, to have access to or to comment on representations made to the Review Committee by any other person.

It has been asserted that since the subsection can be read as denying access to "representations" only, it does not deny access to the presentation of evidence or the personal appearance by any other person. Such an interpretation, if upheld by the courts, would make Committee investigations dealing with classified national security matters all but impossible.

We do not believe that this assertion is well-founded. However, it would be useful to reword subsection 48(2) to clarify its intent.

12. *We recommend*, therefore, that the words "evidence adduced, or statements made" be added to subsection 48(2) so that it provides:

... but no one is entitled as of right to be present during, to have access to or to comment on representations made, evidence adduced, or statements made to the Review Committee by any other person.

Security Clearances

Without a security clearance, many employment opportunities--both in the public and private sectors--are effectively lost. The *CSIS Act* allows only some affected persons to complain to the Committee (s. 42).

First, the person must have been denied employment, dismissed, demoted or transferred, or denied a promotion or a transfer in government or else be refused a contract to supply goods and services to government for the same reason. As we noted in our 1987-88 Annual Report (page 56), the present wording means that when a person is fired or not hired by a contractor in order to remove an obstacle to doing business with government, he or she has no effective redress. In addition, where certain activities require the use of federal facilities, such as airports, which are denied to individuals lacking a security clearance, some persons will be unemployable. They too have no right to complain to the Committee.

Second, the decision to deny a security clearance must be one taken by a "deputy head".

Third, the right to complain at all is predicated upon a denial. This term may be narrowly interpreted to mean that only an outright refusal will trigger the statutory right. What happens if the authorities delay unreasonably, but never get around to a formal denial? At present, the individual concerned can complain to the Review Committee pursuant to the procedures specified in section 41, but more protection against such delay may be needed in the *Act*.

Fourth, the *Act* refers to a loss of employment opportunity "by reason *only* of the denial of a security clearance". What happens if the employer can honestly say that there were other reasons, albeit very secondary ones? This particular point has been cited on at least two occasions in challenges to the Committee's jurisdiction to investigate a complaint.

We believe that the right to complain to the Review Committee should be available to anyone who is denied a security clearance. There should not be categories of Canadians or landed immigrants who do not have the right to complain to SIRC when they are denied a security clearance, while others have the right to a full investigation by the Committee. It is a fact of life in the modern world that the denial of a security clearance usually has an immediate effect on an individual's employment; it always has a long term effect on the individual's employment potential.

In any event, above and beyond the serious effects on employment, no Canadian or landed immigrant should be put in the position of having his or her loyalty questioned to such an

extent that a security clearance is refused without having an automatic right to request an investigation by the Review Committee.

Often, individuals are denied *any* level of security clearance, but in some circumstances individuals who require a TOP SECRET clearance for their employment are granted only a SECRET or CONFIDENTIAL level of security clearance. This usually has the same effect on the individual's employment as an outright denial of any level of security clearance would have had.

The amendments we propose would provide the right to an investigation by the Review Committee to any Canadian or landed immigrant denied a security clearance at the level required.

16. We recommend that subsections 42(l) and (2) be repealed and replaced by:

> "42(l) When a security clearance, required by the Government of Canada for an individual for any purpose, is denied or is granted at a lower level than that required or is downgraded to a lower level than that required, the deputy head or other person making that decision shall send, within ten days after the decision is made, a notice informing the individual of the denial of a security clearance at the required level, and of the individual's right under this section to complain to the Security Intelligence Review Committee."

The remainder of section 42 would require minor consequential amendments.

Effect of Committee Recommendations about Complaints

At present, the Thomson case is again before the Federal Court of Canada. There is a disagreement between the Appeal and Trial Divisions of that Court as to whether the Committee's recommendations on security clearances should be binding upon deputy heads. Regardless of the eventual outcome of this case, Parliament may wish to clarify its intent during the five-year review of the *CSIS Act.*

We note that in Australia's *ASIO Act,* the "findings" of the Security Appeals Tribunal must be treated as "superseding" the original security clearance (s. 61).

We believe that it would in no way violate conventions of ministerial responsibility if Parliament decided to empower the Security Intelligence Review Committee to make final determinations in those cases where it disagrees with a decision of a deputy head to deny a security clearance. Decisions that determine whether an individual may work in a chosen field directly affect the rights of individuals. To be vindicated before a neutral tribunal like SIRC, only to learn later that a security clearance has still been denied by a deputy head in his or her absolute discretion must be deeply disturbing.

