SECURITY INTELLIGENCE
REVIEW COMMITTEE

Annual Report

1989-1990

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 1990
Cat. No. JS71-1/1990
ISBN 0-662-57774-4

September 28, 1990

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

Dear Mr. Cadieux:

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 1989-90, for submission to Parliament.

Yours sincerely,

John W.H. Bassett, P.C., O.C.
Chairman

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

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

Paule Gauthier, P.C., Q.C.

Stewart D. McInnes, P.C., Q.C.

What's in a name? That which we call a rose
By any other name would smell as sweet.

William Shakespeare

Contents

1. A Year for the Books

Two years ago we used the familiar expression "turning the corner" as the epigraph at the front of our annual report. The idea was that, after some early difficulties, the Canadian Security Intelligence Service (CSIS) was turning onto the path that Parliament mapped in 1984 when it adopted the *CSIS Act*. It is tempting to recycle the line this year, because a lot of corners have been turned since our last annual report was tabled.

For CSIS, there has been the first-ever Cabinet decision setting intelligence priorities. While political meddling in security intelligence is universally recognized as a menace because of the danger of misuse for partisan purposes, political leadership is universally applauded. In a democracy like ours, ultimate responsibility for the well-being of the nation lies with elected politicians. To paraphrase Georges Clemenceau, security intelligence is too important to be left to people in the trade. We have more to say about the new priorities in Chapter 2 of this report (see page 7).

As for the Security Intelligence Review Committee (SIRC), on which we serve, there has been the landmark decision of the Federal Court of Appeal in the *Thomson* case (see page 56). It recognizes the Committee's status as a quasi-judicial tribunal in the investigation of complaints against the denial of security clearances. This decision is a spur to respect for the principles of fundamental justice and the *Canadian Charter of Rights and Freedoms* at all stages in the clearance process.

The year under review also brought our first change of membership. Ronald G. Atkey, our first chairman, and Frank McGee moved on to other activities. Our new chairman, John W.H. Bassett, and a new member, Stewart McInnes, joined SIRC in November, 1989.

In addition, the past year has seen the review of the *CSIS Act* and its companion *Security Offences Act* by a Special Committee of the House of Commons. We have had to write this report without knowing what the Special Committee would recommend. This is something to be borne in mind by regular readers who notice that we are silent in the present annual report on a number of issues we have raised before; we do not want to second-guess the Special Committee.

Review or Oversight?

With this annual report, we turn another small corner ourselves in hopes of ending a controversy over our past use of the term "oversight" interchangeably with "review" to describe our work. We now use the term "review" only.

There has been more to the controversy than a simple matter of vocabulary. Recalling the wide powers of the congressional oversight committees in the United States, some critics have read into the word "oversight" an attempt by us to stretch our mandate further than Parliament intended. The real issue has not been the word itself.[1] It has been the substance of what we do.

---

[1] Indeed, the question of vocabulary as such does not even arise in French. The French version of the *CSIS Act* uses the word "surveillance" which translates both "oversight" and "review".

So for an epigraph to this year's annual report we have chosen Shakespeare's well-known observation that a rose by any other name would smell as sweet. What we mean to convey is that the change of terminology does not--repeat not--mean we read our mandate any differently. We want it clearly understood that as far as what we do is concerned, as opposed to what we call it, it is business as usual at SIRC.

The Scope of Review

In light of the change of vocabulary and also of membership, a brief restatement of some key elements of our approach to review may be timely.

On Top of Events: First, we continue to believe that SIRC needs discretion to examine ongoing operations. Review would be meaningless if it were limited to closed files and completed operations. In security intelligence, many files are never closed. Many operations never end. If we stuck to after-the-fact review, we would not have discovered, for example, that CSIS has still not documented the threat--if any--posed to national security by some individuals whose files remain open in the "residue" of the former counter-subversion program (see Chapter 6).

We are, of course, mindful of the possibility that inquiries could sometimes hamper ongoing operations, and we accept some limitations on a case-by-case basis in consequence. For example, we sometimes postpone studies so intelligence officers can devote all their attention to urgent information-gathering and analysis before pausing to answer our questions. And, in practice, much of our review is after the fact. An example in the present report is our study of on-campus operations (see page 23).

We do not expect to be given notice of intelligence operations in advance, the way the U.S. oversight committees are. Because of the opportunities--indeed, the responsibility--it would give us to advise CSIS on day-to-day activities, notice of operations would tend to make us players in the intelligence game rather than reviewers. That would not be desirable, and it is not the intent of the *CSIS Act*.

But it is clearly our duty to stay abreast of events. It is implausible that Parliament meant us to be historians. We can offer Parliament and Canadians reasonable assurances that CSIS is on track only if we have discretion to examine ongoing operations when we believe that this is what the public interest demands.

Access: Effective review also implies a right to decide for ourselves what we will look into, and Parliament clearly recognized this in the *Act*. Under section 39, we are given access to all information under the control of the Service or the Inspector General, excepting only cabinet confidences. Parliament also told us, in paragraph 38(a), "to review generally the performance by the Service of its duties and functions".

The scope of review must--it seems obvious to us--include financial information and budgets. Whatever else makes the world go round, it is money that makes government agencies go round, and we would be shutting our eyes to important insights if we did not look at how CSIS spends.

We do not want to take part in the budget-making process the way the U.S. oversight committees do. This too would tend to make us players instead of reviewers. Nor do we seek to duplicate the work of the Auditor General, who is better equipped than we are to ensure that money is used effectively.

But we will continue to seek detailed financial information for the help it gives us in carrying out our major responsibility--the review of the Service's operational activities.

Beyond CSIS: CSIS is just one strand--though a most essential one--in the security intelligence web. It works closely with the RCMP (notably with respect to terrorism), the Departments of External Affairs and National Defence (espionage and terrorism), the Department of the Secretary of State (citizenship applications), Immigration Canada (applications to enter Canada), Customs Canada (illicit exports of science and technology assets), Transport Canada (terrorism again, and clearances of airport workers), the Privy Council Office (intelligence analysis), and others.

Our review of CSIS would be incomplete if it did not take account of these relationships. While we have no mandate to comment on the work of other agencies, we would not be doing our job if we were not alive to the interfaces that CSIS has with them and say what we think.

New Ideas: One of the most significant differences between congressional oversight in the United States and our review is that the former extends to the entire security and intelligence support system in the United States. Oversight there stops only at the door of the White House. Here in Canada, there is no independent review of the federal security and intelligence apparatus as a whole.

As a result, seeing how CSIS interacts with other agencies gives us a unique perspective. It is also apt to prompt ideas about how security intelligence could be improved. We believe that Parliament expects us to share our ideas. It would be too much to hope that every one of them is a crackerjack. But it would be irresponsible of us to hold our tongues and "let George say it" when we see room for improvements. There is no "George" with the same opportunities we have to see how things work--or do not work--and to speak up.

The Credibility of the Service

Does public criticism of the Service sap its credibility among Canadians and among the other agencies, at home and abroad, with which it works?

That fear needs to be stood on its head. CSIS gains credibility from the frankness we have tried to practice in our annual reports and other public statements. Frankness is the evidence that SIRC has not--as review agencies are often accused of doing--been co-opted and become a mere apologist for the people it is supposed to be keeping in line. And SIRC's independence provides assurances that the whistle will be blown if CSIS falls down in terms of either effectiveness or fairness. Furthermore, Parliament and the public are entitled to all the information that national security allows us to reveal.

As for the Service's credibility with sister agencies abroad . . . well, external review is becoming a widely-shared experience. It is a well-established fact of life for the Australians and the Americans, and the British are inching their way towards it. CSIS is not such an unusual specimen in being subject to review. Even in the Soviet Union, the KGB seems to be scrambling to catch up with glasnost. KGB chief Vladimir Kryachkov has said his agency would welcome a legal framework for its operations.

And it is surely clear that CSIS is a stronger organization today, after six years of review, than it was when it began in 1984. CSIS has been through some difficult times, not entirely by its own fault. From what we can see, it has successfully negotiated the corner and continues to gain credibility.

The Necessity of Review

Review obviously adds to the complexity of life for security intelligence agencies. Not many public institutions get the kind of close attention that we give CSIS, or the publicity that goes with it. But independent review is the tradeoff for the powers that an intelligence agency has-and needs--to intrude on individual privacy for the sake of national security. Independent review is essential to assure Parliament and the public that the Service is not making unreasonable or unnecessary use of these powers.

Review came into being because of the demonstrated potential for abuse of secret powers by those charged with national security. That was the case in the United States and in Australia as well as in Canada. In the U.K., where review is essentially bureaucratic rather than external, there seems to be less check on wrongdoing. Earlier this year, British authorities acknowledged that false stories had been spread in an attempt to discredit the Irish Republican Army. External review is a bulwark against such abuses.

For what comfort it brings, as the years go by and as CSIS increasingly takes the shape Parliament intended, it is in the nature of things that we should have fewer and fewer fundamental criticisms to make. It is generally recognized that the difficulties of separating CSIS from the RCMP were underestimated at the start. Under the circumstances, some growing pains were unavoidable. But as CSIS completes its transformation into a modern intelligence agency, it is to be expected that there will be less of a fundamental nature to complain about.

However, the need for independent review will never disappear. Our epigraph three years ago was Juvenal's "Who is to guard the guards themselves?" The line has survived close to 2,000 years because it is always relevant. The existence of independent review is the best available guarantee that security intelligence will stay within the law.

2. Review

Because of its wide investigative powers and the secrecy in which much of its work is necessarily shrouded, CSIS comes under a number of controls. It requires warrants from the Federal Court of Canada to use such intrusive techniques as wiretaps. It gets policy direction from the Solicitor General. The Inspector General acts as the Solicitor General's personal auditor of the Service. SIRC's role is to be Parliament's and the public's watchdog.

Our duties under the *CSIS Act* fall into two broad streams--the investigation of complaints and review of the Service's performance of its duties and functions.

We discuss complaints in Chapter 8. This chapter and the five that follow describe what we have learned in the review process, as fully as is consistent with the protection of national security. This chapter focuses on the activities specifically enumerated in the *Act* and on the review process.

Ministerial Direction

Subsection 6(2) of the *CSIS Act* authorizes the Solicitor General to give written direction to the Service. Subparagraph 38(a)(ii) makes the review of the Solicitor General's directions one of our routine duties. We look at amendments to the CSIS Operational Manual too, because they can also be a vehicle for direction.

A list of the seven directions issued in 1989-90 can be found in Appendix A. It is not practical to list amendments to the Operational Manual--most of which are just housekeeping in any case. We do not have concerns about any of the 1989-90 directions or amendments to the Manual.

However, in the course of one study we found that direction had been provided outside the usual channels. As a result, it could have escaped our review. We have brought this to the attention of the Solicitor General.

In the past, much ministerial direction has been a patchwork stitched together in response to immediate needs. As a problem arose, a direction would be whipped up to deal with it. These problems typically involved privacy, the integrity of social institutions, and legitimate advocacy and dissent. The general thrust has been to increase protections for individual rights.

A Second Thrust: This continued in 1989-90, but a second thrust was also evident. Some welcome attention is now being given to making ministerial control more systematic more -- policy-driven than, as in the past, event-driven.

A direction on the Accountability of the Director to the Solicitor General provides, among other things, that as far as possible, ministerial directions will set out principles and guidelines in the key areas of Service activities. Under this direction, the Solicitor General commits himself to develop a strategic policy framework which will integrate existing direction.

Among the most important provisions is that the Solicitor General will provide the Director every year with a written direction setting out the Government's security intelligence

priorities. We discuss the first such direction on National Requirements for Security Intelligence later in this chapter.

A direction on General Principles and Policies Governing the Conduct of Investigations is designed to be an umbrella under which more specific direction will be given. Among other things, it reiterates and elaborates upon the five fundamental principles laid down by the McDonald Commission:

- the rule of law must be observed;
- investigative means must be proportionate to the gravity of the threat and the probability of its occurrence;
- the need to use various investigative techniques must be weighed against possible damage to civil liberties or to valuable social institutions;
- the more intrusive the technique, the higher the authority required for its use;
- except in an emergency, the least intrusive techniques of information collection must be tried before there is recourse to more intrusive techniques.[1]

These principles deserve frequent repetition, for they are just as relevant today as when they were written. They have not exactly been a secret, of course, but this is the first time that CSIS has had explicit direction from the Solicitor General to apply them.

We are especially pleased that the direction on General Principles echoes one of our recurring themes, calling for the use of open sources like published articles whenever possible as an alternative to more intrusive investigations that can carry the risk of unnecessary intrusion on personal privacy.

A Definition of Direction: In line with the tidying up being done in this area, steps were also taken in 1989-90 by the Ministry of the Solicitor General to nail down a precise definition of "ministerial direction". The lack of an agreed definition has been a problem in the past when we found that the Ministry was not providing us with some documents that the Service regarded as direction.

Grey areas remain -- notably correspondence from the Solicitor General to CSIS about day-to-day operations. The Solicitor General does not consider this to be direction because it does not contain "instructions of a continuing nature". However, a specific direction in one case may serve as a precedent for the next and the next until it becomes as rigid a rule as any overall direction.

Nonetheless, recognizing that a perfect definition is probably beyond human reach and in light of consultations we had with the Ministry, we are satisfied that we will continue to get everything we need to discharge our statutory responsibilities to review ministerial direction.

---

[1] Freedom and Security under the Law, the Second Report of the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, 1981, pages 513-514.

Responsibility for Adverse Recommendations: One direction revises the level of responsibility for recommendations by CSIS against granting security clearances. It requires that the Director (or a designated deputy director in his absence) personally approve each recommendation to deny a clearance under the Government Security Policy (GSP) -- that is, screening of public servants, government contractors, airport workers and so on. Approval was previously at a much lower level.

This is something we have recommended. We believe that recommendations to deny clearances should be made only at a very high level to ensure that they are not treated lightly. Evidence at our hearings shows they sometimes have been in the past.

National Requirements for Security Intelligence

In the long term, the most significant development of 1989-90 for CSIS will almost certainly prove to be the establishment of security intelligence priorities by the Cabinet. It deserves separate treatment from other ministerial directions because of its historic importance as an innovation. This is the first time Cabinet has set priorities for CSIS, and it fills an important gap in legitimate political supervision of security intelligence.

Cabinet's decision underlies the first of a promised annual series of directions on National Requirements for Security Intelligence. It sets five priorities for the Service's collection of information, analysis and dissemination of finished intelligence to March 31, 1991:

- public safety,
- the integrity of the democratic process,
- the security of government assets,
- economic security, and
- international peace and security.

Most of these priorities are self-explanatory. As described publicly by the then Solicitor General, the "integrity of the democratic process" covers:

> the function of our national institutions, and the rights and freedoms fundamental to the political well-being of a democratic society. CSIS has a role to warn the government about clandestine foreign attempts to influence Canadian policy-making and about activities that seek political change through violence.[2]

"Economic security" focuses on the protection of the nation's scientific and technological assets. In Chapter 3, we report on developments following our study last year of science and technology issues (see page 22).

The Solicitor General has said that public safety is his first priority and must be the top priority for CSIS as well as the other agencies for which he is responsible.[3]

---

[2] *Accountability and Effectiveness: National Requirements for Security Intelligence in the 1990s*, notes for a speech by the then Solicitor General to the Canadian Association for Security and Intelligence Studies, September 29, 1989.

[3] Notes for a statement by the Solicitor General to the Standing Committee of the House of Commons on Justice and Solicitor General, April 5, 1990.

It exceeds our mandate to comment publicly on policy established by the Government. The right and duty to scrutinize Cabinet's decisions lies with Parliament itself. Our proper concern is with the impact of policy on CSIS operations. A general observation we can make now is that the establishment of priorities at the Cabinet level represents a quantum leap in the management of security intelligence in Canada. It is only a slight over-simplification to say that priorities have generally resulted until now from a combination of tradition (generally speaking, one year's target is also next year's target) and ugly surprises as new threats erupted.

Except for a few lines in our reviews of the Analysis and Production program and the protection of science and technology assets in Chapter 3 (see pages 19 and 22), it is still too early to report the CSIS response in more detail. We will, of course, be monitoring the situation closely.

Operational Manual

The long-term overhaul of the CSIS Operational Manual continues. Some sections still date from before July 16, 1984, when CSIS came into being and inherited the procedures as well as the responsibilities of the former RCMP Security Service.

However, CSIS has addressed the major areas highlighted in our reports and by the Independent Advisory Team created by the then Solicitor General in 1987 to follow up on our report on the counter-subversion program. These include procedures for designating the targets of investigation, controls on human sources and the conduct of investigations. Since July 16, 1984, there have been 106 amendments and 30 new bulletins have been issued for addition to the Manual.

