SECURITY INTELLIGENCE
REVIEW COMMITTEE

Annual Report

1990-1991

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 5 p.m. Ottawa time.

Minister of Supply and Services Canada 1991
Cat. No. JS71-1/1991
ISBN 0-662-59997-7

September 30, 1991

The Honourable Doug Lewis, P.C., M.P.
Solicitor General of Canada
House of Commons
Ottawa, Ontario
KIA OA6

Dear Mr. Lewis:

As required by section 53 of the *Canadian Security Intelligence Service Act*, we hereby transmit to you the Annual Report of the Security Intelligence Review Committee for the fiscal year 1990-91, for submission to Parliament.

Yours sincerely,

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

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

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

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

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

The Security Intelligence Review Committee at a Glance

The Security Intelligence Review Committee (called "SIRC" or "the Committee" in this report) acts as the eyes of the public and Parliament on the Canadian Security Intelligence Service.

The Canadian Security Intelligence Service (CSIS) is a federal government agency created in 1984 by the *Canadian Security Intelligence Service Act*. CSIS investigates terrorists, spies and others whose activities may be a "threat to the security of Canada". CSIS must operate primarily in secret. This makes it difficult for politicians and the Canadian public to ensure that CSIS operations are effective and that at the same time CSIS respects the rights and freedoms of Canadians. To remedy these problems, the same law that created CSIS created SIRC.

The Committee is independent of the Government. The *Canadian Security Intelligence Service Act* provides that its five members be appointed by the Governor in Council after consultation among the leaders of all parties having more than twelve members in the House of Commons. Individuals may be appointed to the Committee only if they are already Privy Councillors or are appointed to the Privy Council for that purpose by the Governor General.

To the extent that national security permits, the Committee reports to Parliament through its annual reports. Annual reports are available to the public. They constitute a "report card" on CSIS operations that would otherwise not be allowed to come under public scrutiny because of national security considerations.

The Committee also has the power to investigate complaints relating to CSIS. First, it can investigate complaints by a person about "any act or thing" done by CSIS. It is not necessary that the person complaining be personally affected by what CSIS did. Second, the Committee can review certain denials of security clearances affecting federal government employees or job applicants or persons who seek to sell goods or services to the federal government under contract. In a related vein, it can also review adverse security findings that would affect a person's right to immigrate to Canada or obtain Canadian citizenship. If the Committee finds a complaint justified, it recommends a remedy.

Glossary

ANC -	Association of New Canadians
ARAACP -	Airport Restricted Area Access Clearance Program
CAUT -	Canadian Association of University Teachers
CI -	Counter-Intelligence
COCOM -	Co-ordinating Committee for Multilateral Export Controls
CRNC -	Criminal Records Name Check
CSE -	Communications Security Establishment
CSIS -	Canadian Security Intelligence Service
CT -	Counter-Terrorism
DIRECTOR -	the Director of the Canadian Security Intelligence Service
DND -	Department of National Defence
FBI -	Federal Bureau of Investigation
GSP -	Government Security Policy
IO -	Intelligence Officer
IPC -	Intelligence Production Committee
MINISTER -	the Solicitor General of Canada, unless otherwise stated
NSID -	National Security Investigations Directorate
RAP -	Analysis and Production Branch
SERVICE -	Canadian Security Intelligence Service (CSIS)
SIRC -	Security Intelligence Review Committee
SIU -	Special Investigation Unit
TAPP -	Technical Aids Policies and Procedures
TARC -	Targeting Approval and Review Committee

Contents

1. Introduction

The Five Year Review Brings Little Change

The 1990-91 fiscal year represented a watershed for the *CSIS Act;* it received its five year "report card". The drafters of the Act had inserted a requirement that its provisions and operation be comprehensively reviewed five years after the Act came into force. In September, 1990, a special parliamentary committee chaired by Blaine Thacker, M.P. completed this review.

We (the Security Intelligence Review Committee, or "SIRC") had submitted 31 recommendations to the Thacker Committee. We then published a report, *Amending the CSIS Act,* containing these recommendations and the reasoning behind them. The Thacker report, *In Flux But Not in Crisis,* adopted about two thirds of our recommendations. In total, Thacker made 117 recommendations aimed at improving the *CSIS Act,* its implementation and the Canadian "security and intelligence system" as a whole.