Finally, the new Government Security Policy (GSP) of June, 1986, specifies that the Security Intelligence Review Committee constitutes the redress procedure for all public servants who are denied a security clearance. We believe that the clear implication of these arrangements is that SIRC has decision-making powers.

17. Therefore, *we recommend* that subsection 52(2) of the *Act* be amended to provide that Committee rulings in respect of security clearances are final and binding upon a deputy head.

Access to Information and Privacy

In the normal course of events, the powers of the Security Intelligence Review Committee will almost certainly overlap with the separate powers exercised by the Information Commissioner or the Privacy Commissioner. This has already occurred with respect to the Privacy Commissioner.

In investigating complaints under the *Access to Information Act* or the *Privacy Act*, either Commissioner may have entered into negotiations with the Service, perhaps with respect to the same records that the Committee wishes to inspect in the discharge of its separate statutory responsibilities. The Committee believes that access by either Commissioner should not be hampered because of a parallel SIRC investigation or vice versa. Each independent agency has its own statutory responsibility to discharge. Though we believe that the present wording of the *Act* amply provides for SIRC access under any and all circumstances, some government authorities are not entirely convinced of this.

18. Therefore, *we recommend* that Parliament consider the advisability of clarifying this issue by adding a paragraph to subsection 39(2) of the *CSIS Act* specifying that the Committee is entitled to have access to any information under the control of the Service, notwithstanding the existence of any investigations that may be undertaken by the Information Commissioner or Privacy Commissioner.

The Canada Evidence Act--I

In testimony to the Justice and Solicitor General Committee on November 20, 1986, the Chairman replied to a question regarding section 37 of the *Canada Evidence Act*. Under this section, a member of CSIS can curtail testimony in criminal trials. This practice has been much criticized and Mr. Atkey reported that "there is discomfort within the Service with the particular wording and operation of that section... I think this is a problem area" (page 2:16). He then suggested that this was a good topic for consideration during the parliamentary review of the *CSIS Act.* He agreed that it was "a terribly awkward procedure... [and that there was] a potential for prejudice to the accused in a criminal trial". However, SIRC fully appreciates why any security intelligence service would struggle to keep its sources and "tradecraft" secret. We agree that CSIS intelligence should only rarely be used as evidence in court proceedings. However, it must be recognized that there will be exceptions and procedures should be available to protect the national interest when that happens.

In our 1986-87 Annual Report (page 25-26), we noted that in section 486 of the *Criminal Code*, the public may be excluded from courtrooms for various reasons that are listed.

19. In that light, *we recommend* that section 486 of the *Criminal Code* be amended

a) to add the phrase "threats to the security of Canada, as defined in section 2 of the *CSIS Act"* so that the judge would have the power to exclude the public from portions of

trials where national security matters might foreseeably be raised; and

b) to allow a judge to exclude the defendant and counsel as well as the public when security matters were raised.

The Canada Evidence Act--II

Until the enactment of amendments to the *Canada Evidence Act* in the early eighties, the Solicitor General could sign a certificate to the effect that the disclosure of certain information would be injurious to national security. The minister's certificate was final and completely unassailable before any court.

Section 38 now provides a means by which the written or oral objections to evidence on national security grounds may be reviewed. The review may be carried out by the Chief Justice of the Federal Court or by a judge designated by him or her. In other words, the review of the evidence in question can only be carried out by one specified person or the nominee of that person, and the hearing must be carried out *in camera* and in the National Capital Region.

This process was designed to enhance the rights of individuals involved in criminal cases before the courts. However, these rules have caused problems in certain situations arising after the Review Committee was created in July, 1984.

Review Committee recommendations/decisions are sometimes challenged before the Federal Court of Appeal under section 28 of the *Federal Court Act.* When this occurs, special direction must be obtained from the Court to protect national security documents which would normally be made public if the usual rules were followed. In addition, when the Department of Justice objects to the disclosure of national security information to the appellant, the Court must then await a ruling from a judge designated by the Chief Justice as to the validity of the "national security" objection. This ruling by the designated justice can be appealed to the Federal Court of Appeal, and Appeal Court justices can then examine the documents in question. Ironically, however, without an appeal in the face of a ruling in favour of the Crown by the designated judge, the Appeal Court cannot examine the documents.