Amendments in 1989-90: The major amendments to the Operational Manual in 1989-90 increase protections for individual rights. Three substantial amendments were made with respect to warrants under which the Service may be authorized by the Federal Court of Canada to use such intrusive techniques as wiretaps. In part, they codify existing practices. They also fill holes identified in our study of the Counter-Intelligence program last year--the definition of "solicitor" for purposes of respecting client-solicitor privilege, for example. These changes are all for the better.

Ministerial Authorizations

Many directions require the Service to obtain the consent of the Solicitor General on a case-by-case basis for certain kinds of operations. As part of our statistical review under subparagraph 39(a)(vii) of the *CSIS Act*, we monitor the number of authorizations by type of activity, by CSIS program, and by region. We are thus able to note any significant changes that merit a more detailed look.

In particular, we keep a watch on authorizations under paragraph 2(d) of the *CSIS Act*--the "subversion" provision. While CSIS can gather open information and unsolicited information generated by other inquiries on alleged "subversives", it needs the Solicitor General's personal consent to use intrusive powers against them. Again in 1989-90, as in previous years, there were no paragraph 2(d) authorizations. CSIS tells us that it did not face any significant difficulties

as a result. We report further in Chapter 6 of this report on the "residue" of the counter-subversion program.

We also zero in from time to time on more closely-defined areas. In 1989-90 we made special studies of authorized operations on university campuses and in one region. We review our findings in Chapter 3 (pages 23 and 25).

Arrangements with Other Governments

Subsection 17(l) of the *Act* allows CSIS, with ministerial approval, to enter into arrangements with provincial governments, provincial and local police forces, foreign governments and their agencies and international bodies. Under subparagraph 38(a)(iii), we are required to review such arrangements and to monitor the provision of information and intelligence by CSIS under their terms.

Within Canada, there were no new arrangements in 1989-90. There is still no formal arrangement with Quebec, and the arrangement with Ontario is still limited to the exchange of information with police forces.

Internationally, five new arrangements were approved in 1989-90, extending the Service's contacts in Europe, Latin America and Africa. One, designed to give CSIS access to information for use in vetting visas, is with a country that has a clouded human rights record. CSIS is sensitive to the difficulties of this situation, and we intend to monitor the product of this arrangement especially closely. CSIS also broadened the scope of its liaison arrangements with police and security agencies in some 60 countries, in order to improve its access to information needed for security clearance assessments. Exchanges of information with one country were sharply cut back in 1989-90, and the arrangement with a second was terminated outright. The Service took exception to the activities of these countries' agents within Canada.

Chapter 5 of this annual report discusses the findings of a study we made of releases of information to other agencies in Canada and abroad under subsection 17(1) arrangements.

Unlawful Acts

During 1989-90 we were advised under subsection 20(4) of two instances in which the Attorney General was told that CSIS employees might have broken the law in the course of their work.

In one case, an employee is alleged to have obtained information from a police force and given it to a friend for business purposes. In the other, an employee is alleged to have fabricated field reports. The latter individual is no longer employed by the Service. In both cases, the Attorney General has determined that national security would not be compromised by prosecutions and so has relayed the information to the provincial authorities responsible for determining whether charges should be laid.

Disclosures

Section 19 of the *Act* sets out the conditions under which CSIS may disclose information it obtains in the performance of its duties and functions. A report must be made to us when, under paragraph 19(2)(d), information is disclosed to a minister or public servant after a determination by the Solicitor General that the disclosure is essential to the public interest outweighing any invasion of privacy that would result.

One such disclosure was reported to us in 1989-90. It gave us no concern. But in Chapter 4 we deal with concerns about the public release of information by the Service with respect to inquiries into the potential for violence among native Canadians (page 32).

Report of the Director and Certificate of the Inspector General

Under subparagraph 38(a)(i), we review the annual report that the Director of CSIS makes to the Solicitor General under subsection 33(l) and the certificate in which the Inspector General, under subsection 33(2), indicates to the Solicitor General whether the annual report is satisfactory.

In his 1988-89 certificate, the latest to reach us, the Inspector General says that the Director's annual report was not sufficiently comprehensive for his purposes. For example, the Director's annual report did not deal with some matters that had been reported to the Solicitor General through other channels. This particular concern is compounded by the new ministerial direction on the Accountability of the Director to the Solicitor General, discussed earlier in this chapter (page 5). It calls for additional vehicles for reporting by the Director. We understand that this year's annual report by the Director will reflect suggestions made by the Inspector General.

The Director's annual report and the Inspector General's certificate both reach us so long after the end of each fiscal year that we can make little use of them in preparing our own annual report for that year. The Director's report reaches us in July and the Inspector General's certificate in the autumn. We will continue, however, to follow up salient points in both documents and comment as required at the first opportunity.

Special Reports

Under section 54 of the *Act*, we have the authority to make special reports to the Solicitor General. We do so to raise issues of such importance or urgency that they cannot await discussion in our next annual report and when it is necessary to go into detail that could not, for national security reasons, be included in an annual report.

During 1989-90, we made two reports under section 54. One, on security screening in immigration, was ready by the time we wrote last year's annual report and is discussed there. (We have more to say about security screening in immigration in Chapter 3; see page 19.) The second, dealing with CSIS inquiries on native issues, is discussed in some detail in Chapter 4 of the present report.

Consultations and Inquiries

Our relations with the Service remained cordial but wary in 1989-90. This is normal. In the long term, our goals are identical with the Service's--to protect national security with the least possible infringement of individual rights. But in the short term, the heavy responsibility CSIS bears for national security puts it at risk of accenting the former at the expense of the latter while our *raison d'être* as a Committee is to uphold the latter as strongly as is consistent with the former. CSIS and SIRC look at the same coin, but from different perspectives. Naturally this produces occasional strains.

Formal Inquiries: In our review function, not counting inquiries arising out of complaints, we directed a record 175 formal inquiries to the Service in 1989-90 and had 168 replies.[4] The trend in recent years has been sharply upward; we submitted what now seems a modest 96 formal inquiries in 1987-88 and 141 in 1988-89.

In 1989-90 we noted an increasing tendency by CSIS to monitor closely the information it provides to us. We recognize that this reflects a development we approve of, namely generally tighter management of the Service. However, it is a factor in the time it takes to get some answers. In 1989-90, the average time CSIS took to answer a formal inquiry was more than two months.

Briefings: We met three times with the Director in 1989-90. He called on our regular meetings in Toronto on June 9, 1989, and Vancouver on September 8, 1989. We also met him during a visit we made to CSIS Headquarters on March 6, 1990.

As in years past, we visited regional offices of the Service when our regular meetings took us out of Ottawa. We were briefed on regional operations in Toronto on June 9, 1989, in Vancouver on September 8, 1989, and again in Toronto on February 19, 1990. We were also briefed by the CSIS liaison officer in Washington on April 12, 1989.

Beyond CSIS: As the minister responsible for both CSIS and the RCMP, the Solicitor General is a key figure in the government-wide security intelligence network. We met the then Solicitor General, who was accompanied by the Deputy Solicitor General, on May 11, 1989, and with the new Solicitor General soon after the fiscal year covered by this report ended, on April 9, 1990. We met separately with the Deputy Solicitor General on March 6, 1990.

We also met the new chief of the Communications Security Establishment (CSE) on May 12, 1989, the new Deputy Secretary to the Cabinet responsible for intelligence and security on June 30, 1989, and, during a brief visit to Washington, D.C., in April, 1989, the Canadian diplomat responsible for liaison on behalf of Canada's Intelligence Advisory Committee.

The principal purpose of the Washington trip was to hold general discussions with representatives of the Select Committees on Intelligence of the U.S. Senate and the House of

---

[4] This does not take into account the hundreds upon hundreds of oral questions answered on the spot in briefings and interviews.

Representatives. Like security intelligence, the review business has its "tradecraft", and we were able to exchange views on how best to fulfill our roles.

Inspector General: We continued to enjoy close cooperation with the Inspector General. While the Inspector General's central role is to be the Solicitor General's operational auditor, paragraph 40(a) of the *CSIS Act* allows us to commission research from him. We also see reports on the research he carries out to support his reporting to the Solicitor General. We draw on some of them in Chapter 3 of this report, where we discuss warrants (see page 15) and joint operations (page 18).

3. CSIS Operations

In addition to duties explicitly spelled out in the *CSIS Act*, we have an open-ended review mandate under paragraph 38(a) and section 40. Paragraph 38(a) tells us to "review generally the performance by the Service of its duties and functions". In particular, subparagraph 38(a)(vii) says we are to "compile and analyse statistics on the operational activities of the Service". Section 40 allows us to conduct or commission studies "for the purpose of ensuring that the activities of the Service are carried out in accordance with this *Act*, the regulations and directions issued by the Minister ... and that the activities do not involve any unreasonable or unnecessary exercise by the Service of any of its powers".

Having dealt in Chapter 2 with the review activities enumerated in the Act, we now turn to our more general review. In Chapters 4 to 6, we discuss the findings of three large-scale studies--on CSIS and native peoples, on exchanges of information between CSIS and other agencies at home and abroad, and on the counter-subversion "residue". Chapter 7 deals with the internal affairs of the Service. The present chapter covers a broad range of CSIS programs and activities.

Warrant Statistics

Under subsection 21(3) of the *CSIS Act*, the Service requires warrants from the Federal Court of Canada for most of its intrusive activities. (The exceptions are the use of human sources and undercover agents.) We monitor both warrant applications and the use made of powers under warrants. As can be seen in Table 1, the total number of warrants granted and renewed dropped somewhat in 1989-90 from the previous year.

Table 1. New and Renewed Warrants, 1987-88 to 1989-90

	1987-88	1988-89	1989-90
New warrants granted	67	55	34
Warrants renewed	8	35	50
Total	75	90	84

Source: CSIS

For both statistical and substantive reasons, it is not possible to read much into the overall totals reported here. The statistical reason is that the absolute numbers are not great, so a few events, which may not be significant in themselves, can have a big impact on the totals. The substantive reason is that a single warrant can permit the use of many powers against many targets, with the result that vastly increased activity would be difficult to discern if it were authorized by fewer but broader warrants.

Better Informed: Canadians used to be more adequately informed about the use of warrant powers in security intelligence. Before the *CSIS Act* was adopted in 1984, such warrants were issued under the *Official Secrets Act*. Because a warrant under this *Act* ordinarily permitted the use of one power against one target, meaningful comparisons could be made between the annual

totals made public by the government. An increase in the total ordinarily meant an increase in intrusive activities.

We continue to hope that amendments to the *CSIS Act* will soon enable us to provide more meaningful figures--specifically, the number of Canadian citizens or landed immigrants who are the subjects each year of powers granted by warrants.

Of course, we see far more detailed statistics than we are able to publish. We monitor them closely and ask the reason when we see changes that may be significant. Twice in 1989-90 we made formal inquiries about trends we observed. We were satisfied with the answers.

Even in the published statistics, some changes are dramatic enough to call for explanation. The four-fold rise in renewals from 1987-88 to 1988-89, as we have noted before, does not mark a sharp change in targeting. Rather it reflects the catching up there was to do after delays in renewing warrants during 1987-88 while a more rigorous process was put in place. The downgrading of most "counter-subversion" targets in 1987-88 also had an impact.

Reporting Régime: During 1989-90, CSIS changed the format of its reports on applications for and the use of warrants, producing a different and less detailed selection of data. As a general rule, we try to limit the burden of review on CSIS; whenever it is reasonable to do so, we do our statistical review on the basis of data CSIS generates for its own purposes. In this case, however, we do not consider the new reports adequate for our work, and we have submitted a request for the kind of detailed statistics we need to ensure continuity in our review.

Protections

In addition to our statistical studies, we read the warrants granted and a selection of the affidavits submitted to the Federal Court in support of warrant applications. One thing we watch with special care is the protection of individual rights. As noted in Chapter 2 (see page 8), the CSIS Operational Manual was amended in 1989-90 to increase protections for individual rights. The warrants and affidavits we reviewed in 1989-90 gave us no concern.

Intercepts with Consent: Further protection for individual rights results from a ruling by the Supreme Court of Canada in January.[1] Citing the ban on unreasonable search and seizure under the *Canadian Charter of Rights and Freedoms*, the Court held that police need a judicial warrant to record conversations that informers or undercover agents have with suspected criminals. Previously there was no limit on eavesdropping as long as one party the informer or agent--consented.

CSIS is also bound by this ruling, and the Service took immediate steps to comply. The day after the Supreme Court handed down its decision, the Service advised its staff that no conversations with targets could be recorded without a valid warrant for the interception of oral communications.

---

1 *Mario Duarte v. Her Majesty the Queen and Attorney General for Ontario, Attorney General of Quebec*, January 25, 1990.

While a Supreme Court ruling on video recordings is pending, the Service put a similar limitation a few days later on video recordings. Even when one party consents, it told investigators, video recordings can be made only under warrants in situations where the target has a reasonable expectation of privacy--not on the street, that is, but in such places as motel rooms.

The Service still routinely tapes incoming telephone calls to its Emergency Operations Centre. We think this is appropriate. CSIS gets calls with tips that deserve close analysis and it needs tape to work with, if only to determine what a mumbled word is.

We looked into the Service's use of warrantless intercepts before the Supreme Court ruling, and were satisfied with the answers.

Inspector General's Reports: The Inspector General reported in 1989-90 on two studies related to warrants. In a microscopic review of four affidavits sworn in support of applications for warrants, the Inspector General found a number of minor errors of fact--incorrect dates, for example. However, a more serious failing came to light: he was not satisfied that the officers responsible for preparing and verifying the affidavits were rigorous enough in determining that the facts alleged were correct before certifying them so. We will monitor the follow-up actions in this area.

The Inspector General also made an in-depth study of the execution of warrants, particularly the Service's compliance with ministerial direction and conditions written into the warrants themselves. In activities up to March 31, 1988, he found no instances of non-compliance.

We were especially reassured by the Inspector General's conclusion that the Service has adequate systems in place to protect client-solicitor privilege. The essence of this protection, which is written into warrants, is that when electronic eavesdropping picks up a conversation between a lawyer and client, a senior CSIS official is called in to determine whether the conversation relates to the security threat specified in the warrant. If the conversation deals with legitimate legal issues, no record is made of it and the tape is erased.

Access to CPIC

One long-standing problem was resolved in 1989-90, when members of CPIC (the Canadian Police Information Centre) decided to give CSIS direct access to two of its three data banks-Motor Vehicle Records and Identification Records. Access had been limited for years because some CPIC members were reluctant to admit a non-police user.

We do not believe that the exclusion of the third data bank is a serious limitation. It includes information on open police investigations, and CSIS access would raise serious concerns about individual privacy.

Another limitation gives us less concern now than it did when we referred to it in last year's annual report. Because Quebec has not signed a formal cooperation agreement with CSIS, it does not allow the Service direct access through CPIC to its motor vehicle records. On the face of it, this appears to be a significant gap. However, we are assured that CSIS is able to get the information it needs.

Relations with the RCMP

The Service's relations with the RCMP were put on a more systematic footing in 1989-90 with the signature of a Memorandum of Understanding (MOU) between the two. The MOU does not add anything new, but it brings together in one, coherent document a number of ministerial directions issued to both agencies over the years.

Among other things, it "sets out undertakings by both parties to provide each other with specific types of information and provides for procedures to protect the information exchanged".[2]

This refers to an unavoidable source of tension between CSIS and the RCMP. Criminal proceedings concerning security offences, a key RCMP role, sometimes carry the risk of public exposure for CSIS operations in areas where secrecy is essential to effectiveness. As a result, CSIS is sometimes unable to tell the RCMP all it knows. Chapter 5 includes an example of the difficulties that can arise as a result (see page 38).

Counter-Terrorism Program

Canada's new National Counter-Terrorism Plan (NCTP) was endorsed by Cabinet in 1989-90. Under the NCTP, the Service's primary responsibility is to gather intelligence on terrorist threats and pass it on to government decision-makers and police. The Service may also be called upon to give operational support in the course of a terrorist incident, including specialized technical aid to police at the scene.

This dual role has now been incorporated in the Service's internal Counter-Terrorism Management Plan. A special emergency preparedness unit has been created within the Counter-Terrorism Branch (CT), and work has begun on an automated system to monitor and control data generated during exercises and terrorist incidents.

The Branch generated more than 1,000 threat assessments in 1989-90. This is off somewhat from the 1988-89 level because 1988 was an unusual year with a number of major international events, including the Toronto Economic Summit. We have reviewed CSIS post-mortems on all these events except the one on the Toronto Economic Summit, which came to us too late for examination before the present report had to go to the printer.

In a second important decision during 1989-90, the government for the first time set intelligence priorities (see page 7). Among them is public safety--a matter of obvious concern to the CT Branch. The then Solicitor General said publicly that public safety was Number 1 in his view. One result of this priorization has been an improvement in communications between the CT threat assessment unit and other federal departments. The Branch now also participates in a working group that develops brief profiles on foreign countries for the Department of External Affairs.