In February, 1991, the Government responded to the Thacker report with its own report, *On Course*. The Government accepted Thacker's recommendation that SIRC continue to carry out the role specified for it in the *CSIS Act.* The Government's main response to the other recommendations of the Thacker report, however, was that there would be no change in the Act and only modest changes in the functioning of Canada's security intelligence system.

Significantly, however, the Standing Committee on Justice and the Solicitor General has created a Sub-committee on National Security, as the Thacker report recommended. Mr. Thacker will chair the Sub-committee. It will begin work on September 18, 1991, and will have two functions:

> to undertake a review and consider the budgets and functions of CSIS, the RCMP's National Security Investigations Directorate (NSID) and their relationships with all agencies with which they have a Memorandum of Understanding or other working arrangements; and
>
> to consider SIRC's annual report, all SIRC reports made under section 54 of the *CSIS Act*, the annual statement by the Solicitor General about national security and the public annual report from the Director of CSIS.

The Future

How will this conclusion to the five year review of the *CSIS Act* affect us? Our major role is to review all CSIS activities. We seek to ensure an appropriate balance between an effective Service and a responsible Service. By *effective,* we mean that the Service should give timely warning of

threats to our national security. By *responsible*, we mean that the Service must go to great lengths, not only to stay within the law, but also to use its powers with restraint and with a proper sensitivity to the rights of individuals.

Our job is to determine in each case we examine whether CSIS is acting wholly within the law or going beyond it. Our decisions depend to some extent on the clarity of the law governing CSIS. The *CSIS Act* was the product of much time and hard work. We do not underestimate the difficulty its designers and drafters faced. However, with the benefit of five years of experience, it is clear to us, as it was to the Thacker Committee, that the Act is deficient in some respects. We made representations to Thacker about these deficiencies. We hold to those representations.

The Structure of this Report

Chapter 2 of this report reviews what we consider "general matters" relating to protecting Canada against threats to its security. Chapter 3 examines specific CSIS operations. In addition, we have singled out several topics for a more thorough reporting: CSIS activities regarding native Canadians (Chapter 4), security screening (Chapter 5) and domestic terrorism (Chapter 6). Chapter 7 presents three case studies of CSIS operations. Chapter 8 examines the complaints process -- how persons complain about the activities of CSIS or about being denied a security clearance. Chapters 9 and 10 report on certain internal workings of CSIS and this Committee respectively,

In this report we do not go into great detail about the precise steps we take in reviewing CSIS activities, This does not mean that our reviews are not thorough. In general, our review activities may include the following: interviews with complainants, CSIS employees at Headquarters and in regional offices, examination of files, court testimony and decisions, surveys and in-depth research. Our goal in each case is to ensure that our investigations are sufficiently detailed to warrant the trust placed in the Committee.

Impact of the Gulf War on this Report

The fear of increased terrorism flowing from the Gulf War led CSIS to move many intelligence officers temporarily from their normal work to counter-terrorism desks. This meant that the Committee had to accept a somewhat slower response to our questions to CSIS. We also had to accept much longer than normal delays before being able to interview CSIS experts about the areas of review we had planned for this year. We have since regained most of this lost ground.

2. Review of General Matters

One of our major functions is to review CSIS activities. The results of this year's review are reported in subsequent chapters. In this chapter, we review several topics that are not strictly subsumed under the rubric "CSIS activities", but that have an important impact on how CSIS performs its duties.

Ministerial Direction

Under subparagraph 38(a)(ii) of the *CSIS Act*, SIRC is required to examine the Minister's written directions to the Service. In fiscal year 1990-91, the Minister gave CSIS only one direction. We welcomed this direction because the Act's core, section 2 -- the definition of "threats to the security of Canada" -- lacks sufficient precision, and the Government response to Thacker made it clear that the definition would not be amended. The direction makes up for this deficiency by offering CSIS a detailed interpretation of sections 2 and 12. It defines several crucial terms such as "espionage and sabotage" and "foreign influenced activities" more precisely than does section 2. The Solicitor General informed the Chairman that he intends to make the direction public in his statement to the House of Commons later this year.

Ministerial directions typically cover the most sensitive types of investigations, such as campus investigations or joint operations with allies in Canada. A number of the directions require the Service to seek the specific authority of the Solicitor General to undertake certain types of operations.