This complex process takes place as part of a procedure whose purpose is to review the Review Committee's recommendation/decision following an investigation. Such an investigation by the Review Committee examines all documents, whatever their classification, and hears oral evidence regardless of its "national security" sensitivity. All classified evidence is withheld from the complainant during a Review Committee investigation.

Since the Review Committee's recommendation/decision is very often based, for the most part, on "national security" evidence, any court charged with reviewing the Review Committee's conclusions and procedures could only do so effectively if it also had access to all the evidence considered by the Review Committee.

20. Accordingly, *we recommend* that the *CSIS Act* be amended to provide, in the event of judicial review, that the Federal Court of Appeal have exclusive jurisdiction under s. 28 of the *Federal Court Act*, and be entitled to review any Review Committee report

rendered pursuant to section 42 or any report affecting the rights of an individual rendered pursuant to section 41, together with all relevant documents.

21. *We further recommend* that special procedures be authorized either by statute or by regulations to enable Review Committee files and documents to be transferred to the Federal Court of Appeal without the nature of those documents being made public, and, where necessary, without even the existence or absence of such files being acknowledged.

Acceptance of these recommendations would have the beneficial side-effect of eliminating any requirement for an individual to challenge a Review Committee ruling under section 18 of the *Federal Court Act.* This procedure is unfair at present because the individual concerned usually knows very little indeed of the case made against him and has very little chance of being able to construct an adequate application for judicial review. The practical effect of the present procedure is to deprive most individuals who complain under section 41 of the *CSIS Act* of the right to challenge a Review Committee report effectively.

The Framework of Accountability

After five years of experience, the Committee has formed strong opinions on whether the institutions now set out in the *Act* are effective and necessary. In our unique Canadian model, the Solicitor General, accountable to Parliament, is ultimately responsible for the Service. Under the *Act,* there is also a full-time "insider" in the Inspector General, who is "the Minister's person" and assists him in carrying out his responsibility for CSIS. SIRC completes the picture. It is a part-time, tri-partisan committee, independent of the government of the day. In our view, the combination of a tri-partisan group of part-time Privy Councillors found in SIRC has worked well. Consensus has usually been achieved and partisanship has been minimized. Another advantage is that as compared to the experience with oversight bodies elsewhere, "leaks" have not been a problem.

22. *We recommend* that the *CSIS Act* retain the Security Intelligence Review Cornmittee with its present jurisdiction.

The alternative, of course, is to provide for a standing committee of Parliament to oversee CSIS. There are two such committees in the Congress of the United States. In Australia, Parliamentarians were recently appointed to the Parliamentary Joint Committee on the Australian Security Intelligence Organization; however that Committee is somewhat limited in gaining complete access to documents held by ASIO. Moreover, the McDonald Commission recommended a joint parliamentary oversight committee. Nevertheless, we think that the experiment with SIRC has proven successful and propose that the Committee be retained in a revamped *CSIS Act* as the principal oversight body. In urging this continued role for SIRC, we would make a related recommendation.

23. We recommend that the *CSIS Act* contain a provision requiring the Director of the Service to offer to consult regularly with the leaders of the major opposition parties represented in Parliament, in order to keep them informed on matters relating to security.

This kind of provision is found in the *ASIO Act (s.2*1) and, to our knowledge, has worked well. It would strengthen the role of Parliament in the chain of accountability.

Should SIRC be empowered to review the activities of all the other institutions that comprise the Canadian intelligence community? In Appendix C of our 1987-88 Annual Report, we outlined the main constituents of Canada's intelligence network. In testimony to the Justice and Solicitor General Committee on June 3, 1986, Mr. Atkey stated that "this was an issue that Parliament should address at some time" (page 21:25). Mr. Atkey did not discuss whether such expanded oversight duties should be conferred upon SIRC.

Australian legislation provides for an independent oversight body for the entire Australian security intelligence community. The Office of the Inspector General of Intelligence and Security is responsible for "oversight and review of the compliance with the law by, and the propriety of particular activities of, Australian intelligence or security agencies" *(The Inspector General of Intelligence and Security Act*, 1986, section 4). This Office oversees the Australian counterparts to CSIS, the Communications Security Establishment, the Office of National Assessments, and the directorates of intelligence and security in the Department of National Defence, as well as ASIS, Australia's counterpart to the CIA.