---

[2] Notes for a statement by the then Solicitor General before the Special Committee of the House of Commons on the Review of the *CSIS Act* and the *Security Offences Act*, October 31, 1989.

The CT Branch took part in a Canada-U.S. counter-terrorism exercise in the summer of 1989. Afterwards, it was represented on a working group that reported to the government's Security Advisory Committee on the strengths and weaknesses revealed by the exercise. A further exercise was scheduled for the early summer of 1990.

There were no serious terrorist incidents in Canada in 1989-90. But CSIS played a role in the apprehension in the United States of four persons alleged to have tried to buy sophisticated weaponry for the Provisional IRA.

Air India and Narita: We are still being briefed regularly by the Director of CSIS on the investigation of the Air India and Narita explosions. There is nothing new we can report. This is now more a matter for the police than for a security intelligence agency.

While we understand public impatience with the failure to lay charges in connection with the Air India tragedy, we still defer to suggestions that a full-scale inquiry by us into the CSIS role should wait because the risk of impeding the police investigation and the judicial process remains too great.

Counter-Intelligence Program

The *détente* essential to President Gorbachev's reform program has an impact on the counter-intelligence program. In January, 1990, the first of a new series of unclassified occasional papers, issued under the name *Commentary*, deals with President Gorbachev's program. We made plans in 1989-90 to explore the impact of galloping *détente* on security intelligence ourselves at the seminar discussed in Chapter 9 (see page 64).

Foreign Influence Targets: Paragraph 2(b) of the *CSIS Act* defines one 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". Targets under this paragraph are investigated by the Counter-Intelligence (CI) Branch. In 1988, the Service implemented new rules for the investigation of these targets. In order to limit the risks of overstepping the bounds of paragraph 2(b) into the realm of legitimate protest, advocacy and dissent, the new rules limited the scope of investigative activities and the amount of reporting.

During 1989-90, we had a look at how the 1988 rules were working out in practice. We made a random selection of 2(b) targets from all regions, then obtained all reports in which they were mentioned. We also examined the relevant decisions of the Service's internal Target Approval and Review Committee.

Some concerns in this area emerged from our study of campus operations, reported later in this chapter (see page 23). But, overall, our findings in the study of 2(b) targets were reassuring. While we saw a few reports that seemed to us unwarranted, CSIS has clearly moved towards more focused reporting to meet defined investigative purposes.

Joint Operations

The Inspector General reported to the Solicitor General in 1989-90 on his review of the Service's adherence to ministerial direction in the conduct of joint operations within Canada with foreign security and intelligence agencies.

The overall conclusion is reassuring: the Inspector General reported that CSIS conducted these operations capably and professionally. The random selection of cases for in-dept study included one that is well known--the sting that landed Stephen Ratkai in jail in 1989 for gathering classified information about a U.S. Navy base at Argentia, Nfld. The Inspector General complimented CSIS for its work with the U.S. Naval Investigative Service in this case.

Security Screening

Security screening got even slower at Levels I (confidential) and 11 (secret) in 1989-90 but CSIS does not seem to be to blame. Demand kept on mushrooming, and the RCMP took an average of eight weeks to check fingerprints during its conversion to new computer hardware. As a result, CSIS needed an average of 110 days to process a clearance application at Levels I and II, up from 60 days the previous year.

However, the news was brighter at Level III (top secret). The average time to process an application for clearance at this level was down to 200 days in 1989-90 from 240 days the year before.

The Service believes that its targets of a 30-day average at Levels I and II and 120 days at Level III remain appropriate and attainable. When the RCMP has its hardware running smoothly, it is expected to bring the average turnaround time for fingerprint checks to less than two weeks, which will significantly help the Service meet its targets.

In addition, a number of changes to the Government Security Policy (GSP) in December 1989, and March, 1990--while they were made for different reasons--are expected to reduce demand as a side-effect. For example, departments now have the option of no requiring fingerprint checks at Level I except when a check of the applicant's name indicates a possible criminal record, and Levels I and II clearances require updating every 10 years rather than every five. (Level III clearances still have to be renewed every five years.)

A new "portfolio" system assigns responsibility for each client to a particular unit within the Security Screening Branch. Clients are also being informally briefed on the steps the Branch goes through in preparing security assessments. Closer contact between the Branch and its clientele should result in a better understanding of each other's needs and priorities.

Meanwhile, CSIS figures indicate that demand grew dramatically again in 1989-90. The number of applications submitted by the 10 largest users (not counting Level I checks for airport workers) rose to 54,342 in 1989-90 from 37,051 the year before--an increase not far short of 50 per cent. Additional investigators were assigned to security screening in

Ottawa and Toronto to keep the number of outstanding field investigations from rocketing out of control.

Immigration Screening

The Service's role in screening immigrants has concerned us for some time.[3] The tremendous effort CSIS was devoting to this work seemed out of proportion to the very small number of undesirable immigrants turned up. A huge backlog and excessive delays were hardly surprising.

We are, therefore, pleased that a new system which appreciably streamlines CSIS participation in the process is being given a trial run in four locations. An assessment of these pilot projects was planned by CSIS, together with Immigration Canada, the Department of External Affairs (DEA) and the RCMP, in the summer of 1990. CSIS told us in June that "signs to date are most positive". We will, of course, monitor this situation.

Extra Investigators: Meanwhile, nudged by DEA, CSIS put some experienced investigators from its regional offices in Canada to work on immigration screening in order to clear a backlog.

DEA cited some cases of excessive delay--more than a year to process an honourably discharged former officer in the U.S. armed forces, with a high-level clearance, and more than a year for a 20-year-old American fresh from high school. Yet a former police officer already denied a U.S. visa because he was suspected of human rights abuses in his homeland breezed through the system.

The Department also cited an apparently unrealistic request that a person who spent a year as a child in a refugee camp in Thailand supply fingerprints from that country. It would be virtually impossible to meet this demand; insisting on it would amount to denial of clearance.

Analysis and Production

The Cinderella story of the Analysis and Production Branch (RAP) continued in 1989-90. When we made a special study of RAP in 1987-88, we found it was a neglected step-sister in the CSIS family.[4] Today it seems to be the glamorpuss. The change is good news.

The Solicitor General's new direction on National Requirements for Security Intelligence (see page 7 of the present report), while it did not launch the transformation, gives it further impetus. The National Requirements emphasize that CSIS is an *intelligence* agency whose role is not merely to pile up facts but to advise the government on the strength of thoughtful analysis. The National Requirements lend to RAP a necessary prestige comparable to that of the operational branches, Counter-Intelligence and Counter-Terrorism.

---

3 See our *Annual Report, 1987-88*, page 8.

4 See our *Annual Report, 1987-88*, page 35.

Strategic Intelligence: We especially welcome the emphasis that the direction puts on strategic assessments which "consolidate and go beyond the immediate interests of individual consumer departments and agencies".[5] One of our most fundamental criticisms of RAP in 1987-88, shared by the Independent Advisory Team under Gordon Osbaldeston, was that we found too much emphasis on short-term analysis of events as they unfolded and immediate threats. There was little basic strategic intelligence--in-depth studies to help the government develop policy and make strategic decisions.

Of course the National Requirements guide the Intelligence Production Committee (IPC) and the Executive IPC in ordering intelligence production and in reviewing the papers that result.

There has also been direction by the Solicitor General to try open sources first, before there is recourse to investigation (see page 6). This is also welcome. Increased use of open sources as an alternative to investigative techniques that may intrude on the privacy of Canadians has been one of our recurrent themes. Statistics compiled by the Service show that RAP is the largest single source of reference requests to the CSIS Information Centre (the library).

Progress Report: At the risk of repeating in part what we said in last year's annual report, we think it is worth summing up here what has happened in RAP since 1987-88.

The number of analysts has nearly doubled. We do not mean merely the number of positions drawn on the organigram. RAP has been plagued in the past by unfilled positions. We mean that the number of living, breathing--and thinking--people doing analysis has nearly doubled. Overall, the number of person-years in RAP has risen 70 per cent.

Bigger Is Better: This is a case in which bigger is better; sheer size brings advantages. The number of senior positions has been fully doubled, with the result that there are more senior intelligence officers doing hands-on analysis instead of being swamped with management duties.

With more senior and mid-level positions available, RAP is also better able to keep talented people whose normal career ambitions might have encouraged them to leave when they had used up all the opportunities within the Branch. In 1987-88, RAP was a kind of siding where an intelligence officer might park for a while between runs on the main line of Counter-Intelligence and Counter-Terrorism. Now RAP is a main line too. And the more people who make a career in RAP, the larger the collective fund of knowledge and memory that is vital to good analysis and assessment.

Size also permits greater diversity. RAP now has a strong contingent of people with back-grounds in economic affairs, for example, and capability in IO foreign languages (as well, of course, as in both English and French).

---

[5] *Accountability and Effectiveness: National Requirements for Security and Intelligence in the 1990s*, notes for a speech by the then Solicitor General to the Canadian Association for Security and Intelligence Studies, Ottawa, September 29, 1989.

Several very highly qualified experts have been recruited from outside the security intelligence field for strategic analysis assignments. These experts have two roles--to advise junior analysts and to prepare major papers of their own. Two papers have already been completed for the Intelligence Advisory Committee (IAC) of the Privy Council Office.

We note with approval that two Security Liaison Officers (SLOs)--that is, CSIS officers posted in foreign capitals--have joined RAP upon completion of their tours abroad. As we have said before, we see returning SLOs as a natural pool of special knowledge and experience that would benefit RAP.

New Resources: RAP has been strengthened with new resources for the production of intelligence on foreign meddling in the affairs of ethnic communities in Canada. This is an essential counterpart to Canada's multiculturalism policy.

New resources have also been provided for the analysis of science and technology issues. The then Solicitor General announced last autumn that he had asked for a strategic security intelligence assessment and advice on clandestine technology transfer.[6] The science and technology program is discussed later in this chapter.

A Growing Reputation: There are a number of signs that RAP's growing importance within CSIS is matched by growing respect government-wide. RAP is now represented on virtually all the SARGs (Special Assessment Review Groups) under the auspices of the Privy Council Office; the Director General of RAP attends most ARG (Assessment Review Group) meetings.

Four more departments started getting all *CSIS Reports*, RAP's primary vehicle for disseminating intelligence, in 1989-90. The distribution list now extends to more than 20 departments and agencies.

RAP surveyed its customers again in 1989-90 and found that most believed the intelligence product continued to improve, both in writing and presentation and in the quality of the analysis and the information provided. We generally agree with that assessment, with two related reservations.

- RAP seemed slow to adjust its assessments to developments in Central and Eastern Europe.

- Some reports on science and technology still focus too tightly on traditional targets. We will be interested to see whether there is a change after a stronger relationship in this area, now planned, between CSIS and the Department of External Affairs is in place.

---

6 *Accountability and Effectiveness: National Requirements for Security Intelligence in the 1990s*, notes for a speech by the then Solicitor General to the Canadian Association for Security and Intelligence Studies, Ottawa, September 29, 1989.

Science and Technology

In a special report to the Solicitor General in 1989-90, we put forward a number of proposals for improving the protection of Canada's scientific and technological (S&T) assets. We recommended that CSIS seek a mandate--and additional resources if need be--to raise the priority given to the protection of S&T and the creation of mechanisms for greater coordination of S&T-related investigations. We also urged that the government strengthen intelligence analysis, research and policy development in this area.[7] During 1989-90, steps were taken on all these fronts.

The new National Requirements directive is a significant factor. One of the five priorities it establishes is "economic security", which is defined in terms of the protection of S&T assets. The then Solicitor General publicly revealed last autumn that CSIS had been directed:

> ... to give the government a strategic security intelligence assessment and advice in the area of clandestine technology transfer. We want an assessment of the extent of the vulnerability of Canada's high technology knowledge base. The government also requires an assessment of the extent to which it is being abused by foreign governments and advice on how to counter this abuse.[8]

As we noted earlier in this chapter, the Analysis and Production Branch (RAP) has been given additional resources for the analysis of science and technology issues. It started work in the autumn of 1989 on the study ordered by the Solicitor General. With the assistance of the Service's Planning Branch and in consultation with the Counter-Intelligence Branch, a workplan had been prepared by year-end for a very extensive study. One issue CSIS has identified and not yet resolved is the scope of its own role in the protection of science and technology assets.

Different Perspectives: Wide-ranging preliminary discussions revealed some divergence of views among the government, and the academic community, and industry. Academics tend to be suspicious of anything that might impede the free flow of ideas and information. Industry seems more worried about domestic competitors than foreign governments. To the extent industry fears foreign competition, it is from the NICs (newly-industrialized countries) rather than the inefficient East Bloc, which still tends to preoccupy government.[9] Industry does not see East Bloc nations as having the know-how to pose a serious threat.

Another issue that needs thorough debate, inside and outside government, is whether CSIS has a proper role in providing intelligence for use in protecting commercial advanced technology as well as traditional national security secrets--better mousetraps that might boost Canadian exports as well as better lasers that might be used in bomber sights. It may be

---

7 See our *Annual Report, 1988-89*, page 37.

8 *Accountability and Effectiveness: National Requirements for Security Intelligence in the 1990s*, notes for a speech by the then Solicitor General to the Canadian Association for Security and Intelligence Studies, September 29, 1989.

9 In testimony before the Special Committee of the House of Commons on the Review of the *CSIS Act* and the *Security Offences Act*, November 2, 1989, however, the Director of CSIS recognized that other countries are also interested in our technology.

difficult to bring commercial and industrial interests into the framework established by the definition of "threats to the security of Canada" in section 2 of the *CSIS Act*. The “strictly necessary" limitation on CSIS activities, found in section 12, might also become stretched beyond recognition.

This debate has started. In a submission to the Special Committee of the House of Commons on the Review of the *CSIS Act* and the *Security Offences Act* on May 5, 1990, the Law Union of Ontario said, "We do not believe that the prevention of industrial espionage is a proper function of a national security agency".

Counter-Intelligence: In operational terms, the protection of S&T falls within the mandate of the Counter-Intelligence Branch. Many of its ongoing investigations have S&T components, and it has an S&T desk to coordinate them. That is not new.

What is new is a commitment--though it had still not been fulfilled by the end of the fiscal year under review--to fully staff this desk. In addition, the S&T desk in Counter-Intelligence now has regular monthly meetings with the key players in controls on exports of high technology. They include the Department of External Affairs, which administers the *Export and Import Permits Act*, Customs Canada, which monitors exports, the RCMP, which works with Customs Canada in investigating suspected offences, and the Department of National Defence, which has an obvious interest in military technology.

Campus Operations

Security operations on university campuses inevitably raise special difficulties. Academic freedom is a significant social value in what the Canadian Charter of Rights and Freedoms calls our "free and democratic society". Universities are commonly hotbeds of the "lawful advocacy, protest and dissent" protected in section 2 of the *CSIS Act*.

At the same time, of course, academic freedom cannot be a cloak for activities that genuinely threaten the security of Canada. There is a world of difference between a thinker and a plotter. Routine security screening can also bring intelligence officers onto campuses, for example to check the accuracy of claimed academic credentials.

During 1989-90, we conducted a review of campus operations. Its starting point was the policy framework--notably the ministerial direction under which CSIS requires the Solicitor General's approval, case by case, to use human sources and listening devices on campuses and, second, relevant portions of the Service's Operational Manual. The foundation of current policy is the 1963 commitment by the government that:

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

We went on to look at all ministerial authorizations in the calendar years 1988 and 1989, and made an exhaustive examination of two randomly-selected cases (one in each year; one involving

counter-terrorism and the other counter-intelligence). Finally, we examined the extent to which CSIS may conduct operations on campuses outside the framework of ministerial approval.

The Policy Framework: We found weaknesses in the ministerial direction. It does not cover all investigative activities. It makes no clear reference to various forms of surveillance, for example. In addition, the direction uses terminology not found in the *CSIS Act*--which is a potential source of confusion. For example, where the *Act* requires “reasonable grounds", the direction speaks of "definite indications" that proposed targets threaten the security of Canada.

We also found an important difference between the ministerial direction and the Operational Manual during the period covered by our study. While the direction required the Service to seek ministerial approval before using a human source on campus, the Manual allowed in-Service approval when students or university employees were not expected to be present at the activity concerned.[10]

Operations: That being said, as a practical matter CSIS is generally cautious in its approach. For example, in at least one instance the Service went to the Solicitor General of the day with plans for an operation of a kind not covered by the ministerial direction.

Some preliminary observations that emerged from our review: operations authorized by the Solicitor General are not numerous; they are split fairly evenly between the counterintelligence and counter-terrorism programs; they are found in all regions. In no case did we find any indication that the operations had any short-term effect on normal campus activities.