Part of the Committee's mandate is to collect statistics on CSIS operations. One statistic we collect is a count of all authorizations given by the Minister under the terms of Ministerial directions, by type and date. The Committee is then able to address any significant trends in sensitive operations.

We also review CSIS decisions made pursuant to Ministerial directions. Sometimes we do this through special studies. Thus, for example, we have audited decisions made under the Ministerial direction on security investigations on university campuses. We also do this as part of a periodic review process. In our regional audits, we review all authorizations for investigations in that region.

One direction, made public by the Minister, requires his personal approval of any intrusive investigations under paragraph 2(d) of the *CSIS Act*. Paragraph 2(d) has been termed the "subversion" aspect of the definition of "threats to the security of Canada". Our research showed that there were no investigations during the 1990-91 fiscal year under paragraph 2(d). We are further informed by the Service that the Minister authorized no such investigations in the 1990-91 fiscal year.

Operational Manual

This year, CSIS made four minor changes and one major change to its Operational Manual. The minor changes related to the following topics:

- help given to Employment and Immigration Canada "in support of the detention of a person on security grounds in order to contain a potential threat";

- procedures for the Service to provide reports supporting subsection 40.1(1) certificates under the *Immigration Act.* With such a certificate, the Government can halt all immigration inquiry actions and subject a person to immediate deportation. An example of the application of this procedure is provided in our report on the two Iraqi nationals detained during the Gulf War (see Chapter 3);

- caveats to be placed on documents conveying information to domestic and foreign agencies. These caveats prevent further dissemination without obtaining the approval of CSIS; and

- the mandate and structure of the Operations and Analysis Policy Committee. This committee guides the development of Service policy.

The one major change to the Manual has been the revision by the Service of the human sources section. The revision puts into operation a 1989-90 Ministerial direction. We have examined these minor and major changes closely, and commend the Service for its efforts. In the human sources section, however, we found one variance between the direction and the Manual.

Each year we ask the Service to detail its progress in updating those instructions in the Operational Manual which were written before the *CSIS Act* came into force. We can report that most sections of the Manual have now been updated. Several sections (for example, targeting policy) have been revised more than once.

We cannot say the same for the Technical Aids Policies and Procedures (TAPP) Manual. This manual governed the use of warrant powers. It consisted almost completely of instructions pre-dating the *CSIS Act.* The manual as such no longer exists. Most of its chapters have been replaced by other policy instruments. At present, officers follow a patchwork of instructions, some in the form of "Bulletins" found in the CSIS Operational Manual. We think the Service needs comprehensive guidelines on the use of its most intrusive powers.

Disclosures in the Public Interest

There were no public interest disclosures under section 19 of the *CSIS Act.*

Report of the Director and Certificate of the Inspector General

Under subparagraph 38(a)(i) of the *CSIS Act,* the Committee is to review the report of the CSIS Director and the Certificate of the Inspector General. This constitutes part of the Committee's general review of the performance of CSIS.

As we went to press, we received a copy of the CSIS annual report for the fiscal year 1990-91. The Director sends this report to the Solicitor General, as subsection 33(l) of the *CSIS Act* requires. The 1990-91 report gives a useful overview of the national and international environment in which CSIS works. The report contains more detailed information than before on recent developments in counter terrorism.

In his 1989-90 certificate, the Inspector General indicated that he was generally satisfied with the CSIS annual report. He particularly commended the CSIS summaries and analysis of international events.

Nonetheless, he was disappointed that the Director had chosen not to comment on several issues, such as the public and media perception of CSIS, the relationship between the Service and its client departments and agencies, and the work of the Thacker Committee. We concur with the Inspector General's comments.

The certificate identified three areas of non-compliance with the *CSIS Act or* Ministerial direction. These involved warrant conditions, the collection and retention of information, and the Ministerial direction on campus operations. The Inspector General also noted that, since his last certificate, in November, 1989, the Director had submitted two reports to the Minister about possible unlawful activities by CSIS employees in performing their duties and functions. The Inspector General expressed concern about Service delays in submitting such reports to the Minister. We concur with these concerns.

Inspector General's Reports and Studies

The Inspector General conducts reviews of CSIS activities at the Committee's request pursuant to paragraph 40(a) of the *CSIS Act.* The Inspector General also consults with us at the beginning of each year to ensure that there is no duplication in our respective review programs.