In the United States, of course, the situation is similar to that in Australia: all intelligence agencies are subject to review and oversight by Congressional committees.

The McDonald Commission recommended that the review body it proposed should cover all federal agencies engaged in the clandestine collection of intelligence, except for the RCMP. (Recently, the RCMP admitted to the formation of a National Security Investigation Section (NSIS). There seems to be no obvious reason why this organization should not also be subject to external review.) Its report suggested that unless the review body was given this broader jurisdiction, "it would be all too easy for a government to evade its scrutiny by *de facto* transfers of responsibilities from the security intelligence agency to some other organization which is not subject to its review" (McDonald Commission Report, Volume 2, page 885).

We observe that there is still no review mechanism in place for the balance of the Canadian intelligence community apart from ministerial responsibility. Of course, if Parliament were to accept our recommendation to establish an Intelligence Assessment Office (see page 72), all Canadian intelligence agencies would benefit from the resulting "quality control" which would be exercised by such a body. But such quality control would not be the equivalent of a system of review. We believe that it would be appropriate for Canada to follow the Australian and American practice by instituting, in line with the McDonald Commission's recommendations, a system of review for all federal agencies engaged in the collection of intelligence.

24. *We recommend* that Parliament consider enacting legislation to provide for the independent monitoring of other institutions within Canada's intelligence network.

We have no strong view as to whether this responsibility could be assumed by an expanded SIRC or some other independent body established for this purpose.

Intelligence: Balancing Supply and Demand

Especially at a time when sound financial management is at the forefront of the public's attention, Parliamentarians will be particularly interested in assessing the cost-effectiveness of the Service. As an intelligence agency, is CSIS gathering and analyzing information effectively and then transforming it into useful "intelligence"? SIRC defines "security intelligence" as "the collection, from both open and covert sources, and analysis of information which provides advance warning and advice about activities which may constitute a threat to the security of Canada".

There are two major categories of intelligence: security intelligence which can originate at home or abroad but which deals with threats to the security of Canada, and foreign intelligence which deals with information about other countries. The Service is the primary contributor of the former.

A further useful distinction between different types of intelligence was made by the Independent Advisory Team that investigated the Service in 1987 (the Osbaldeston Committee). Operational intelligence is "related to the investigation of particular activities considered threatening to the security of Canada". It relies heavily (but not exclusively) on investigative techniques, is usually short-term and is produced for specific consumers or for a specific purpose. *Strategic intelligence* "relies more heavily on research using information from all sources, tends to be longer term and more global in scope and is produced for an interdepartmental audience or for the government as an entity". It is "evaluated in the context of other Canadian national interests".

In our 1987-88 Annual Report, we summarized the results of our investigation of the Analysis and Production Branch in CSIS. We concluded that significant improvements have been made. However, we noted a lack of the multi-disciplinary input necessary in generating the economic, political and social components of comprehensive strategic intelligence. For instance, to date there has been little input from specialists external to government. In our view, changes in the environment of the Branch are still required if CSIS is to move away from producing mainly operational intelligence.

We note that the Osbaldeston Committee was also concerned about the intelligence produced by CSIS and "the lack of a coordinated system for production". Similarly, in 1987 the Senate Special Committee on Terrorism and Public Safety (the Kelly Committee) recommended that "the Security and Intelligence Secretariat of the Privy Council Office be expanded and strengthened to provide a single focus for the gathering of intelligence and assessments from federal departments and agencies for review by the Intelligence Advisory Committee (IAC) and for dissemination to the relevant federal departments and agencies" (page 61).

The IAC is "the closest Canada comes to having a single focus for the gathering, analysis, discussion and dissemination of defence and security information and intelligence". IAC members cooperate and coordinate the production of intelligence, drawing on research and analysis carried out by federal agencies, notably CSIS, the Department of External Affairs (DEA), the Department of National Defence (DND) and the Communications Security Establishment (CSE). At present, the IAC serves all departments; it also supports the Cabinet Committee on Security and Intelligence which is the Prime Minister's vehicle for exercising leadership and setting priorities for both the security intelligence and foreign intelligence agencies.