But we have concerns about the scope of some reporting. For example, under paragraph 2(b) of the *CSIS Act*, "foreign influenced" activities must be "*clandestine or deceptive* or involve a threat to any person" (emphasis added) to qualify as "threats to the security of Canada", but we found a few reports on open activities that did not involve threats to any person.

Another concern arises out of other examinations we have made of CSIS operations. We know that the Service sometimes goes to universities in connection with security screening and that it sometimes interviews professors and others in the course of investigations. Because these activities do not fall under the ministerial direction, they are not coded under the heading of campus operations. We come across some in the course of other review activities, but it would be preferable if all such operations were coded so as to allow for easy review in this very sensitive area.

Recommendations: We recommend that the ministerial direction be rewritten to bring it in line with the *CSIS Act* and to make it more comprehensive. Everyone, including the Service

---

[10] The Manual is now being amended in this area. It will require the Solicitor General's approval for all use of human sources under the direction of the Service, without exception, in campus operations.

and the Ministry of the Solicitor General, recognizes that the present direction is flawed. We believe it would be useful if representatives of the academic community were consulted in the redrafting process.

As part of the revision, we recommend especially that reporting on public events should be as limited as possible, in order not to discourage the free exchange of ideas.

Finally, we recommend that all campus contacts--those that take place outside the framework of ministerial authorization as well as those that take place within it--be logged so that we can monitor them.

Open Sources

There is no practical way of measuring the use of open sources--published material including newspaper articles and books--as an alternative to investigation. Investigators and analysts can use open information that has come their way in their own, private reading. And it would be virtually impossible to know whether open information collected by analysts was actually used.

But statistics provided by the CSIS Information Centre give at least a welcome indication of increasing use. Requests for information were up 45 per cent in 1989-90 from 1988-89 levels. Not surprisingly, the Analysis and Production Branch (RAP) was the biggest source of reference requests by far. The Counter-Intelligence and Counter-Terrorism Branches each made about half as many requests for information as RAP did in 1989-90.

During 1989-90, the Information Centre created a new regional coordinator position with responsibility for providing support and services, including training, to the reference centres (libraries) that have now been established in all regions.

Regional Study

During 1989-90, we closely examined the use of investigative tools in one region in particular. We delved into all aspects of intrusive investigations, including the use of warrant powers and surveillance; sensitive investigations authorized by the Solicitor General; and the affidavits sworn in support of applications for warrants to use intrusive powers provided by law.

Targeting: Under CSIS policy, no investigation can be conducted at any level without written justification and approval by management. We found in a number of cases that the decision to investigate was based on very little information. However, since the *CSIS Act* sets a very low threshold for investigation--"reasonable suspicion"--we found that all investigations we looked at could be legally justified.

Ministerial Authorizations: Certain types of investigations--for example, those on campuses--require the authorization of the Solicitor General on a case-by-case basis. We looked at all such investigations in the region in 1988-89.

We were satisfied with the factual base laid by CSIS in all its requests to the Solicitor General and with the system of controls imposed on these investigations. In one instance, the

investigation drifted into forbidden territory, but the Service responded by issuing new instructions intended to prevent this problem from recurring. The total number of investigations authorized by the Solicitor General was small.

Warrants and Investigations: We informed CSIS of our concern about two affidavits in support of warrant applications. They read too much like pleas for warrants rather than objective statements of the facts.

It should be pointed out, however, that overall we noted improvements in the quality of affidavits from previous years and that we found no abuses in the Service's use of powers granted by warrants.

Similarly, our review of requests for surveillance and the actual conduct of surveillant with respect, in particular, to the privacy of individuals with whom targets came in contact--revealed no cause for criticism.

The conduct of one investigation, however, raised sufficient questions to require a separate review. We will report our findings in next year's annual report.

Product: We also examined "warrant product"--that is, information actually obtained through the use of powers granted by Federal Court warrants. We cannot, for security reasons, discuss our findings in any detail. Generally we were satisfied with the process, although we did flag one instance when some fairly important information was left out.

4. CSIS and Native Canadians

Native peoples are undoubtedly among the most disadvantaged groups in our society. The Canadian Human Rights Commission describes their situation as "a national tragedy". It notes, for example, that native peoples accounted for only .73 per cent of employment in 1988 although they made up 2.1 per cent of the available labour force.[1]

Like other Canadians, native peoples sometimes use confrontational tactics. Events during the summer of 1990 amply demonstrate how violence can erupt as native peoples pursue their goals.[2] The potential was already clear in 1988, a year of special significance in this chapter. One study toted up ten blockades of roads and bridges in five provinces by native groups in that year. Among others, the Innu people of Labrador gained wide public attention with sit-ins protesting low-level military flights over their traditional hunting grounds. Defence officials feared that the Innu might have been targeted by hostile intelligence agencies.

There were also a number of statements by native leaders in 1988, warning about the potential for violence. In May, for example, the National Chief of the Assembly of First Nations, Georges Erasmus, warned that his people were losing patience with seemingly endless talk about their problems. Addressing the nation at large, he said:

> We may be the last generation of leaders that is prepared to sit down and peacefully negotiate our concerns with you .... If you do not deal with this generation of leaders ... then we cannot promise that you are going to like the kind of violent political action that we can just about guarantee the next generation is going to bring to you.[3]

All of this was noted within CSIS, and two separate things happened in December, 1988. First, an intelligence officer interviewed Robert Bartel, a lay missionary working with the Innu. Two days later, a senior CSIS official authorized a nation-wide inquiry into what was termed "native extremism".

Our Review

Prompted by questions from Svend Robinson, M.P., when we appeared before the Standing Committee of the House of Commons on Justice and Solicitor General on May 30, 1989,[4] we undertook a review of CSIS inquiries into native issues.

Following a briefing by the Director of CSIS on June 9, we examined all relevant files from 1986 to June, 1989, and all messages, telexes, reports and other documents concerning both the

---

1 CHRC, *Annual Report*, 1989, pages 14 and 16.

2 Because of these events, we are revisiting this matter in 1990-91.

3 Quoted by the Canadian Press, June 1, 1988.

4 Mr. Robinson also wrote to us on June 1, 1989, to brief us on what he knew. In the course of our review, we had letters from Mr. Erasmus and from a member of the Mennonite community (not Mr. Bartel), both expressing concern about the CSIS inquiry.

"native extremism" inquiry and the interview with Mr. Bartel. We then interviewed officials at CSIS headquarters.

We went into the basis for undertaking the "native extremism" inquiry and the authority for the interview with Mr. Bartel; the degree of intrusiveness authorized for the "native extremism" inquiry; the actual conduct of the investigation; the nature of the interview with Mr. Bartel; and the release of information to the public and Parliamentarians. After determining at an early stage that the "native extremism" inquiry and the Bartel interview were separate events, we examined them separately.

On November 29, 1989, we submitted our secret *Report on the Innu Interview and the Native Extremism Investigation* to the Solicitor General under section 54 of the *CSIS Act*, with a recommendation that it be made public. On February 5, 1990, the Solicitor General released a version of the report, with significant portions blacked out for reasons of national security and privacy, accompanied by a news release.[5]

In this chapter, we outline our findings to the extent permitted by national security, and we give a fuller account of our conclusions than is found in the text released by the Solicitor General. It will be seen that a statement in the Solicitor General's news release, namely that we found no evidence of any misconduct by Service employees, does not reflect our conclusions. In our report, this statement refers to only one of the activities we examined. Indeed, we did conclude there had been a breach of regulations, as is explained in what follows.

"Native Extremism"

The CSIS inquiry on "native extremism" was authorized on December 14, 1988, to determine two things:

- whether there was a threat of "serious violence" under paragraph 2(c) of the *CSIS Act*;[6]
- whether, if such a threat existed, more intrusive investigation was warranted.

The Nature of the Inquiry: The inquiry was defined in very general terms. No individuals or organized groups were named as targets. A very low level of investigation was authorized, with no use whatsoever of intrusive powers. The authorization was drawn up in a way that excluded intrusion on the privacy of any individual. In the actual conduct of the inquiry, intelligence officers did not make full use of even the limited powers they were given, and no one in or close to the native community was personally investigated.

In fact, the use of the word "investigation" in discussions of this initiative, while correct may be misleading if it hints at anything in the nature of wiretaps or shadowing targets. What CSIS carried out was more like a fact-finding exercise or research program, relying on open sources like newspaper reports and on interviews with knowledgeable people.

---

5 Copies of this version are available from the Ministry of the Solicitor General.

6 Paragraph 2(c) provides that "activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political objective within Canada or a foreign state" constitute threats to the security of Canada.

A relatively short deadline was set, and the authorization explicitly provided that the inquiry was to be terminated as soon as a firm conclusion could be reached. Within a very short time, the analysts concluded that they had as much information as they needed to advise the government on the possible threat of violence in this area, and the inquiry was ended before the expiry of the period for which it was authorized.

The Role of CSIS: We consider that CSIS had the statutory authority to conduct this inquiry. It is precisely the kind of thing CSIS was created to do--assemble facts about situations with some potential to become explosive at a later date, draw conclusions and, finally, advise the government.

No reasonable person can deny that native peoples in Canada have legitimate grievances it was not far-fetched to suppose that at least some elements might become so frustrated by delays in resolving these grievances that they would resort to serious violence. In fact, there was more than one warning to that effect from native leaders in 1988. There were also in that period some indications, available to any attentive newspaper reader, of attempts to use political motives as a cover for violent criminal activities.

Under these circumstances, CSIS would have been remiss had it *not* made inquiries.

Further, we considered that the inquiry was conducted at a reasonable level. There was no snooping into private lives. It is in this inquiry that we found no evidence of any misconduct by Service employees.

The Targeting Process: However, in light of the sensitivity of the issue and the scope of the inquiry, we do have concerns about the way the decision was made to investigate "native extremism".

As we have already indicated in passing, the inquiry was authorized by a senior official on his own authority. That was within the rules. He had the power under CSIS procedures to order an inquiry at this level. In fact, he could have ordered a more comprehensive inquiry than he did.

But two further factors must be considered in judging the appropriate level for this targeting decision.

The first is a long history of wary--to say the least--relations between native peoples and the larger society and the resulting likelihood that inquiries by a security intelligence agency would be received with particular concern.

Second is an unusual feature of this particular inquiry. Documentation underpinning a targeting decision is normally quite specific about the persons and organizations to be investigated. In this case, no individual or organization was named, with the result that almost any member of the native community or anyone close to it might have been drawn into the net. There are sometimes good reasons for targeting very broadly at the outset of an investigation. However, in a case such as this, the decision ought to have been made at a higher level. The fact that, as it happened, no individual was personally investigated does not change the fact that the targeting was essentially open-ended vis-à-vis the native community.

CSIS contends that the steps leading to the targeting decision showed a proper degree of sensitivity. There was unusually extensive internal consultation in advance, involving the Director General of the Counter-Terrorism Branch and the Deputy Director, Requirements, among others. A note was prepared for the Director, informing him of the intention to authorize the inquiry.

As further evidence of its sensitivity, CSIS cites instructions given to regional offices to inform Headquarters at the completion of each of the three stages into which the inquiry was divided.

We acknowledge that CSIS showed--and acted on--an awareness of the sensitive nature of this inquiry. But it would have been well advised, in our view, to place the issue before its internal Target Approval and Review Committee (TARC) for a decision. This would have ensured that the Director was directly involved, as he chairs TARC personally.

Because of the concern raised by this case, we are now examining the approval process for all other current investigations.

The Special Case of the Innu

One native community using confrontational tactics with some success in 1988--and later--to gain public attention and sympathy for its protests was the Innu people of Labrador. According to one newspaper report, in the autumn of 1988 members of the Innu community "invaded a secure airfield seven times in three weeks and forced four western powers to suspend northern bombing exercises for a month".[7]

When a CSIS officer visited Goose Bay in December, 1988, Defence and RCMP official, there discussed the Innu protests with him. The officer was not in Goose Bay to investigate anyone. He had come to brief government officials on CSIS programs. But he took the opportunity to talk with Mr. Bartel, whom he described later as a religious leader trusted by the Innu.

After this interview became public knowledge, statements by CSIS left the impression that it took place in the context of the "extremism" inquiry. We will have more to say later ir this chapter about the release of information by CSIS. For the moment, the important point is that the chronology makes it clear that the interview with Mr. Bartel was not part of the "extremism" inquiry: the interview took place on December 12, 1988, while the "extremism" inquiry was not authorized until December 14.

Community Contacts: The question then arises: did the CSIS officer need explicit authority to interview Mr. Bartel?

Both he and the Service present the interview as a case of open-sources information gathering of a general nature, not requiring a formal targeting decision at any level. They say the interview was not the beginning of an investigation but merely liaison with Mr. Bartel among others, to determine whether there were offshore interests or influences trying to manipulate or exploit the Innu protests, which could lead to acts of serious violence. They were not interested in the Innu protests *per se*.

---

7 *St. John's Sunday Express*, November 13, 1988.

As a general proposition, we accept the distinction between liaison and investigation. And we believe that intelligence officers should have considerable freedom to establish and maintain community contacts. In last year's annual report we applauded new instructions making it clear to field investigators that they can maintain contacts with people who are not themselves targets or sources of information about targets, keeping an ear open for tips or hints of significant developments.[8] We also share the Service's understanding, based on the debates leading to passage of the *CSIS Act* in 1984, that Parliament intended to let it collect information freely from open sources.

But we concluded our comments last year by saying we were "pleased that precise guidelines have been established [for community contacts] because of the chill that attention from CSIS can put on legitimate political activities".

CSIS procedures clearly require that before an individual is interviewed about a suspected threat to the security of Canada, there must be an authorization specifying the threat.

The interest that hostile intelligence services might well take in trying to manipulate the Innu protests was such that a reasonable argument could have been made for an investigation. We have already said we do not quarrel with the Service's decision to inquire into the potential for violence among native peoples generally.

It is clear that the interview was conducted with this specific potential threat in mind -- foreign influence in the Innu community, leading potentially to political violence.

But this takes the interview out of the realm of "liaison" or "contacts with people who are not themselves targets of investigation or sources of information about targets", where intelligence officers can use their own discretion. The interview was in the realm of inquiries about a specific threat, which means to our mind that it needed to be authorized.

No Major Breach: In conclusion, we consider that CSIS policy was contravened because an interview with reference to an identifiable target was conducted without the necessary authority.[9]

We do not regard this procedural breach as significant. We are convinced that the interview was conducted in good faith, to seek a first-hand reading of a situation the Service had been told about, and was not intended to subvert procedures. We also found that the interview was not in any way intrusive. Before the interview, Mr. Bartel was told with whom he would be talking, and no further inquiries were carried out.

---

8 *Annual Report, 1988-89,* pages 19 and 25.

9 It is our understanding that CSIS does not consider that any breach of policy or procedures occurred.

Release of Information

Earlier in this chapter, we touched on one concern about the way information was released by CSIS in these matters: its statements left an inaccurate impression that the interview with Mr. Bartel came under the umbrella of the "native extremism" inquiry.

The consistency of the misunderstanding is remarkable. Mr. Robinson reports that this is the impression he got from the Director General of Communications when they spoke on May 3, 1989.[10] This is what *The Globe and Mail* reported after it interviewed the Deputy Director of Internal Communications.[11] This is what we understood after the Director's briefing to us on June 9, 1989.

Our concern about the confusion is no inconsequential quibble. Only when it is understood that the two events are entirely separate is it possible to judge correctly whether there was adequate authority under CSIS policy for the interview with Mr. Bartel.

CSIS has a rationale for associating the two events. A report submitted to Headquarters on January 25, 1989, on the interview with Mr. Bartel became part of the factual base considered in the "extremism" inquiry. We accept that logic only to the extent that the report was made under the authority of the broader inquiry.

Regardless of this rationale, an internal *aide-mémoire* dated April 27, 1989, makes it clear that the interview was not conducted as part of the "extremism" investigation but was, in fact, a quite separate event. CSIS should have understood the potential for confusion.

Disclosure: There is a second issue related to the release of information. One of the most unusual features of this whole story is how open CSIS was. Ordinarily, the Service reveals nothing about its investigations -- certainly not before they have become public knowledge from other sources. But the "extremism" inquiry was first publicly revealed by the Director General of Communications, when Mr. Robinson asked him about the Bartel interview--a different matter.

In our report, we raised the issue of whether this was consistent with the provisions of section 19 of the *CSIS Act*--namely, that "information obtained in the performance of the duties and functions of the Service under the Act shall not be disclosed by the Service except in accordance with this section".

CSIS considers that it has the prerogative to confirm, deny or do neither when it deems this to be in the public interest. Commenting on our concern, it said that its comments had the effect of clarifying the status of its activity. It noted as well that the results of the investigation were not disclosed.