(i) Warrants and File Destruction

In 1990-91, the Committee received one study by the Inspector General on warrants and one on file destruction.

The warrant study examined the processing of intelligence collected under warrants for the interception of oral communications and telecommunications. The Inspector General noted that CSIS is now paying well-deserved attention to this area. He reported a generally high quality of processing

and reporting, and found no serious compliance problems.

We report on the Inspector General's study on file review and destruction activities in Chapter 3.

(ii) CSIS and the Communications Security Establishment (CSE)

CSIS exchanges information with many foreign and domestic agencies. One of the domestic agencies that we knew least about was the Communications Security Establishment (CSE). CSE, Canada's signals intelligence agency, is shrouded in secrecy due to the nature of its work.[1] Although our mandate does not extend to CSE, the involvement of CSIS in information exchanges with CSE makes the relationship between the two bodies relevant to us. We wanted to learn more about the relationship to ensure that information exchanges did not compromise individual rights.

During a review last year, we took a preliminary look at one aspect (which we cannot disclose for security reasons) of the relationship between CSIS and CSE. During fiscal year 1990-91, we used our authority under section 40 of the *CSIS Act* to ask the Inspector General to review information exchanges between CSIS and CSE and the policy framework in which they occur. We asked that he pay particular attention to a series of issues. These included the nature of the cooperation and the arrangements in place between the two agencies, the impact on CSIS operations, and whether the procedures involved any unreasonable or unnecessary exercise of powers by CSIS.

We have not yet received the final report, but the Inspector General was able to answer all our questions in a preliminary briefing. The Inspector General considered whether the information and intelligence exchanges complied with the *CSIS Act* (sections 12, 17 and 19 in particular) and Service policies and procedures. He found that those technical and operational exchanges between the agencies that he reviewed complied with the *CSIS Act* and with existing cooperation agreements. The cooperation agreements provide, among other matters, for the protection of information about Canadians.

Our key questions pertained to the role of CSIS in collecting information about Canadians. We wanted to know what was collected, by whom, and how it was used. The Inspector General's conclusions indicate that current CSIS policies and procedures safeguard the interests of Canadians

---

[1] This Committee and the Thacker Committee had both expressed concern about the absence of external review mechanisms covering most of the Canadian intelligence community, including CSE.

by limiting the information obtained from CSE to that which CSIS has the mandate and authority to collect.

More generally, the Inspector General found no evidence of any unreasonable or unnecessary use of powers by CSIS in exchanging information and intelligence with CSE. The review indicated that CSIS clearly recognizes the sensitivity of the relationship with CSE.

The Inspector General did identify a need for CSIS to develop and document operational policy about its relations and exchanges with CSE. Cooperation agreements recently concluded between the agencies now permit CSIS to accomplish this. We will monitor CSIS exchanges in this area.

The newly-implemented tracking procedures for domestic and foreign information exchanges, described in Chapter 3, will allow us to sample CSIS/CSE exchanges appropriately in the future. We will begin regular reviews and report our findings in our next annual report.

We caution that the review carried out by the Inspector General at our request assessed the propriety of the actions of CSIS, not those of CSE. It should not therefore be mistaken for an external review of CSE operations.

(iii) The CSIS Threat Assessment Program

In our 1987-88 Annual Report,[2] we reviewed the operations of the Counter-Terrorism (CT) Branch. We concluded that the principal consumers of CT intelligence were generally satisfied with the quality of intelligence they received about terrorist threats. They were satisfied with their access to CT personnel to discuss issues and problems. The analyses describing the level of danger to particular interests from terrorist groups were also well-received. This latter function -- analysis of dangers from terrorist groups -- forms the core of the CSIS Threat Assessment Program.

The Threat Assessment Program in the Service relies largely on the Counter-Terrorism Branch for its information. The program functions as an early warning system to the federal government about imminent threats to Canadians and other groups here and abroad. As such, it serves as a crucial front line defence against terrorism. We wanted to update our knowledge about how this important system was working. In short, we wanted to know how well it contributed to protecting Canadians.

During the 1990-91 fiscal year, we again used our authority under section 40 of the *CSIS Act* to ask the Inspector General to conduct a review. The study revealed a well-coordinated and effectively

---

[2] At pp. 27-33.

operating program. It successfully adapted to different situations, whether the visit of a head of state, the Economic Summit or the Gulf War. The study concluded that the program provided useful intelligence to the Government in all these situations.