The McDonald Commission also urged that there be a centralized assessment function in Canada, with a centralized assessments body. It recommended that a Bureau of Intelligence Assessments be established in the Privy Council Office (Second Report, volume 2, at pages 854-56). The Bureau would have no collection capacity. The McDonald Commission urged that the Bureau be separate from the Security and Intelligence Secretariat, with a nucleus of its own intelligence analysts augmented by officers seconded from the departments and agencies of government with responsibilities for security and intelligence matters. The Director General of the Bureau would report to the Prime Minister through the Secretary to the Cabinet and would also be a member of the Intelligence Advisory Committee.

The Commission also urged, however, that the security intelligence agency (now CSIS) should have a strong analytic capacity, producing both short-term and long-term threat assessments. Its assessments would be used by the proposed Bureau, and its intelligence officers would frequently be part of groups working under the auspices of the Bureau to produce long-term estimates and priorities.

We have been favourably impressed with Australia's Office of National Assessments (ONA). In Australia, a clear distinction is made between "collection agencies" and "assessment agencies". Established over ten years ago, the ONA is responsible for collating and evaluating information on many political, economic and strategic matters. The Director-General of the ONA reports to the Prime Minister. It does not collect intelligence as such; instead, it assesses what the collection agencies in that country's security intelligence community--including the Australian Security Intelligence Organization (ASIO)--may provide to it. The ONA also produces reports on specific issues to assist ministers in formulating policy. It was created as an independent body designed to give objective, unfettered advice. It also assists the government in setting its intelligence priorities and requests the collection agencies to obtain specific information it lacks. The ONA consists of a mix of analysts drawn from both the public service and the private sector, including academics with expertise in specific areas. The previous head of the ONA, Michael Cook, was recently appointed Australian ambassador to Washington. He has been replaced by Australia's ambassador to Japan.

25. *We recommend* that Parliament examine the feasibility and merits of establishing an institution similar to Australia's Office of National Assessments.

Such an Intelligence Assessment Office would assess the intelligence product generated by the Service, as well as by other federal agencies, such as CSE and the Foreign Intelligence Bureau in DEA. In addition, it would assist the Cabinet Committee on Security and Intelligence in setting the Government's priorities, and would exercise a quality control function over the intelligence produced by all federal agencies. Like CSIS, it might be given a statutory mandate; like ONA, it should encourage the involvement of a mix of qualified citizens, including experts from outside the government. It would report to the Intelligence Advisory Committee.

Foreign Intelligence

In modern times, Canada has not had a secret foreign service. Should we have an offensive intelligence-gathering function, like the CIA in the United States or the Australian Secret Intelligence Service (ASIS)? Since we have no capacity to collect foreign intelligence by covert human means, we are dependent upon other countries for some types of information about foreign countries, which may pose a threat to Canadian independence in some circumstances. To the extent that covert sources of intelligence are an asset in gaining access to markets and technologies and in international bargaining, Canada will be at a disadvantage with its major trading partners. However, it is by no means clear that Canada needs a secret foreign service.

In light of its location and the difficulties it had in obtaining the foreign intelligence it needed from its allies, Australia established ASIS to concentrate on areas of particular interest to that country . Both political and economic intelligence is generated for Australian policy-makers. There does not appear to be any comparable need in Canada for an "offensive" foreign intelligence agency. However, the case may be more compelling for security intelligence and perhaps criminal intelligence relevant to Canada that is collected abroad.

The Committee is opposed to the establishment of a separate, offensive foreign intelligence agency for Canada. We simply do not believe that the case has been made for such an agency. However, we believe that the *CSIS Act* could provide at least the possibility of the collection of foreign intelligence by CSIS, should the need arise.

26. Therefore, *we recommend* that section 16 of the *Act* be amended to remove the words "within Canada".

This amendment would enable CSIS to assist the Minister of National Defence or the Secretary of State for External Affairs in collecting intelligence relating to the capabilities, intentions or activities of foreign states or persons from any source whatsoever. Under the section, CSIS would only be able to assist outside Canada if it received a "personal request in writing" from either Minister and obtained the written consent of the Solicitor General as well. Such an amendment should not impair the ability of SIRC to review the operations of the Service, either at home or abroad.

However, in the event that Parliament chooses to make this amendment to section 16 of the *Act* and there is any doubt as to SIRC's jurisdiction in this regard, we would propose that an amendment be made to section 38.

27. *We recommend* that section 38 of the *Act* be amended to clarify the Committee's authority to monitor any CSIS operations that may take place outside Canada.

The adoption of recommendations 26 and 27 would not necessarily mean that there would be any real change in CSIS operations. However, in considering such an amendment, Parliament could debate whether it wanted to provide the opportunity for CSIS, in particular cases.