---

[10] In fairness, it should be recorded that the Director General of Communications says he believes that he clearly distinguished the two events when he spoke with Mr. Robinson.

[11] "CSIS probed Labrador Innu and other native groups", *The Globe and Mail*, June 1, 1989.

We stand by the opinion we stated in our report, that the Service should not usually confirm nor deny the existence of particular investigations because "the very knowledge that someone is or has been subject to CSIS investigation can cast a shadow of guilt".

Future Reports

Because of our experience in this inquiry, we have decided on new arrangements for special reports that we submit to the Solicitor General under section 54 of the *CSIS Act*.

Whenever we think there is a real possibility that the Solicitor General may want to make public portions of a classified section 54 report, we will assist him by preparing two versions for his consideration. There will be the usual secret or top secret version for official eyes only. And we will ourselves prepare a second version from which sensitive information has been removed so it can be made public if the Solicitor General so decides.

5. Exchanges of Information

In order to fulfill its mandate, CSIS must participate in a constant give and take of information with other agencies, both at home and abroad. For example, CSIS needs to access birth records to determine the bona fides of people seeking security clearances. Information also goes in the other direction--to police and other agencies when, for example, CSIS inquiries turn up evidence of criminal activity.

The *CSIS Act* provides a statutory framework for such exchanges. Subsection 17(i) allows the Service to enter into arrangements "or otherwise cooperate" with federal and provincial departments and police forces, with foreign governments and their agencies and with international bodies. Subsections 13(2) and (3) permit arrangements under which the Service would provide security assessments to provinces and their agencies, Canadian police forces, foreign governments and their agencies or international bodies.

Subparagraph 38(a)(iii) gives us a dual mandate in this area. It directs us "to review arrangements entered into by the Service pursuant to subsections 13(2) and (3) and 17(l)" and "to monitor the provision of information and intelligence pursuant to those arrangements".

Our Study

We have kept the arrangements under review on an ongoing basis. We laid the groundwork with a comprehensive reading of all existing arrangements (see our 1987-88 Annual Report). Our comments on the present status of the arrangements can be found in Chapter 3 of this report (see page 9).

However, the volume of exchanges that take place is so great that the only practical way to monitor the provision of information and intelligence is by sampling. This we did in 1989-90. A special concern was, of course, the treatment of sensitive personal information about Canadians.[1] We wanted to determine whether the interests of Canadians were protected when CSIS provides information to other agencies. We also wanted to know whether CSIS was staying within policy and the law when it collected information about Canadians from either domestic or foreign sources.

To the extent permitted by national security considerations, we set out key findings and conclusions in this chapter. We deal with foreign and domestic exchanges separately because we examined them separately and the two studies took somewhat different directions because of differences in the material we were able to assemble.

Foreign Arrangements

CSIS has more than 100 foreign arrangements and has Security Liaison Officers (SLOs) in some countries. They permit exchanges in one or more of several areas--security assessments, vetting of immigration and visa applications, and security intelligence.

---

[1] By "Canadians", we mean both Canadian citizens and landed immigrants.

Some arrangements are with countries and agencies whose human rights records are no good. This is, of course, unfortunate, but we acknowledge that it cannot be completely avoided. It is obvious, for example, that CSIS cannot give up its investigation of a suspected terrorist at the borders of such countries. It also needs access to information in these countries for immigration and visa vetting.

Controls: Partly because CSIS cannot always be choosy about the countries and agencies with which it has arrangements, we expected to find stringent procedures for controlling the provision of information to foreign agencies. We did not.

In the Counter-Terrorism (CT) and Counter-Intelligence (CI) Branches, which account for most exchanges, there are few formal controls. These branches rely almost exclusive on the common sense and experience of managers, the case files and oral tradition to convey the do's and don'ts. Middle management often has the final say in what goes overseas.

Ministerial direction requires the Service to take "precautions" in the provision of information on Canadians to other countries. But the record gives us no means of monitoring whether the Service has actually taken nationality into account; in a number of the records of exchanges we saw, there was no indication of nationality.

It would be helpful if these records were coded so it could be seen at a glance whether the individual was a Canadian or not. This would give some assurance that nationality bad been taken into account before the information was released.

In some files we found warnings that care should be exercised concerning information that a branch sends to specific destinations. But these warnings are usually buried in the files, where they could easily escape notice. CSIS has not provided blanket warnings in the Operational Manual regarding agencies and countries where special care should be exercised because of human rights concerns.

This is not to suggest that CSIS is indifferent to the dangers of exchanges with countries with poor human rights records. Arrangements with such countries are commonly limited to immigration and visa vetting checks, and, for the most part, the volume of exchanges is low. CSIS has ended cooperation with one country completely because of human rights concerns.

We also found that the Foreign Liaison Branch has played a significant role. Our review of the files showed that it sometimes prevented or at least forced reconsideration of--the dissemination of information to foreign agencies because it might have exceeded the limits set in agreements or because the information was highly sensitive. This Branch also intervened from time to time when operational branches sought to establish agreements that would have been contrary to Canadian foreign policy.

However, the Foreign Liaison Branch has now been eliminated. While not all the details have been worked out, it is clear that day-to-day foreign liaison will be controlled entirely by the operational branches.

This portion of our review left us with two concerns--the lack of comprehensive policy and procedures for ensuring that only appropriate exchanges take place, and, second, the loss of

the more or less independent review that had been provided internally by the Foreign Liaison Branch.

Information on Canadians: We were not able to make an adequate sampling of information provided by CSIS to its foreign partners. Logs of exchanges are kept at SLO posts and it is possible to check the files on site. But communications which pass through SLOs seem to be filed according to subject at CSIS headquarters. As a result, file numbers recorded in the SLO logs generally cannot be used to trace the records at headquarters, and we have not yet been able to review many documents we want to see. We will continue our sampling in 1990-91, to build an adequate basis for review.

In what we did see, we found no illegal dissemination of information to foreign agencies. Indeed, we found cases in which CSIS quite rightly refused to respond to requests from foreign agencies. An example is a request for information on a non-governmental aid agency.

But we saw some cases--which we cannot discuss for security reasons--that gave us concern and we have not yet seen enough files to judge whether exchanges with other countries generally take place in an appropriate manner.

Ministerial direction specifies that information about Canadians can be provided to the Service's foreign partners only if it concerns activities "prejudicial to the interests of Canada". This may not provide sufficient protection. Before releasing information, U.S. agencies consider whether it is "compromising to the interest of the individual" and weigh this against the national interest.

Perhaps CSIS should also be formally required to strike a balance between the interests of the individual and the national interest before releasing information. This would not prevent the Service--any more than its U.S. counterparts--from fully disclosing information about, for example, a bomb plot, because Canada's national interest includes its international obligations to thwart terrorism everywhere. But it would prevent the disclosure of information that is of little importance in a Canadian context but might be regarded as damaging elsewhere--for example, information about a person who had participated in peaceful protest in another country.

CSIS has a policy against providing information for use in domestic repression by a foreign government or agency. But it has no real control over the use of information it provides.

Entry to the United States: One area where the provision of information on Canadians to a foreign agency has had a high profile in past years is with respect to entry to the United States. For many years the RCMP Security Service passed information about Canadians to the U.S. Immigration and Naturalization Service (INS), which has used it to block entry to some individuals. Much of this information, beyond a doubt, could not be collected under the limitations set by the *CSIS Act* in 1984.

In 1980 the RCMP rescinded its information-sharing agreement with the INS and asked it to delete from its files information provided in the past. We understand that the INS started the job but did not complete it. One reason was a provision of the U.S. McCarran-Walter Act,

which allowed the border to be barred against persons who had expressed views in opposition to U.S. government policy. The INS apparently felt an overriding need to know the identity of people in this category.

CSIS has no direct contact with the INS. And when one U.S. agency with access to Canadian information asked the Service to let it pass outdated information to the INS, CSIS rightly refused permission.

In January, 1990, the U.S. Congress repealed the relevant provision of the McCarran-Walter Act. CSIS might take advantage of this to renew the request that INS purge its files of outdated Canadian-supplied information.

Cooperation with Police: Canadian police forces are also involved in international operations involving security offences, and their paths sometimes cross the Service's. This provides a field for some of the police-Service tension that is built into the system. With a mandate to bring criminals to justice, the police have reason to treat all information as potential evidence for production in court. CSIS has a different mandate, to gather information as a basis for advice to government, and is understandably anxious to protect information that could "burn" a source.

During our review, one problem was drawn to our attention by a high-ranking official of a foreign country. This official was concerned about an apparent lack of cooperation between CSIS and the RCMP which, in foreign eyes, complicated an international counter-terrorism investigation. The operation was ultimately successful; the alleged terrorists were apprehended. The possible damage would lie in the insecurity felt in an important friendly country about the ability of CSIS and the RCMP to work together.

We also saw a case in which a police force--not the RCMP--dealt directly with a foreign agency. The police force had learned about a possible terrorist threat against the foreign country concerned, and CSIS first heard about the threat through a sister intelligence agency in the other country.

Incoming Information: In our visits to SLO posts, we found that most of the information exchanged passed from foreign agencies to CSIS rather than the other way around. This confirms Canada's reliance on the good graces of other countries for foreign security intelligence.

Recommendations on Foreign Exchanges: We believe that the Service needs to develop a comprehensive framework of policy and procedures governing exchanges.

As part of this process, it needs to develop something corresponding to the U.S. concept of information "compromising to the interest of the individual" to give Canadians some assurances that information about them, even when it is legitimately held by CSIS, does not fall into the wrong hands. If the appropriate information were labelled this way, it could be removed from reports disseminated abroad, especially to countries with a record of human rights abuses.

In addition, new procedures are needed for coding documents on exchanges conducted through the SLOs so we can trace them in headquarters files.

Domestic Exchanges

CSIS has memoranda of understanding (MOUs) with most provinces and most major police forces as well as with federal departments and agencies. Much of its requirement for information from departments and agencies, both federal and provincial, is for purposes of security screening. It has two-way exchanges with police forces in relation to security offences.

Public concern in this area has focused on the Service's access to sensitive personal information--health and welfare records, for example.

As in our study of foreign exchanges, the logs maintained by regional offices at CSIS gave us some difficulty. Each region has its own practices. Some regions, for example, log only written exchanges while others record all contacts with other agencies. However, we are satisfied that we were able to make an adequate sampling of exchanges in all regions.

Health Records: Our discussions with CSIS managers indicated a strong awareness of the pitfalls in the use of medical information and a view that there is not normally any good operational purpose for such information. In some provinces, access to medical information is limited by law and, further, a number of the Service's agreements with provincial agencies explicitly exclude medical information.

CSIS does, however, access some other records held by health authorities. It uses data on births, deaths and marriages to establish the identities of individuals in security screening and in the investigation of suspected threats to national security. It also sometimes gets information from health insurance records, such as names, addresses and employers. This is also for the purpose of establishing identities.

Other Personal Information: Our audit turned up a few cases in which CSIS had received sensitive personal information of other kinds. For example, the Service got biographical data, an employment history and a record of Unemployment Insurance benefits received on one individual. While the information was sensitive, we consider that the Service was justified in building a complete profile of this individual, an embittered former federal employee who had threatened to provide information to another country known to spy on Canada and had gone so far as to seek out representatives of that country.

But, in general, requests by the Service for sensitive personal information are few in number.

The Mandate: We found some CSIS requests, especially to police, that did not seem to us strongly grounded in the *Act*. These concerns are perhaps more technical than substantive; we do not believe that any real harm was done. But we believe it is important to flag them here as a reminder that the Service's mandate is not unlimited.

In one case, the Service asked for information on the owner of a shop who had agreed to sell a certain publication associated with a targeted organization. The intelligence section of the local police force told the Service that the establishment had criminal connections. The publication is, obviously, above-ground and legal. This request seems to us to to have skirted dangerously close to infringing the protection offered by section 2 of the *Act* to "lawful advocacy, protest or dissent".

Extraneous Information: We found that the Service also often receives information it does not ask for. Responding to one request for data from medical insurance records, for example, the provincial authorities told CSIS that the individual in question was in prison on a given date. The Service cannot stop people from providing unnecessary information, but it should ensure that such information is not kept on its files.

However, volunteered information can also be useful. One province reported certain inquiries that led CSIS to suspect a foreign country known to spy on Canada might be gathering information for use in building cover stories for "illegals"--agents who masquerade as Canadians. Such information is clearly within the Service's mandate.

Requests from Police Forces: In two regions we found requests from police forces that, in our view, may have taken CSIS beyond its mandate.

In one case, a local force asked for information about an individual who had been making complaints to the police commission and the Service responded with extensive detail, including the individual's political associations and the activities of his children. We do not see how this could be justified under the CSIS mandate to deal with "threats to the security of Canada". However, this took place some years ago, and CSIS assures us that arrangements since entered into with police forces would prevent a recurrence.

We have what might be termed a technical concern with a series of requests from one province which seeks information from CSIS for security screening purposes. There is nothing wrong with this in principle. But the *CSIS Act* makes explicit provision in subsection 13(2) for formal agreements under which CSIS can provide security assessments to provinces. No such agreements exist. We are currently examining the legal basis for such releases under the *Act*.

Policy and Procedures: As in the study of foreign exchanges, we found a gap in headquarters direction on domestic exchanges. There is not even a definition of what constitutes an exchange, which leaves the regions on their own in deciding what to log. All six regions have created manuals of their own to fill the gap, and we were impressed by the quality. But this is an area where there clearly should be country-wide procedures, standards and definitions.

Recommendations on Domestic Exchanges: In the full report we will send to the Solicitor General, we make a number of recommendations designed to enable us to make better audits in future. Most are technical, but three are of a more substantive nature.

One is that any information taken from security screening files for use in other investigations should be logged in the same way as exchanges with other agencies, so it can be easily identified for our review. Information obtained for screening purposes is held separately from the main CSIS data base and can be accessed only with special authority. But once it has been accessed and transferred into other files, further access to it is not limited in the same way.

We also recommend that CSIS maintain logs of all exchanges that take place with other agencies, whether within the framework of formal MOUs or not. In the absence of logs, responsibility for these unofficial exchanges can end with the individual investigator who engages in them.[2]

Finally, we recommend that CSIS be required to obtain a Federal Court warrant before it is given access to medical records. We are told by CSIS that there are explicit understandings already with some provinces that no request for such information would be made without a warrant. We believe that the same protection should be extended to Canadians in all provinces through a warrant requirement that could either be written into the *CSIS Act* or established by ministerial direction.

---

[2] After our research was completed, CSIS advised us that the Director, in July, 1989, ordered the development and implementation of a process to track all information exchanges.

6. The Counter-Subversion Residue

Three years ago, in our first in-depth study of an operational branch of CSIS, we found that the counter-subversion program had cast its net too widely. Too many people were under intrusive investigation not because of their own activities but because of links with organizations deemed "subversive" or simply because they were in contact with people associated with such organizations.[1]

We recommended that the Counter-Subversion Branch be shut down. Among "counter-subversion" investigations worth pursuing at all, we said, the Counter-Intelligence Branch (CI) should take on those relating to organizations and individuals acting under undue foreign influence, while the Counter-Terrorism Branch (CT) should do the same where there was real potential for political violence. This, we believed, would lead to more realistic targeting. We especially urged an end to "targeting by category"--that is, automatically investigating every person associated to any degree with a targeted organization. Individuals, we said, should be targeted only when their personal activities represent a threat to the security of Canada as defined by the *CSIS Act*.[2]

Our recommendations on targeting mesh with one of the five McDonald principles cited in Chapter 2 (see page 6): investigative means must be proportionate to the gravity of the threat and the probability of its occurrence and with the requirement in section 12 of the *CSIS Act* that the Service limit its information gathering to what is "strictly necessary". Clearly, the strictly necessary investigation proportionate to a documented threat of nil is nil. This thinking also underlies key conclusions set out later in this chapter of the present report.

The Residue

The report of the Independent Advisory Team established by the Solicitor General of the day to follow up our findings on the counter-subversion program (the Osbaldeston Report),[3] echoed both our criticisms and our recommendations. The Counter-Subversion Branch was disbanded in November, 1987, and its most important investigations were transferred to CT and CI.

But the Osbaldeston Report said that even after some files had been reallocated and others mothballed, there would still be a "residue ... that would legitimately fall under [paragraph] 2(d)" of the *Act*.

Paragraph 2(d) is part of the definition of threats to the security of Canada. It embraces “activities directed toward undermining by covert unlawful acts, or directed toward or intended

---

1 We want to say immediately that we use the term "subversion"--and its relatives--strictly as a convenience. They are not found in the *CSIS Act* and, without an authoritative definition, "subversion" too easily becomes a ragbag in which all sorts of people, from oddballs to psychopaths, are tossed together without distinction. However, it is the word used by the Service and many others so, instead of inventing a substitute, we use it here.