As we had found in 1987-88, CSIS staff working on threat assessment issues were accessible to client departments and agencies. The departments and agencies consulted frequently with CSIS staff to ensure the quality of the intelligence product. The program was also linked to the various interdepartmental committees and international bodies concerned with terrorism, threat assessment, and security and intelligence matters.

The Inspector General surveyed the usefulness of the assessments to the major clients. The result was a unanimously favourable response. Assessments were considered timely and comprehensive. The Inspector General found no evidence that CSIS was involved in any unreasonable or unnecessary exercise of its powers. In short, Canadians appear to be well-served by the Threat Assessment Program.

Special Reports

Under section 54 of the *CSIS Act*, we can make special reports to the Solicitor General on any matter relating to the performance and functions of the Service. In 1990-91, we submitted four studies to the Minister under section 54:[3]

(a) Release of Information to Foreign Agencies;
(b) Domestic Exchanges of Information;
(c) Security Investigations on University Campuses; and
(d) CSIS Activities Regarding Native Canadians.

We also advised the Minister that eight other SIRC studies were available to him on request. A list of SIRC studies is attached as Appendix A to this report.

SIRC Consultations and Inquiries

Formal Inquiries: In our review function, not counting inquiries arising out of complaints, we directed 122 formal inquiries to the Service in the 1990-91 fiscal year. Although it is difficult to be precise, the average time CSIS took to answer a formal inquiry was about two months.

Briefings: We met twice with the Director during the fiscal year -- April 8 and November 14, 1990. We visited regional offices of the Service when our regular meetings took us out of Ottawa. We were briefed on regional operations in Halifax on July 18, 1990, in Montreal on January 9, 1991, in

---

[3] In addition, early in the 1991-92 fiscal year, we sent to the Solicitor General a review of the entry into Canada of Mohammed Al Mashat, the former Iraqi ambassador to the United States.

Vancouver on February 13, 1991, and in Toronto on June 12, 1991.

Beyond CSIS: We met with officials from the Department of National Defence on June 13, 1990, and were briefed about the changes that occurred as a consequence of the Marin Report, *External Review of the Canadian Forces Special Investigation Unit.* On November 14, 1990, we met with a delegation from the Canadian Association of University Teachers (CAUT). The Chairman and Executive Director travelled to Washington in March, 1991 to meet the Director of the FBI and other officials. In April, 1991 the Committee (except Paule Gauthier) travelled to London, Bonn and Brussels to meet with ministers, parliamentarians and government officials.

Unlawful Acts by CSIS Employees

During 1990-91, the Minister informed us of two instances where he had notified the Attorney General of alleged unlawful acts committed by CSIS employees in the performance of their duties and functions. Subsection 20(4) of the *CSIS Act* requires the Minister to notify the Committee when reporting unlawful conduct to the Attorney General.

In one case, a CSIS employee allegedly disclosed the identity of a confidential source. By so doing, the employee may have violated subsection 19(2) and, possibly, paragraph 18(l)(a) of the *CSIS Act.* The disclosure was to the RCMP and does not appear to have had serious consequences.

In the second case, an employee allegedly provided biographical information about an individual to a private investigator working for a provincial government agency. The information was obtained from the CSIS computer system. The Service was able to locate and expunge all the information obtained by the private investigator. Providing such information could contravene subsection 19(l) of the *CSIS Act* and also violate other federal laws. The disclosure was allegedly made without obtaining proper authorization from CSIS.

3. CSIS Operations

The *CSIS Act* gives us a broad mandate to review generally the performance by the Service of its "duties and functions". The present chapter covers a broad range of CSIS programs and activities. Detailed studies of specific aspects of CSIS operations are contained in Chapters 4 to 7.

Arrangements with Other Governments

Subsection 17(l) of the *CSIS Act* allows the Service, with ministerial approval, to enter into arrangements with provincial governments, provincial and local police forces, foreign governments, their agencies and international bodies.

(i) Foreign Arrangements

In 1990-91, the Service concluded limited arrangements with three foreign governments. The Committee, the Service and the Government are aware of human rights violations in all three countries. When the agreements were approved, the security agencies of these countries were apparently not involved in major human rights violations. The record of some agencies may have changed recently. Few information exchanges have taken place since late last year.