Release of Information

Section 19 of the *Act* limits the disclosure by CSIS of information it has collected, using its extensive powers. We believe that in the spirit of the *Act* the same limitations apply to disclosure of such information by the Solicitor General and by officials and exempt staff in the Ministry of the Solicitor General; they have access to secret CSIS information, and uncontrolled disclosure by them would make a mockery of the carefully drafted protections found in section 19. However, although we have no reason to believe there has been any impropriety, we have learned that the Solicitor General and his officials and staff do not believe they are bound by this section.

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

In another respect, however, we believe the disclosure provision should be broader. Section 19 now makes provision for disclosure to a "person in the public service of Canada" under some circumstances. By a narrow reading, this could mean only paid officials employed under the terms of the *Public Service Employment Act*. We believe it should also include Senators and Members of the House of Commons.

29. *We accordingly recommend* that paragraph 19(2)(d) of the *CSIS Act* be amended to permit disclosures to Senators and MPs on the same basis as to Ministers of the Crown and a "person in the public service of Canada".

Human Sources

As has been stated by the McDonald Commission and by this Committee, the most intrusive investigative tool is probably the "human source". A "human source" is a person who informs the Service of the activities of a CSIS target. The human source may have been recruited when he or she was already in a position close to the CSIS target, or may have been asked to gain such a position by infiltrating the target's organization or circle of friends. Human sources arc usually paid according to the value of the information they provide. Some have suggested that the use of human sources be allowed only under the authority granted by a judicial warrant, in the same way as other intrusive techniques are presently authorized. We believe that this would put too onerous a restriction on the Service, and would, in many circumstances, be most difficult to implement in a practical way. It would be difficult, for example, to fit casual or "walk-in" sources, sources under development, and many unpaid sources into such a scheme.

However, we believe that the Service should be required to observe strict ministerial guidelines in the use of human sources.

30. *We recommend*, therefore, that the *CSIS Act* be amended to prescribe that the Solicitor General may issue precise guidelines to the Service on the use of human sources. Such guidelines would be passed to the Review Committee automatically pursuant to subsection 6(2) of the *Act*.

Committee Reports and Statements

Section 55 of the *CSIS Act* provides for consultation between the Review Committee and the Director when SIRC is preparing certain reports, so as to ensure compliance with the security requirements set out in section 37 of the *Act*. Though we believe the intent of the section is clear, it does not state that, in case of disagreement, the final decision as to what may be included in a report or statement is that of the Review Committee.

31. *We recommend*, therefore, that:

(a) the opening words of section 55 be amended to provide that before determining the content of a statement or report described in section 55, the Review Committee shall consult with the Director in order to ensure compliance with section 37; and

(b) a new subsection be added, as follows:

"The Review Committee's determination in this regard shall be conclusive".

APPENDIX B

SIRC Counsel

Because the investigation and hearing of complaints inevitably calls for the examination of much classified information, Committee counsel need security clearance. To permit immediate action on complaints, the Committee has a panel of lawyers, listed here, with Level III (TOP SECRET) clearance, from which it selects its counsel.

Gina S. Brannan, Toronto

Morris Fish, Q.C.,* Montreal

Gordon Hilliker, Vancouver

Robert E. Houston, Q.C., Ottawa

Jack R. London, Winnipeg

Robert W. MacQuarrie, Q.C., Ottawa

Eva Marzewski, Toronto

Simon Noël, Hull

Christopher J. Roper, Toronto

Perry W. Schulman, Q.C., Winnipeg

Jacques J.M. Shore, Montreal

John H. Tory, Toronto

Grant Kenneth Weaver, Vancouver

David L. Zifkin, Toronto

George T.H. Cooper, Q.C., Halifax

Pierre-C. Gagnon, Quebec City

William G. Horton, Toronto

John B. Laskin, Toronto

Allan Lutfy, Q.C., Ottawa and Montreal

Edouard Martin, Quebec City

Mel Myers, Q.C., Winnipeg

Murray Rankin, Victoria

Mary E. Saunders, Vancouver

Graham W.S. Scott, Q.C., Toronto

John M. Sibley, Toronto

J. Peter Vice, Q.C., Ottawa

Alan Whiteley, Toronto

* Now a member of the Quebec Court of Appeal.