2 For a fuller account of our findings and conclusions, see our *Annual Report, 1986-87*.

3 *See People and Process in Transition*, the report to the Solicitor General by the Independent Advisory Team on CSIS, 1987.

ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada". Like other parts of the definition, it excludes "lawful advocacy, protest or dissent" not carried on in association with a defined threat to the security of Canada.

The residue, as determined by CSIS in consultation with the Solicitor General of the day, was handed off to the Analysis and Production Branch (RAP). RAP was directed to monitor the organizations and individuals in the residue and to alert the operational branches if it ever seemed one was likely to move beyond rhetoric and posturing to genuinely threatening national security. Meanwhile, the files in the residue are also a data base used in the Security Screening Branch program to identify people who might betray the national interest to further a cause that is, to them, more important.

Our Study

After more than two years had passed, and RAP had had time to work the bugs out of the new system, we undertook a study of how the residue was being handled. As usual in projects of this kind, we examined both the policy framework and the operational record.

With respect to the policy framework, we familiarized ourselves thoroughly with all relevant ministerial direction and relevant portions of the Service's Operational Manual.

Moving from there to the operational record, we studied all classified files on organizations and a random selection of those on individuals, relevant security screening files, and administrative files. We distinguished two periods in our review of files on organizations and individuals--first, from the creation of CSIS in July, 1984, until the new program began in February, 1988, then from February, 1988, to May, 1990.

We also interviewed the Secretary of the Service's internal Target Approval and Review Committee (TARC) and analysts and managers who had the job of identifying the residue in 1987 or are now managing the program in RAP.

With the customary reservation that what we can say is unavoidably limited by national security, this chapter outlines our findings and conclusions.

Starting Up

The first task facing CSIS in 1987 was to sort through the 57,562 files in the countersubversion program and allocate them among Cl, CT, RAP, the Public Archives and the shredder. Some 54,000 files were easy enough. Already dormant, they were set aside for later review leading either to destruction or to storage under lock and key, awaiting the attention of future historians.

That left an estimated 3,000-plus active files for immediate examination--almost all of them on individuals. For administrative convenience, they were dealt with in two lots. The overwhelming majority were reviewed by a specialized records unit. The others were reviewed by a team drawn from RAP and the former counter-subversion program.

The first step was to determine criteria against which the files would be assessed. Both we and the Osbaldeston Report pointed to the need for an authoritative interpretation of the words "strictly necessary" in section 12. However, the Ministry of the Solicitor General is still working up an interpretation of this key term. So the records unit reviewers examined the files against the *Act* while the other team was given a formula based on available interpretations of sections 2 and 12.

By the end of the winnowing process, there were about 1,400 files on individuals in the residue--fewer than half the number active in the counter-subversion program. The Director told the Solicitor General that these individuals "show a continuing level of participation in their organization and, therefore, are assumed to understand and accept the underlying and often covert objectives of their organizations". The number of files on organizations fell by one from the 1987 level.[4]

New Category: The residue was placed in a new, low-level targeting category especially designed for the purpose. The designation of targeting levels is kept secret by security intelligence agencies worldwide as an element of "tradecraft". For convenience we will call the new category the "special" level here.

The only information that can be added to the files is material from such open sources as newspapers and newsletters and, second, unsolicited information turned up as a by-product of other investigations. A further limitation under ministerial direction is that no more active investigation is allowed without the explicit permission of the Solicitor General, case-by-case. There have never been any authorizations.

In addition, some files in the residue were segregated and access was restricted. Only the RAP analyst managing the program has unlimited access. Others needed permission from a senior manager to look at these files.

The Files

The big surprise when we called up the files on individuals was to find that they had gathered dust for two years. Only late in 1989 did the open-sources collection program even begin. Most of the information on file dates from the Service's first years, 1984 and 1985. There was another spurt of information-gathering in 1987, the last days of the counter-subversion program. Then two years of silence.

CSIS tells us that the residue files were not given high enough priority to justify the allocation of scarce analysis resources. This makes it clear that CSIS does not regard the individuals in the residue as very formidable threats.

As to the content of files on individuals, we estimate that less than 5 per cent is from open sources. This is not surprising, given the two-year dormancy. Almost all the information on file pre-dates 1988 and is classified. Most of it is innocuous. Even when CSIS had a much freer hand to use intrusive techniques, it seldom documented anything more damaging than that the individuals concerned were rank-and-file members of targeted organizations or sympathizers who

---

[4] It is a special satisfaction to report that the file closed is the one on the magazine we cited in our 1986-87 report as an example of a doubtfully appropriate target.

gave their time or money without taking out membership.

But both the open and the classified information showed one disturbing theme: we found a great deal of information on open, above-board activities in federal and provincial elections. This can be explained by the ease with which such information is obtained; organizations and individuals usually seek publicity for their electoral activities. There is no indication that CSIS misused this information or allowed it to be misused for partisan purposes. But that does not excuse what seems to us a disproportionate interest in domestic electoral politics.

One file deserves special mention. It is devoted to an individual who died in 1987; he was gone, but his file lived on.

Organizations: In the files on organizations, we also found a drop-off in the amount of information gathered after 1987, but it was not nearly so great as in the files on individuals. Even so, the open information placed on the files before 1988, when the investigators were in charge, was far more revealing than what has been added since by RAP's analysts. The pre-1988 material paints detailed portraits of these organizations and their leaders, mostly from human sources. Human sources are not permitted under the special targeting level.

Classified information on these files was similar to that in the files on individuals--membership lists, minutes of meetings and biographical data. But there was a lot more of it than in the files on individuals.

Targeting

The special targeting level is not producing an adequate flow of useable information. Meanwhile, though the program has been drastically scaled back since 1987, the principal vice we identified in our counter-subversion study remains intact. The residue program has kept the worst and failed to achieve the best. Our suggestions for improving the situation will be found at the end of this chapter.

The root problem is that after more than two years, RAP had still not demonstrated to TARC that the 1,400 individuals being monitored pose a threat to the security of Canada as defined by paragraph 2(d). The justification for monitoring them is exactly what it was under the counter-subversion program--their association, near or distant, past or present, with targeted organizations. In 1987 we called it "targeting by category".

What is more, in the absence of up-to-date Requests for Targeting Authority (RTAs)[5] on each individual, targeting is based on links that go back at least to 1987 and in many cases to before 1984. Since 1987, there has been no mechanism for dropping individual targets who have severed their links with the target organizations.

---

[5] These replace the former Subject Evaluation Reports (SERs).

This approach represents a step backwards. Responding to criticisms from us and in the Osbaldeston Report, the Service dropped targeting by category from its general procedures in 1987-88. In CI and CT targeting, individuals can be investigated only because of their own activities, documented in an RTA, not because of someone else's. Targeting by category survives only in the special targeting level.

Targeting people without any documented basis for suspecting they personally represent threats to the security of Canada offends the McDonald principle set out at the beginning of this chapter and now forming part of ministerial direction to CSIS. Moreover, it seems to us of doubtful legality in light of the "strictly necessary" requirement in section 12 of the *CSIS Act*.

Without the organizational links, we believe that few of the files on individuals that we examined would survive review by TARC. Most would not survive even with the organizational links, for most of the organizations in the residue look a sorry sight to us-the tattered remnants of discredited movements whose members struggle against odds to keep the spark of revolutionary rhetoric from sputtering out completely.

Level of Investigation

For those targets that could be justified, the level of information-gathering permitted is inadequate. The special targeting level gives the Service even less latitude than journalists, academic researchers and members of the public generally.

CSIS cannot, for example, routinely send its people to public meetings called by organizations in the residue. It can clip newspaper articles or transcribe broadcast information about these meetings, but it would need the approval of the Solicitor General to send an analyst or intelligence officer to take notes personally. If, heaven forbid, an individual in the residue should inadvertently sit down beside a CSIS officer at a lunch counter and say, "What about those Blue Jays, eh?" the logic of the special targeting level is that the CSIS officer would have to opt for rudeness over conversation for fear of being suspected of conducting unauthorized inquiries.

A Structural Flaw: We also see a structural flaw. Carrying out investigations is not RAP's forte. When RAP was handed the residue, the thinking seems to have been that its analysts are more at ease with open information than are the investigators in CT and CI. There may too have been some thought that monitoring by RAP would have a less threatening feel than investigation by CI and CT. But this is, after all, an investigative activity that RAP is not equipped for.

In addition, the residue will always be a sideline in RAP, not a primary activity. One of the surprises of our study was how few resources are devoted to the residue. Only one analyst is assigned to the program--part-time at that. During a heavy month during our review, he spent half-time on the residue. The average is more like 25 per cent of his time--in other words, less than half a minute per week per file.

RAP has done wonders in the past few years--more than we would have thought possible--to improve its ability to produce worthwhile intelligence. In Chapter 3 we report on its success

(page 19). It should be allowed to get on with that job, unencumbered by a second role that could be done much better by the investigative branches.

Meanwhile, the limitations on investigative powers, combined with this structural flaw, is affecting security screening and the Service's ability to flag any genuine threats.

Security Screening

As we have noted, the files in the residue are used in the federal security screening program. These files are among those that the Security Screening Branch of CSIS checks for the names of people whose devotion to a cause might lead them to betray the national interest.

What we have said about targeting makes one thing clear: the unfairness to every single individual who ought not to have a file in the residue. While these individuals are not automatically denied clearance, they are vulnerable to investigation and undue delays in the security screening process although no one knows--because no RTA has been prepared, much less approved by TARC--whether they actually pose a threat to the security of Canada.

There is no denying that the Security Screening Branch needs a data bank of the names of people who threaten national security. What cannot be justified is a data bank that may include the names of people who do not belong there.

The only mitigating factor at the moment is that CSIS recognizes the inadequacy of the information it is able to collect. In response to queries from the Security Screening Branch, RAP is usually only able to say there is not enough information from the open sources to permit conclusions about the threat posed by the individual seeking clearance. Where an assessment could be provided, it usually relied on information going back at least to 1987 and often to 1984 or earlier.

This points to another problem from the security screening point of view. In the absence of RTAs on the individuals in the residue and in the absence of adequate investigation, there is really no way of telling which individuals in the residue actually pose serious enough threats to be denied clearances.

There is concern, both inside and outside CSIS, that if the Security Screening Branch does not have access to complete lists of people who have any association at all with organizations deemed subversive, departments and agencies sensitive to security may be tempted to carry out investigations of their own, without the statutory and other constraints that Parliament has seen fit to impose in the CSIS Act. We think it is self-evident that this would not be in the public interest.

A Way Out

Our first reaction to the residue program was positive.[6] But a closer examination of how it has worked out in practice has made us change our minds.

We believe that CSIS should abandon the special, extra-lite targeting level it created for the residue and give CI and CT the files representing suspected threats that have been properly documented. While it may seem paradoxical, this would have the effect of raising protections for individual rights. Investigation of any individual would have to be justified by an RTA and be approved by TARC. The likely result, we believe, would be the retirement of many files on individuals. It would end targeting by category. It would bring all targeting clearly within the ambit of the *Act*.

Nor would this in itself mean open season for such intrusive techniques as electronic eaves-dropping and surreptitious searches on the targets that remained. A regular targeting level is available which does not permit such practices.

But it would permit more productive investigation of the targets that did survive the RTATARC process. Files on these targets should be transferred to branches that have the experience, the skills and the will to carry out investigations at low as well as at high levels of intrusiveness. It would also ensure that the Security Screening Branch had access only to files on documented threats to the security of Canada. Those that did not stand up to the process should--at last--be retired.

Early in the 1990-91 fiscal year, the Information Management Branch at CSIS intended to launch a review of files in the residue. The product of this review would be recommendations to RAP about the destruction or archival storage of files that seemed to have outlived their relevance. We welcome this as a useful step in itself. But it is not enough. It does not address the fundamental flaws we have identified.

We believe that the steps we have outlined here would complete the reform begun in 1987 in the wake of our report on the counter-subversion program. It would ensure that Canadians are not subject to investigation without sufficient cause and, at the same time, give some assurance that CSIS has an adequate data base for the purposes of security screening and advising the government on genuine threats.

---

6 See our *Annual Report, 1987-88*, page 13.

7. Inside CSIS

In this chapter, we turn to the internal affairs of the Service. The Service's performance in areas like recruitment, staff relations, and official bilingualism are crucial to its effectiveness in the long haul.

Recruitment

Recruitment is the key to the future shape of CSIS. After being critical of the Service's approach in earlier years, it is good to report continuing progress in 1989-90.

For the first time, CSIS advertised openly for recruits. It placed advertisements in more than 100 newspapers last autumn, seeking Canadians with university education, some work experience, good communications skills and an interest in national and international affairs.

The harvest was 8,447 applications. An impressive 1,116 applicants were judged to have high potential for work in CSIS. This is the pool from which CSIS expects to meet its needs for new intelligence officers (IOs) for two years. The first recruits were scheduled to start training in August, 1990.

In March, 1990, CSIS also participated for the first time in the Ottawa Career and Job Show, where it says its booth attracted more interest than any other.

Open advertising is something we have recommended in the past, and we regard last year's campaign as an important step in the right direction. We are also pleased with the Service's decision to participate in job fairs. However, we would still like to see it take its recruiting effort directly to university campuses, the way many corporations do.

The Classes of 1989-90

The CSIS training program had three classes in 1989-90. Recruits were also selected for the first class of the new fiscal year, and the figures that follow include them unless otherwise indicated.

Recruits again show a good range of education and language skills. Nearly 15 per cent hold postgraduate degrees--in journalism, political science, history, science, international relations, and sociology. A fifth speak languages other than English and French--Spanish, Arabic, German, Italian, Ukrainian, and Portuguese. Average age of the recruits was 28 and the range of ages was from 22 to 43.

Equitable Representation: CSIS has made steady progress towards more equitable representation for women in its ranks. In the key IO category, women accounted for 13 per cent of personnel at March 31, 1990, an increase from 10 per cent a year earlier and from 7 per cent five years earlier.

However, there is a considerable way to go before women are as well represented among IOs as in the labour force as a whole, and CSIS has a stated goal of a 1:1 ratio between men and women in its training program. In the three 1989-90 classes, CSIS met this target. In fact, women slightly outnumbered men.

The proportion of francophones--that is, persons whose first official language is French--in the four classes was 42 per cent. This may seem high at first glance, but security intelligence in Canada was an essentially anglophone preserve for so long that the Service has ground to make up.

Figures are not maintained on the representation of visible minorities, aboriginal peoples, and people with disabilities in 10 recruitment, as this would offend federal privacy requirements. While we respect these requirements, we regret that they make it impossible to keep a watch on the Service's efforts through recruitment to achieve a better mix of Canadians among its investigators and analysts.

Official Bilingualism: The Service showed a good commitment to official bilingualism in recruitment. All 1989-90 recruits have at least some command of both English and French. While CSIS policy permits the recruitment of people with only one of the official languages, it puts a priority on filling bilingual positions.

Public Relations

We have always encouraged CSIS to undertake public relations on its own behalf. The Service is in a difficult position, seriously constrained by security considerations from trumpeting its successes, working in a field where success is often measured in any case on the invisible scale of what does not happen rather than what does, and faced with institutional critics like ourselves.

But the Canadian public is entitled to be told what the Service, as a government agency, is doing. And CSIS needs public respect--for the sake of morale in its own staff and for the sake of support from the public. A security intelligence service cloaked in excessive secrecy may seem threatening rather than reassuring.

So we are pleased that CSIS continues to take steps to shed some of the unnecessary mystery that surrounds it.

During 1989-90 it published a glossy booklet and a leaflet, both under the title *The Canadian Security Intelligence Service: Helping to protect Canada and its people*, for public distribution.

Last autumn's recruitment campaign also paid public relations dividends. The Director General of Personnel Services had 21 interviews on radio and two on television in the week following the publication of advertisements for new intelligence officers.

The Service reports a total of 45 interviews with the media in 1989-90 (including three by the Director); three speeches (two by the Director) and 19 other presentations to schools, colleges, the media and service organizations (six by the Director). CSIS also responded to more than 300 media inquiries during the year.

Staff Relations

CSIS also continues to move to a more contemporary, sensitive approach to staff relations. For example, when new policies on conduct and discipline and on grievances and adjudication came

into effect, telephone hotlines were opened for one month to deal with questions. Initiatives of this kind contrast very favourably with the communications gap we found when we reported in 1986-87 on staff relations.

In September, 1989, agreements were signed by the Director and the Union of Solicitor General Employees, which represents support staff, and the Employee Association, representing professional and management staff, to launch a consultation program aimed at better communications between management and the rank and file. The agreement calls for the establishment of joint consultation committees to meet at regular intervals at the national, regional and headquarters levels to discuss policies, programs, procedures and conditions of employment.