We continue to be concerned about relations with states having an undesirable human rights record. Still, we recognize the desirability of maintaining limited agreements to ensure that CSIS receives information about emerging threats to Canada's security.

(ii) Domestic Arrangements

This fiscal year, CSIS concluded four domestic arrangements. One was signed with the Secretary of State. Two agreements were signed with the Communications Security Establishment and one was signed with a provincial government.

Exchanges of Information with Foreign and Domestic Agencies

In previous annual reports, we observed that the computerized management information system in CSIS did not permit us to learn how much information and intelligence CSIS exchanges with domestic and foreign agencies. More important, we were sometimes unable to identify or trace to other agencies or government departments the information which CSIS released. CSIS Headquarters and the regions used different logging methods, as did the Counter-Intelligence and Counter-Terrorism Branches. This gave us many difficulties in trying to monitor the exchanges.

Late in 1990, the CSIS Director informed the Chairman that the Service would implement new procedures to apply to the computerized management information system. By April, 1991, CSIS had implemented the procedures for all exchanges of information between CSIS and domestic or foreign agencies. The system seeks to simplify and standardize the coding of information exchanges

throughout CSIS.

CSIS personnel are still learning how to use the system. We therefore cannot evaluate to what extent it will help us monitor exchanges. The procedures have the potential to enhance the SIRC review function by permitting information exchanges to be traced. Our next annual report will describe our first reviews of the new system.

Warrant Statistics

Under section 21 of the *CSIS Act*, the Service requires warrants from the Federal Court of Canada for most of its intrusive activities. Each year we publish statistics provided by CSIS on warrant use.

This year, as usual, CSIS gave us access to all warrant files. Table 1 gives figures for the last three years. As we explain below, however, these statistics really say little. Our staff will be establishing a statistical collection system that better meets Committee needs.

Table 1. New and Renewed Warrants, 1988-89 to 1990-91

	1988-89	1989-90	1990-91
New warrants granted	55	34	27
Warrants renewed	35	50	51
Total	90	84	78

For the last two years, Committee members have argued that warrant statistics currently provided to the public are inadequate. A single warrant can involve one or many powers, and from one to any number of individuals. Thus, the number of warrants is a poor indicator of the number of individuals subject to investigation and the extent to which intrusive devices are being used.

This year we have decided to give an indication of the scale of the intrusion into the privacy of Canadians[1] directly attributable to the use by CSIS of warrants authorized by the Federal Court. We believe that many Canadians have a highly exaggerated view of the extent of the intrusive activities of CSIS using Federal Court warrants.

[1] Meaning Canadian citizens and landed immigrants.

We have thoroughly analyzed warrant affidavits and warrants approved by the Federal Court. We have decided to make public the fact that Canadians who may be directly affected by intrusive activity by CSIS under Federal Court warrants number in the hundreds, not in the thousands.

Multiple Target Authorizations not Directly Authorized by the Targeting Approval and Review Committee (TARC)

Last year, we expressed concern about the use by CSIS of authorizations covering groups of unnamed persons. These authorizations were for lower level investigations, and had been approved by operational Directors General only, not directly by the Targeting Approval and Review Committee chaired by the Director. We undertook to examine other such "multiple target" authorizations -- authorizations covering more than one person.

This year, we assessed all multiple target authorizations that had been authorized other than by TARC and that remained in force in September, 1990. There were six non-TARC authorizations in all. Five involved potentially serious violence, and one involved foreign influence. We found in all cases that the authorizations did not involve an excessive or unnecessary use of powers. Even so, we recommended that the Service "tighten the screws" in defining who would be subject to investigation. To this end, we proposed that targeting documents list specific individuals where possible, or use narrower definitions of the activities that could be investigated.

Counter-Terrorism (CT) Program

(a) Counter-Terrorism Branch Activities in General

Program Changes: We sought to learn how the Counter-Terrorism (CT) Branch had changed since our last annual report. CSIS replied that due to the Gulf War and developments on the domestic scene, CT Branch has been given an increase in resources.

Direction from the Solicitor General provides a basis for the Branch to plan its operations. To comply with the direction, the CT Branch undertook several initiatives in the 1990-91 fiscal year. These included strategic intelligence assessments relating to foreign influence and other issues.