APPENDIX C

Ministerial Direction to CSIS, 1988-89

1. Procedures for disclosure of criminal record information for security assessments
2. Procedures for section 13 and section 14 *(CSIS Act)* recommendations and reports
3. Procedures for handling sensitive files on individuals
4. Ministerial approval of paragraph *2(d) (CSIS Act)* intrusive investigations
5. Collection of information

APPENDIX D

Summary Case Histories of Complaints Dealt with by the Security Intelligence Review Committee, 1988-89

Security Clearances

1. Level III (TOP SECRET) clearance was denied after CSIS learned in its field investigation that the complainant used drugs. The individual acknowledged during the Committee's investigation and hearing that he made a serious error in judgment in using drugs but said he had stopped using them and was, in fact, enrolled in an intensive rehabilitation program. The complainant had been rated Superior in annual job evaluations ever since he had joined the Public Service. Several experts in drug and alcohol rehabilitation were consulted in the course of the Committee's investigation and hearing. The presiding member of the Committee concluded that the complainant had matured, was serious about rehabilitation and would be unlikely to use drugs in the future. The presiding member recommended that the complainant be granted clearance in one year, subject to random urine tests to ensure that the use of drugs had not resumed. In fact the department went further and granted the clearance immediately subject to the complainant's agreement to urine sampling.

2. Level II (SECRET) clearance was denied when the Defence Department (DND) learned that the complainant used drugs after enlisting in the Canadian Forces. The complainant also lied about his drug use until he faced a polygraph test; just before taking the test, he admitted to using drugs. DND intended to review the complainant's case within two years. During the Committee's investigation and hearing, the complainant admitted using drugs after entering the Forces and lying about it. He said that he lied because he was afraid of losing his job. He said he is now married and had matured. The presiding Committee member recommended that DND review the case in one year.

3. Another DND employee was denied Level II clearance when the Department discovered that he had not been in Canada for 10 years, the usual minimum required by the Government Security Policy (GSP). As a result, the complainant was unable to continue certain electronics courses offered by the Department. DND acknowledged that there had been an administrative error, and the complainant should not have been placed in a position where a Level II clearance was required. During the Committee's investigation and hearing, it was agreed by all parties that DND would place the complainant in a position that did not require a clearance until GSP requirements were met. Courses relevant to his new work are being offered to him.

4. A Level II clearance was denied after DND learned that the complainant falsified his academic record on his employment application form and also said that he had resigned from a previous job when a records check indicated he had been fired. DND questioned the employee's honesty and reliability. During the Committee's investigation and hearing, the complainant admitted that he did not hold a high school diploma at the time of his enlistment, but pointed out that he had later completed his secondary education. The complainant admitted that he had made a serious error in judgment. The presiding Committee member concluded that the complainant had matured and would probably not become a target for blackmail by hostile intelligence services. The member recommended that the clearance be granted. DND reviewed the case, agreed, and granted the clearance.

A civilian employee of DND was denied Level II clearance because of evidence that this person was emotionally unstable and might improperly release classified information. After hearing evidence from the complainant and from doctors who bad seen the complainant, the presiding member of the Committee concluded that there were reasonable grounds to believe that the complainant would threaten the security of classified documentation and recommended that the complainant be denied clearance. The presiding member also recommended that DND provide assistance and counselling to the complainant.

6. Notice that a civilian employee of DND was being denied Level II clearance from DND was forwarded to the Committee. Before the Committee started an investigation, the complainant wrote to say that she did not wish to pursue the complaint.

Citizenship

7. The citizenship case is part of an immigration case, no. 8 below.

Immigration

8. The complainant was fighting the denial of citizenship and deportation based on allegations that he had a close and active association with a terrorist organization and was suspected of having engaged in terrorist acts. During the Committee's investigation and hearing, CSIS substantiated these allegations. Evidence by the applicant lacked credibility. The presiding member of the Committee concluded that there were reasonable grounds to believe that the complainant would engage in violent acts while in Canada and recommended that citizenship be denied and that deportation proceedings go ahead. The Committee's decision is being challenged before the Federal Court.

9. Admission to Canada was denied to the complainant on the grounds that he had had long and extensive contact with the intelligence and police services of foreign countries. Although CSIS did not expect him to engage in any useful intelligence operations if he were admitted to Canada, it believed that his presence in Canada would disturb the ethnic community to which he belonged. The presiding members of the Committee concluded that the complainant ought not be excluded from admission to Canada.