The internal newsletter launched the previous year came out seven times in 1989-90 and covered a range of issues, including our 1988-89 annual report.

Polygraph Testing

In one area, however, we believe that CSIS is out of line in its approach to staff. That is in its continued use of the polygraph (the instrument commonly known as the "lie detector") to assess the loyalty of prospective employees before they are hired.

Even supporters of polygraph testing admit an error rate of 10 per cent or more, and we believe that this brings too high a risk of serious injustice to individuals whose readings are negative--without any compensating assurance that everyone tainted with disloyalty is being identified. While CSIS points out that the polygraph test is only one element of the assessment process, we fear that its aura of "scientific objectivity" may give it more weight than it deserves.

There was no significant change in 1989-90. As a result of our past criticisms, a consultant is evaluating the CSIS polygraph program. The consultant's report is expected to be considered in the establishment of government-wide policy in this area.

Accommodations

Budgetary restraint has unfortunately brought a slowdown in providing CSIS with new headquarters that meet the special needs of a security intelligence service. Work had started on Phase I of the headquarters project--construction of a computer centre in the Ottawa suburb of Gloucester. It is to open in mid-1991. Phase II, the main headquarters building, is now scheduled for completion in 1996.

Meanwhile, headquarters remains scattered through a number of buildings, complicating internal communications. The main building is seriously cramped and movement to accommodate growth is a way of life; at any given time, the accommodation management group is moving one or more units and is expected to continue doing so until the new headquarters is ready.

However, there is also good news about accommodations. The training program was able to move out of RCMP space into quarters of its own in 1989-90, and so did the Quebec City District office. Moving out of RCMP facilities has been the main thrust of the accommodations program since CSIS was created in 1984. When the New Brunswick District office is moved to Fredericton from Moncton, which was scheduled for September, 1990, only two field offices will remain in RCMP facilities--Ottawa Region and Winnipeg District.

8. Complaints

In this chapter, we turn from review to our second role under the *CSIS Act*--the investigation of complaints. Complaints fall into two broad streams. There are complaints against the denial of security clearances required by:

- public servants, members of the Canadian Forces and the RCMP;
- people working on some federal contracts;
- workers in sensitive federal facilities, notably airports;
- prospective immigrants; and
- prospective citizens.

Second, there are the complaints that may be lodged under section 41 of the *Act* "with respect to any act or thing done by the Service" except those that can be dealt with under the staff grievance procedure. We can also be asked to determine whether national security considerations prevent investigation by the Canadian Human Rights Commission of a discrimination complaint lodged with it.

The 1989-90 Record

We received 40 new complaints in 1989-90, down from 55 the year before. The biggest change was in complaints under section 41, which dropped to 26 from 44. There was no obvious reason for this decline. Except for the tidal wave of complaints some years ago about the Service's official languages practices, section 41 complaints have never shown a clear pattern of any kind.

One constant from 1988-89 to 1989-90 was that there were no new complaints in either year about the denial of citizenship or a chance to immigrate to Canada as the result of CSIS security assessments and recommendations. The Department of National Defence (DND) accounted again in 1989-90, as can be seen in Table 2, for the majority of complaints about the denial of security clearances--10 out of 12, compared with 9 out of 11 the year before.

Table 2. Complaints Record, April 1, 1989, to March 31, 1990

	New Complaints	Carried over from 1988-90	Closed in 1989-90	Carried over to 1990-91
Security clearances	12	6	12	6
CSIS	2	2	4	0
DND	10	4	8	6
Citizenship	0	3	3	0
Immigration	0	1	1	0
Human Rights	2	0	2	0
Section 41	26	14	38	2
Total	40	24	56	8

Fewer But More Difficult: Looking back over the record since we opened our doors in 1984, there was a sharp movement to fewer--though generally more difficult--cases involving CSIS and DND recommendations on security clearances. In our first full year of operation, 1985-86, we received 71. After we asked DND to reconsider 44 of those cases, many were withdrawn, and we received only one new complaint the following year.

Many of the early complaints we received were about security clearance denials based upon minor misdemeanours, or the occasional use of drugs. As our Chairman told the Standing Committee of the House of Commons on Justice and Solicitor General when we testified on April 10, 1990:

> Drug-use problems or falsification of enrolment credentials should not be dealt with, in our view, under the guise of national security. They are clearly personnel staffing problems similar to those faced by all large employers and should be solved by staffing branches without recourse to the denial of a security clearance.

As far as CSIS is concerned, the number of complaints about security clearances has remained stable and low at one or two a year since 1986-87. But complaints about DND clearances, after dropping to zero in 1986-87, stabilized at about 10 a year after that.

Complaints Closed: As can be seen in Table 2, we closed 56 complaints in 1989-90, up from 44 the previous year. Brief summaries of cases in which there were written decisions can be found in Appendix B. The number of complaints carried over into the new year is eight, down from 24 the previous year.

Something unusual in 1989-90 is that we had complaints referred to us by the Canadian Human Rights Commission for the first time since 1985-1986. This happens when a minister advises the Commission that the practice to which a discrimination complaint relates is based on national security. The Commission can then either dismiss the complaint or refer it to us for a determination of whether the security concern is justified. We made determinations in 1989-90 in both these cases, so the stories can be read in Appendix B.

Two Landmark Court Decisions

Subject to the possibility of an appeal to the Supreme Court of Canada, the protection provided to individuals by the *CSIS Act* has been strengthened by a decision of the Federal Court of Appeal.[1] It ruled unanimously that deputy ministers and their equivalents must treat a Committee recommendation as a decision; Committee recommendations may no longer be treated as mere informed advice.

---

[1] *Robert Thomson v. Her Majesty the Queen as represented by the Department of Agriculture the Deputy Minister of Agriculture*, Federal Court of Appeal, May 17, 1990. This happened after the end of the fiscal year under review here. But the decision is of such importance that it would be overly precise not to discuss it at the earliest possible moment.

To forestall any misplaced concerns, it should be noted that the Court's decision does not open the floodgates to a lot of shady characters who would not otherwise be granted clearances. Almost all of our recommendations that clearances be granted are, in fact, accepted by the departments concerned. Robert Thomson's case is the only one in which an agency other than DND or CSIS itself have rejected such a recommendation.

In the past, the initial decision to deny a security clearance has often been made with inadequate care. While CSIS assessments have improved markedly since 1984, they have not always stood up to scrutiny. And deputy heads have not had sufficient investigative resources to critically examine the assessments they received; though in DND both deputy heads have the additional assistance of advice from a Security Clearance Review Board (SCRB).

For this reason, the *Thomson* decision is an important turning point. The fact that most of our recommendations are accepted voluntarily by deputy heads is cold comfort to someone like Mr. Thomson who had his "day in court" before us, convinced us that his clearance should be granted, and found that he was no further ahead afterwards because our recommendation was rejected.

Court-like Process: We follow a court-like process in dealing with complaints, and hold formal hearings in clearance cases. We negotiate directly with CSIS and DND when needs be to ensure that complainants are informed as fully as possible about the allegations against them. We take evidence under oath. Whenever possible, we allow complainants, personally or through counsel, as well as respondents to cross-examine the other side's witnesses and bring forward their own. When complainants and their counsel must be excluded for reasons of national security,[2] we ask our own counsel to cross-examine as they would if they were representing the complainant. After such closed sessions, we relay the gist of what has emerged to the complainant and, if applicable, to the complainant's counsel.

Because we have always attempted to be as fair as possible to all parties, a second important court decision has not had an immediate impact on our work. In this decision, the Federal Court held that subsection 48(2) of the *CSIS Act* is unconstitutional.[3] This subsection provides, in part, that, in the course of our investigation of complaints:

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

The court did not hold that national security considerations could never justify excluding complainants from our proceedings. Its objection was that the wording of the subsection is

---

[2] We withhold information from complainants only if revealing it would (a) identify a human source, (b) endanger the life or health of another person, (c) reveal the methods ("tradecraft" in the lingo of security intelligence) or targeting of the investigative agency or (d) otherwise clearly harm national security.

[3] *Joseph (Giuseppe) Chiarelli v. The Minister of Employment and Immigration*, Federal Court of Canada, February 23, 1990.

so broad that it would let us withhold all information, however trivial, for any or no reason. Mr. Justice Arthur J. Stone wrote in the reasons for judgment that this fails the requirements of proportionality.

> Rather than providing a mechanism for balancing the State's interest in protecting police sources and techniques with the individuals's interest in fundamental justice ... the provision opts for a complete obliteration of the individual's rights in favour of the State's interest.

Subsection 48(2) remains in force pending the outcome of an appeal that the Attorney General has made to the Supreme Court of Canada--or until it is amended by Parliament. But we have always given it the narrow reading that the Federal Court appears to find acceptable, and we continue to do so.

Defence Revisited

The security screening process at DND is going through a housecleaning again.[4] Responding to some sharp criticisms in our written decisions on complaints and in our Chairman's remarks before the Standing Committee of the House of Commons on Justice and Solicitor General on April 10, 1990, the Department briefed us on a series of reforms. Among them:

- the Director of Security Clearances (DSC) no longer has a vote on Security Clearance Review Board (SCRB), so he is no longer in the difficult position of being both the initial decision-maker and a member of the Board considering that decision;

- subjects will have an opportunity to address any concerns about their loyalty or reliability as it relates to loyalty, in writing to the DSC;

- any matters raised in this way are investigated and included in the files for review by SCRB;

- an individual who complains to us gets a copy of the full security clearance file (vetted, of course, to remove information that might damage national security or, otherwise infringe the *Access to Information Act* or Privacy Act); and

- assisting officers are provided to uniformed personnel who lodge complaints with us.

Further Steps: These are clearly improvements. We have already seen the first assisting officer at one of our hearings. But we urge two further steps on DND--to:

- openly tape all interviews and interrogations in connection with security assessments. The present situation, in which some are taped openly, some taped surreptitiously and some not at all, is not satisfactory; and

- allow personnel, with assisting officers, to make representations directly to SCRB either orally or in writing.

---

[4] While most federal departments and agencies base their decisions to grant or withhold security clearances on investigations and recommendations by CSIS, DND does its own assessments.

With respect to the second recommendation, it is worth recalling that the Federal Court recently found "basic constitutional deficiencies" in the military's procedure for handling appeals against sentences handed down by courts martial because the appellant did not have a right to be heard.[5] Mr. Justice Francis Muldoon commented that:

> Whatever military discipline requires, it is clear that it does not require stripping members of the armed forces of the dignity of making their own submissions personally or by counsel, directly to the officer designated to judge their appeals.[6]

Considering that the denial or downgrading of a security clearance can do as much damage to a career as a criminal conviction, to say nothing of its impact on personal reputations and private lives, it seems to us that Mr. Justice Muldoon's comments could be applied with equal validity--and vigour--to the assessment process.

This is not the first time that DND has attempted to improve its procedures. After being criticized in our 1985-86 Annual Report, DND ordered a review of its security assessment program in 1986. It found, we have been told, that the mandate and objectives of the clearance program were "relevant, appropriate and met the requirements of [the] Government Security Policy". The 1986 review did, however, "note shortcomings in the management of the Program", and DND says it took steps to correct them. Further amendments to the process were made in subsequent years, particularly in 1989.

While our reading of the documentation provided by DND suggests that these steps were directed mainly at tightening up security rather than protecting individual rights, we did find--and acknowledged in our 1986-87 Annual Report--that things seemed to be improving. New complaints involving DND totalled zero in 1986-87. The Department granted clearances in 39 of the 44 cases we asked it in 1986 to reconsider.

Unfortunately, the improvements were short-lived. Since 1986 we have had numerous occasions to criticize the DND clearance process, in our annual reports and in decisions on individual cases. Our concerns have been both with the way DND screened personnel and the way it dealt with complaints placed before us.

Screening Process: We have had cases in which DND was too quick to act on rumour and half truths or was too prone to put the worst possible interpretation on information and events. In one case, for example, a complainant accused of shoplifting protested that it was just a misunderstanding and offered to make good the loss claimed by the store. DND accepted the store detective's interpretation that "he tried to get away with it by making a deal".

In addition, files submitted to SCRB have every appearance of bias. Negative items are flagged for the attention of the Board while important positive items are not. For example, one flagged item was a report that the complainant had declined to take a polygraph ("lie detector") test.

---

5 *John Robert Duncan v. Minister of National Defence et al*., Federal Court of Canada, March 16, 1990.

6 It should be pointed out that this does not invariably require an oral hearing. Indeed, Mr. Justice Muldoon said that in the case before him, it would have been sufficient had the appellant been given the opportunity to make a written submission after reviewing the opposing counsel's arguments.

These tests--which are of doubtful reliability anyway--are supposed to be voluntary. Yet this complainant suffered a disadvantage by using his right to decline.

There was also the problem of the "security consult". A security consult was a note placed on a personnel file indicating that there were security issues to be cleared up before the individual concerned was to be, say, promoted or moved to a sensitive posting. Recognizing that many consults were founded on next to nothing--one that came to our attention in 1989-90 referred to an unsubstantiated scrap of gossip dating back more than 15 years DND stopped putting them on personnel files a few years ago. But those already on the files stayed there. This was manifestly unfair. We were pleased to hear just before this report went to the printer that all previously existing security consults were removed from personnel files by April, 1990.

Sometimes even elementary decency failed. In one 1989-90 case, just before the formal security clearance re-evaluation commenced, the subject was taken to a hotel room under false pretences for a surprise grilling by two men about her sexual orientation and practices. This complainant was given no opportunity to collect her thoughts before the first interrogation, much less to seek legal or other advice. When she asked whether the interrogation was being taped, she was told No. That was a lie. We have heard the exchange with our own ears, on the tape being made at the time.

Although she did not actually undergo a polygraph test, the questions prepared for her examination showed a prurient interest in homosexual practices rather than revealing an honest effort to establish the truth of some of her statements.

Complaints Process: Until very recently, junior military personnel were given no assistance whatsoever when they wished to complain to us. Time after time young privates, unable to afford counsel, were left to face the assembled brass of the military security and legal machinery alone.

As explained earlier in this chapter, we routinely direct our counsel to keep the interests of complainants in mind as much as possible. But there are necessary limits to the help we can offer in this way. The first responsibility of our counsel is to the public interest, not the complainant.

Thus we especially welcome the DND decision to provide assisting officers to junior military personnel. Civilian employees at DND, as at other departments, have unions they can turn to. Uniformed personnel do not. At courts martial, the accused are provided with a military defending officer to help them in their defence.

In 1989-90, DND challenged our jurisdiction in one complex case. The complainant was released from the military because of her admitted homosexuality, which had also cost her her security clearance. DND argued that this took the case out of our jurisdiction since her release was not, as section 42 provides "by reason only" of the denial of a security clearance. The Federal Court[7] ruled that we could proceed, and, despite further jurisdictional arguments at the hearing, we completed the case and provided our recommendations to the Chief of the Defence Staff.

---

[7] *Her Majesty the Queen in Right of Canada as represented by the Minister of National Defence and The Security Intelligence Review Committee*, Federal Court of Canada, March 29, 1990.

Moving to Clean Up: In May, 1990, senior management at DND decided that something had to be done. Along with the assurances to us at a briefing on June 13, 1990, the Department asked Judge René Marin to look at the mandate and procedures of the Special Investigation Unit (SIU), the organization that deals with all DND's security clearances. He was to report by July 27.

The denial of a security clearance can do great harm to the professional and private lives of the men and women of the Canadian Forces. As Canadians, we expect them to give up a great deal in the way of comfort and safety for our security. We believe this entitles them to be treated with scrupulous fairness.

9. Inside SIRC

Earlier chapters have given an account of our operational activities in review and complaints-the work we were created to do. In this chapter we turn to housekeeping--the work that supports our review and complaints roles. It includes informing Parliament and the public and staying in touch with expert opinion. We also report on our budget and on a reorganization of our staff.

Accounting to Parliament

Parliament is, of course, the primary audience for the information we generate for the public record. Our *Annual Report 1988-89* was tabled in the House of Commons by the then Solicitor General on October 13, 1989. As usual, we held a news conference immediately afterwards. Our then chairman also fielded questions on an open line radio program.

The new Chairman, John W.H. Bassett, and a new member, Stewart McInnes, appeared before the Standing Committee of the House of Commons on Justice and Solicitor General on February 15, 1990, to answer questions on their appointments to SIRC in November, 1989. We appeared as a group before the Standing Committee early in the new fiscal year, on April 10, 1990, to answer questions about our 1990-91 estimates.

Our proposals for amendment of the *CSIS Act*, unveiled in September, 1989, generated considerable interest, and we appeared twice before the Special Committee of the House of Commons on the Review of the *CSIS Act* and the *Security Offences Act* (the Thacker Committee)--on November 23, 1989, and again (in camera this time, on the Special Committee's initiative) early in the new fiscal year, on May 8, 1990.

We also helped the Thacker Committee hear first-hand from complainants. To protect the privacy of those who would not wish their identities revealed, even to a Parliamentary committee, we made the initial contact with the complainants and sent them a questionnaire for return directly to the Thacker Committee. More than a dozen complainants responded.

A Second Thought: For the record, we withdrew recommendation 19(b) from our proposal for amendment of the *CSIS Act*. It called for empowering judges to exclude the defendant and defence counsel from court proceedings in extreme circumstances, where national security interests demanded. The present provisions of the *Canada Evidence Act* allowing CSIS to prevent evidence from being introduced at a trial at all have been much criticized, and this was our essay at an alternative.

But, on reflection, we concluded that the cure we proposed was worse than the disease. As our then chairman explained at the November 23, 1989, sitting of the Thacker Committee:

> The very basis of our criminal law is that an accused person is innocent until proven guilty and is entitled to know the government's case against him or her in all of its aspects. National security considerations should not prevail against the rights of an accused person in the context of a criminal trial. If the government's evidence against an accused cannot be disclosed to him or her as part of the criminal trial process, then the government should be prepared to withdraw the prosecution.

Privacy Commissioner: We also wish to record here our regret that our recommendation 18 seems to have given rise to a misunderstanding. This was the recommendation that Parliament consider making it clear beyond all shadow of a doubt that SIRC is entitled to any information under CSIS control, notwithstanding any investigation by the Privacy Commissioner or the Information Commissioner.

The background to this recommendation was a tussle that developed when we wanted to look at some files that were already being looked at by the Privacy Commissioner. Some government authorities took the view that since the Privacy Commissioner was involved we were not entitled to see these files. We resolved that issue and secured the documents. However, we wanted to make sure the same argument did not recur.

We wish to make it clear that our recommendation was not designed to let us second-guess the Privacy Commissioner or the Information Commissioner in the exercise of their separate functions. We do not seek to inspect correspondence between the Service and either Commissioner. Our sole objective is to maintain our right to see any file prepared by CSIS. When Parliament, through the *CSIS Act*, said we were to have access to all information under the Service's control, excepting only cabinet confidences, we think it meant all. If the Service could start withholding files for whatever reason, review would be badly weakened.

Staying in Touch

Believing that we need to stay in touch with expert opinion to do our job well and that we can make a useful contribution by encouraging informed discussion of security intelligence issues, we have a program of small, private seminars and conferences.

In 1989-90, our focus was naturally on the five-year review of the *CSIS Act*. In last year's annual report, we recorded the evening seminar we held in Toronto on June 8, 1989, with a dozen academic and other experts and lawyers, to exchange views about how the *Act* might usefully be amended. Taking advantage of a scheduled meeting in Vancouver, we held a similar session there on September 7, 1989. We are grateful to the West Coast lawyers, scholars and provincial officials who spent an evening with us to discuss issues in the five-year review. They are listed in Appendix C.

We also helped fund the 1989 conference of the Canadian Association for Security and Intelligence Studies, held in Ottawa September 28-30, where the five-year review was again the focus of discussions. We published our own proposals, *Amending the CSIS Act*, on the eve of this conference. Our then chairman addressed a panel dealing with the role of SIRC.

During 1989-90, we made arrangements for a small seminar for June 14, 1990, to explore the effect that changes in Eastern and Central Europe could have on intelligence and security matters in the Western world. We invited senior officials of CSIS and members of the Thacker Committee as well as a number of academic and other experts and lawyers. Papers prepared for

this seminar by Professor Franklin Griffiths of the University of Toronto and Dr. Maurice Tugwell of the Mackenzie Institute for the Study of Terrorism, Revolution and Propaganda are available from our office.

Staying in touch is a two-way street, and members of SIRC share the expertise they have developed. On April 20, 1989, Jean Jacques Blais addressed a conference arranged by the Centre for Constitutional Studies in Edmonton on "Freedom of Expression and Public Administration".

Spending

Our 1989-90 budget is set out in Table 4. At $1,405,000, it represents an increase of only 2.3 per cent from actual spending of $1,373,114 in 1988-89. Our 1990-91 estimates of $1,505,000 represent a further increase of 7 per cent. As explained in Part III of the 1990-91 estimates, half the increase results from an increase in legal fees, instituted by the Department of Justice for all federal agencies. Our need for counsel in the complaints process makes legal fees a major budgetary item for us.

Table 4. SIRC Budget 1989-90

Personnel		$673,000
Salaries and wages	$582,000	
Contributions to employee benefit plans	$91,000	
Goods and services		$723,000
Professional and special services	$566,000	
Other	$157,000	
Total operating expenditures		$1,396,000
Capital expenditures		$9,000
TOTAL		$1,405,000

Source: 1990-91 Estimates, Part III, figure 7

Personnel

A major restructuring of our staff in 1989-90 permitted a 50 per cent increase in the research team with the addition of only one person-year to our overall complement.

We now have six people doing research full time, instead of four. Our former director of research left for a new position and three new research officers were recruited from more than 100 candidates who responded to advertising within the Public Service of Canada and in the academic community through the newsletter of the Canadian Association for Security and Intelligence Studies. We expect to reduce the excessive need which we had been experiencing for overtime work by our researchers.

We have also reorganized the research team, as projected in last year's annual report. Following the lines of the two major operational arms of CSIS, we have separate groups devoted to counter-intelligence and counter-terrorism. These are not, however, their exclusive interests. Other areas are divided between them. For example, the director of the counter-terrorism group is also responsible for CSIS analysis and production and the director of the counter-intelligence group runs our statistical research program.

The abolition of two positions allowed us to increase the research staff this way at the cost of only one new person-year, to 14 from 13. We no longer have an overall research director; coordination between the counter-intelligence and counter-terrorism research groups is provided by the executive director. And now that most officers have desktop computers, there is less need for typing and we were able to eliminate one secretarial position.

Outside the research program, our staff remains as it was last year. It is headed by the executive director who oversees day-to-day operations. We also have a senior complaints officer, an executive assistant who supports both research and complaints functions, an administrative officer who is also registrar of our investigations and coordinates our responsibilities under the *Access to Information Act* and the *Privacy Act*, a records officer, a records clerk and two secretaries. A full staff directory can be found in Appendix D.

APPENDICES

A. Ministerial Directions to CSIS, 1989-90

These are the directions issued to CSIS in 1989-90 by the Solicitor General, under subsection 6(2) of the *CSIS Act*:

1. National Requirements for Security Intelligence

2. Accountability of the Director to the Solicitor General

3. Termination of Foreign Liaison

4. Use of Confidential Human Sources

5. Responsibility for Adverse Recommendations on Security Clearances

6. General Principles and Policies Governing the Conduct of Investigations

7. *Secret*

B. Case Histories

Following are brief outlines of complaints on which SIRC reached decisions in 1989-90.

Security Clearances

Note: Recommendations were not required on all clearance complaints closed in 1989-90. Those resolved before the Committee completed its investigations, withdrawn or beyond SIRC's jurisdiction are not reviewed in this appendix. This includes four complaints against the Department of National Defence.

1. The complainant's Level III clearance was withdrawn because he did not report contacts with officials of a foreign country thought to spy on Canada, contrary to regulations governing his highly-sensitive employment.

The Committee acknowledged that there were grounds for disciplining the complainant for this breach of regulations. But evidence presented by CSIS did not show that the contacts were made for purposes inimical to the security of Canada or that any actual threat to national security resulted.

As there is no reason to doubt the complainant's loyalty to Canada, the Committee recommended that his clearance be restored.

2. The complainant was refused a Level III clearance required for highly-sensitive government employment. After employment was offered, the Service found reason to refuse to recommend security clearance. Major issues raised by the Service cannot be discussed here for security reasons; in very general terms, most boil down to a view that there was a large number of complications in the complainant's life.

The Committee reviewed each of the areas of concern and concluded that all could be met when they were examined in light of the complainant's personal circumstances. The Committee was satisfied that there were valid reasons to believe that the complainant was reliable.

It recommended, therefore, that the clearance be granted.

3. The Canadian Forces were unable to grant the Level II security clearance that the complainant needed to complete specialized training. There was nothing to indicate that he would be a security risk. But it was not possible to meet the requirement of the Government Security Policy that information normally be verified for the previous 10 years or from age 16, whichever is shorter. The complainant was born in another country which cannot be relied on to provide accurate information and he came to Canada less than 10 years ago.

Acknowledging that they slipped up by failing to check the complainant's eligibility for security assessment at the time of enrolment, the Forces offered redress during the Committee's investigation. It proposed to re-enrol the complainant with no loss of seniority and assign him for the time being to duties for which a clearance was not required. He could reapply for Level II clearance in 1992, when the 10-year rule could be met. If clearance was granted then, he would be allowed to transfer back into his former occupation and take the specialized training he sought.

The Committee agreed that the Forces had no choice but to deny this clearance. It recommended that the redress offered by the Forces be implemented.

4. The Canadian Forces cited a number of allegations in support of its decisions to downgrade the complainant's clearance to Level I from Level II and then to withdraw his clearance completely. They centre on the propriety of the complainant's management of his own financial affairs and of his professional conduct before he began full-time employment in the Forces.

The Committee's jurisdiction to hear this case was challenged by the Forces. Under section 42 of the *CSIS Act*, the Committee can investigate when "by reason only of the denial of a security clearance ... a decision is made ... to dismiss ... an individual . . .". The complainant did, in fact, lose his employment, but the Forces said it was not "only" because clearance was denied and, therefore, the Committee had no authority to entertain the complaint. The Committee rejected this objection and proceeded with its investigation.

On the substance, the Committee found fatal flaws in the documentation underlying the decisions to downgrade and withdraw the clearance. For example, "net debt" was confused with "total indebtedness", so the board that made the decisions was not given a correct picture of the complainant's financial situation.

The Committee concluded that the Forces did not have adequate grounds for downgrading or withdrawing the complainant's clearance. It recommended that the original Level II clearance be restored.

Citizenship

5. CSIS held that the complainant had provided information to foreign interests for pay and that the disclosure of some of this information was detrimental to the security of Canada. Paragraph 2(a) of the *CSIS Act* provides that "espionage ... that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage . . ." is a threat to national security.

The complainant acknowledged that he had made contact with foreign interests but said he had done so at the request of his employer and as part of his job.

The Committee concluded that the complainant should not be granted citizenship because CSIS was able to substantiate its allegations against him, providing reasonable grounds to fear that he would engage in activity that threatens national security under paragraph 2(a).

6. CSIS held that the complainant had acted as an agent of a foreign country, interfering in the lives of refugees from that country and of Canadians whose ethnic roots are there. It said that the complainant had used pressure to limit criticism of the régime in that country.

The complainant responded that his activities were carried out openly on behalf of a legal organization, incorporated in Canada, most of whose members are Canadians.

In this context, the Committee's responsibility is to determine whether the complainant's activities constitute a security threat under paragraph 2(b) of the *Act* -- “foreign influencedactivities 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".

The Committee concluded that there were no reasonable grounds to believe that the complainant would engage in activities that constitute a threat to the security of Canada, and it recommended that citizenship be granted.

The Governor in Council has accepted the Committee's recommendation.

7. This case is identical in substance to No. 6, above, and the Committee's recommendation was the same. The Governor in Council has also accepted the Committee's recommendation in this case.

Immigration

8. CSIS held that the complainant had undertaken activities in Canada in support of acts of violence in his country of origin. He headed the Canadian branch of an international association alleged to support politically-motivated violence. Under paragraph 2(c) of the *Act*, threats to the security of Canada include "activities within ... Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political objective within ... a foreign state".

The Committee was satisfied that the Service had a valid case against the complainant, and it recommended that he be deported.

The complainant has challenged the Committee's procedures and its decision before the Federal Court.

Human Rights Complaints

9. In a complaint lodged with the Canadian Human Rights Commission, the complainant alleged that he was denied employment by the Department of National Defence (DND) because of his national or ethnic origin, contrary to the *Canadian Human Rights Act*. As permitted by law, the Commission referred the complaint to SIRC for a determination whether security considerations cited by the Minister of Defence justified the denial of employment.

DND explained that the complainant could not be employed in the position he sought because it was impossible to complete the necessary Level II security assessment. Under the Government Security Policy, information normally has to be verified back 10 years or to age 16, whichever period is shorter. It would have been necessary to obtain information from the complainant's country of birth, but information from this country was not reliable.

However, after the initial human rights complaint was made, DND offered the complainant alternative employment that did not require security clearance.

The complainant did not avail himself of the opportunity to present evidence to the Committee.

The Committee found that DND applied procedures too mechanically in that it did not even consider using its discretion to waive the 10-year rule. DND did not have any evidence that the complainant might be a security risk, and it made no attempt to rind sources of information outside the complainant's country of origin.

The Committee agreed that there was reason to block the human rights investigation on security grounds. But it went on to recommend that security assessment policy be applied in a flexible and humane manner founded on its intent-protection of national interests rather than on its procedures.

10. Except that the country of origin is different and the complainant is a landed immigrant rather than a Canadian citizen, this case is identical in substance with No. 9, above, and so were the Committee's finding and recommendation.

Section 41

Note: In addition to the cases reviewed here, there were 36 complaints under section 41 that were clearly beyond the Committee's jurisdiction or in which preliminary investigation showed that there was an insufficient factual basis to justify any further inquiry by the Committee. The cases described here are those on which investigations were conducted and reports made.

11. Because of security concerns raised by CSIS, the then Minister of Employment and Immigration cancelled the permit on which the complainant was teaching and conducting research in Canada. The effect was to interrupt the complainant's application for landed immigrant status, and he was ordered to leave the country within two weeks.

The Committee upheld the complaint because the Service's letter to the Minister contained a number of material inaccuracies. There were also a number of material omissions. Together with the tone of the letter, they may have prejudiced the outcome of the Minister's exercise of his discretion.

12. The complainant, a research scientist, was the subject of investigation by CSIS both before and after his application for Canadian citizenship. Among other things, the complainant alleges that the security check for his citizenship application was unnecessarily delayed because he refused to act as a CSIS agent.

CSIS showed that a lengthy investigation was required as it sought clarification of a number of matters, including the complainant's admitted conveyance of documents to his country of origin, which is thought to spy on Canada.

The Committee was satisfied that CSIS acted within its legal mandate and that its conduct in this matter was at all times proper and professional. In particular, CSIS could not be faulted for any delay in processing the complainant's application for citizenship.

C. Vancouver Seminar

Taking advantage of a regular meeting in Vancouver, we invited a number of knowledgeable people from British Columbia to join us on September 7, 1989, for a seminar on our proposals for amendment of the *CSIS Act*. Participants are listed here. They gave us the benefit of their insights without fee, and we are grateful to them.

Phillip Bryden
Faculty of Law
University of British Columbia
Vancouver

E. Robert A. Edwards, Q.C.
Assistant Deputy Minister
Ministry of the Attorney General
Victoria

Brenda Gaertner
Barrister and Solicitor
Vancouver

David Gibbons
Barrister and Solicitor
Vancouver

Georges A. Goyer
Barrister and Solicitor
Vancouver

Gordon Hillicker
Barrister and Solicitor
Vancouver

Art Lee
Barrister and Solicitor
Vancouver

Craig Paterson
Barrister and Solicitor
Vancouver

Val Pattee
Assistant Deputy Minister
Police Services
Ministry of the Solicitor General
Victoria

Murray Rankin
Faculty of Law
University of Victoria
Victoria

Mary Saunders
Barrister and Solicitor
Vancouver

Patrick Smith
Chair, Department of
Political Science
Simon Fraser University
Burnaby, B.C.

Don Stewart
President, Omni Canada
Vancouver

James D. Taylor, Q.C.
Office of Crown Counsel
Nanaimo, B.C.

D. SIRC Staff Directory

Following is a directory of the SIRC staff as of August 31, 1990, when this report went to the printers.

Maurice Archdeacon, Executive Director	(613) 990-6839
Danielle Blache, Secretary	990-8442
Maurice M. Klein, Director of Research (Counter-Terrorism)	990-8445
Luc Beaudry, Research Officer	990-8051
Joan Keane, Research Officer	990-8443
John M. Smith, Director of Research (Counter-Intelligence)	991-9111
Michel Paquet, Research Officer	990-9244
Elaine Grant, Research Officer	991-9112
Sylvia Mac Kenzie, Senior Complaints Officer	993-4263
Claire Malone, Executive Assistant	990-6319
Madeleine DeCarufel, Administration Officer & Registrar	990-8052
John Caron, Records Officer	990-6838
Roger MacDow, Records Clerk	998-5258
Diane Roussel, Secretary	990-8441