10. Admission to Canada was denied by the Department of Employment and Immigration on the grounds that the individual had close and active associations with terrorist organizations and was suspected of having engaged in terrorist acts. In this case, the individual was briefly admitted to Canada to give evidence to the Committee. CSIS substantiated the allegations against this individual, and the presiding member of the Committee agreed that admission should be denied.

Section 41

Note: In addition to the four cases summarized here, there were 30 others that were clearly beyond the Committee's jurisdiction or in which the complainant offered no factual basis on which an investigation could proceed. The cases described here are those on which investigations and hearings were conducted and completed.

11. An individual complained that on the basis of information provided by CSIS, the Minister of Employment and Immigration concluded there was a risk that he was or would be co-opted by a foreign intelligence service. The presiding member of the Committee concluded that the Service's advice to the minister contained inaccuracies and was incomplete, and that the person's being allowed to stay in Canada would not constitute a threat to this country's security.

12. An individual who required a Level III clearance complained that CSIS was taking an unreasonable time to complete its investigation. The individual was granted a security clearance before the Committee's investigation had been completed. However, this did not satisfy the complainant who also alleged that the Service engaged in unnecessary harassment and conducted its investigation in a way that affected the complainant's professional reputation. According to CSIS, the complainant was suspected of having personality traits that might give rise to the possibility of blackmail. The presiding member of the Committee found that the complainant was unnecessarily interrogated several times and that investigators were unprofessional and unskilled in handling such sensitive issues. However, the presiding member concluded that the Service did not make unreasonable use of its powers.

13. The complainant came to the Committee after reading in a newspaper article that CSIS might be investigating him. CSIS contended during the Committee's investigation and hearing that the complainant was an agent of influence consciously acting on behalf of a foreign government. While CSIS did not conclusively show that this person was in fact an agent of influence, the presiding member of the Committee concluded that there were reasonable grounds for an investigation to have been initiated.

14. An individual alleged that he was being investigated by CSIS because of his activities in left-wing organizations, and he asked the Committee to provide him with relevant information and files held by the Service. The presiding member decided that the Committee should neither deny nor confirm whether CSIS was holding files on the individual. The complainant subsequently went to the Federal Court to obtain the alleged files, but his request was also rejected by the court.

APPENDIX E

Participants in a Seminar for Members of SIRC
on the Five-year Review of the CSIS Act

On June 8, 1989, a number of lawyers and scholars, listed here, accepted the Committee's invitation to share their observations on the *CSIS Act*. They did so without fee, and the committee is grateful to them for the contribution they made to its thinking on amendment of the *Act*.

Allan Borovoy
General Counsel
Canadian Civil Liberties Association
Toronto

Gina S. Brannan
Lyons, Goodman, Iacono, & Berkow
Barristers & Solicitors
Toronto

Professor Jean-Paul Brodeur
Centre international de Criminologie comparée
Université de Montréal
Montreal

Professor C.E.S. Franks
Department of Political Studies
Queen's University
Kingston

Allan Lutfy, Q.C.
Lavery, O'Brien
Barristers and Solicitors
Ottawa

Simon Noël
Noël, Décary, Aubry & Associés
Avocats
Hull

Professor Murray Rankin*
Faculty of Law
University of Victoria
Victoria

Professor Peter Russell
Department of Political Science
University of Toronto
Toronto

Graham W.S. Scott, Q.C.
McMillan, Binch
Barristers and Solicitors

David Stafford
President
Canadian Association for Security and Intelligence Studies
and
Director of Research
Canadian Institute of International Affairs
Toronto

Professor Reg Whitaker
Departmental of Political Science
York University
Toronto

Alan Whiteley
McMaster Meighen
Barristers and Solicitors
Toronto

---

* Professor Rankin wrote the background paper on which discussion was based.

APPENDIX F

SIRC Staff on July 1, 1989

Maurice Archdeacon, Executive Secretary	(613) 990-6839
Danielle Blache, Senior Secretary	990-8442
Maurice M. Klein, Senior Research Officer, Counter-terrorism	990-8445
John M. Smith, Senior Research Officer, Counter-intelligence	991-9111
Joan Keane, Research Officer	990-8443
Sylvia Mac Kenzie, Senior Complaints Officer	993-4263
Claire Malone, Executive Assistant	990-6319
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