Threat Assessments: The Branch produces assessments advising the Government of threats to national security. During fiscal year 1990-91, the Branch produced more than 1,100 threat assessments. This was higher than last year's total largely because of the Gulf War.

Post-Mortem: We noted in our last review of the CT Program that 1988 was an unusual year because of major international events being held in Canada -- the Toronto Economic Summit, for example. During the 1990-91 fiscal year we received the CSIS "postmortem" report on CSIS activities during the Economic Summit. While we were generally satisfied with the document, we were concerned about how long the Service took to prepare it.

In addition, one important aspect of CSIS operations -- liaison with foreign agencies -- was not discussed in the post-mortem. At an international event such as an Economic Summit, the host country is responsible for security. Cooperation and coordination with foreign security agencies are essential to avoid incidents. However, when we asked the Service for details about foreign liaison for the Economic Summit, the questions were answered to our satisfaction.

Just as we went to press, we received information about a post-mortem on the Open Skies Conference that was held in Ottawa from February 12 to 28, 1990. We have begun our analysis and we will report on this post-mortem in our next annual report.

Latin American Group: In our 1987-88 Annual Report, we discussed the investigations carried out by the CT Branch. We were troubled by one case, an investigation of a Latin American group.

CSIS collects information to detect emerging threats to Canada. The Service may collect information on persons in Canada when certain conditions are met. The Service is interested in groups in Canada that are affiliated with and endorse the purposes and the violent methods of overseas organizations. In particular, the Service has a mandate to investigate groups in Canada that give concrete support to perpetrators of violence at home or abroad.

We noted in our 1987-88 Annual Report that the Service must ensure it does not investigate "lawful advocacy, protest or dissent" except where it relates to terrorist threats. Furthermore, the Service must be able to recognize when threats diminish, to avoid unduly prolonging investigations of groups in Canada.

We believed that the CSIS investigation of the Latin American group, while legal, was slow to recognize that the group's contribution to the conflict abroad was dwindling. After our review, the Service narrowed the scope of its targeting. During the 1990-91 fiscal year, we learned that the CSIS investigation was reduced further and is now limited to the least intrusive investigative procedures.

(b) CSIS Activities During the Gulf War

Much of the world expected terrorist attacks following threats made by Saddam Hussein before and during the Gulf War. This caused a large increase in the counter-terrorism workload of CSIS. In turn, the President of the Canadian Arab Federation alleged harassment of Arab-Canadians by CSIS.

We are now conducting a final review of CSIS activities immediately before and during the Gulf War. In early January, 1991, we began a preliminary review. We sought information on the number of targets and the levels of investigation under which the targeting took place.

To place CSIS activities in context, we are reviewing directives that the Service issued in relation to the Gulf crisis. We are assessing in detail whether the Service took unnecessary or inappropriate actions.

(i) Allegations of CSIS Harassment of Arab-Canadians

During the Gulf War, the Canadian Arab Federation complained in the media about CSIS activities directed towards Arab-Canadians. We responded quickly to these allegations. The Chairman received a personal briefing from the Director of CSIS. At the same time, the Committee forwarded a detailed questionnaire to CSIS and asked for access to all relevant files. A short time later the Chairman offered to appear on an open-line radio program with the President of the Canadian Arab Federation. The President did not appear.

Late in March, 1991, our Executive Director and Director of Research (Counter-Terrorism) met with the President of the Canadian Arab Federation, his legal adviser and the Federation Executive Director. We initiated the meeting to give the Federation a chance to express its concerns to us. We had not at -that time received any complaints about CSIS community interviews.

The President told us of his concern about CSIS techniques used to monitor Arab Canadians and their impact on the Arab community in Canada. The Federation estimated that CSIS had interviewed between 200 and 500 Arab-Canadians. The President noted the "intimidating" effect of the interviews, especially if conducted without advance notice. We were told that this was especially disconcerting to those Arab-Canadians who could not distinguish between the mandate and tactics of CSIS and the operations of security intelligence agencies in Arab states. We were also told of the distrust among many Arab-Canadians of government agencies, including SIRC. Their perception was that this attitude also arose in part from their experiences in other countries; governments in Canada, they assumed, would be no different. Federation representatives explained that some members agreed to interviews with CSIS largely out of fear.

Federation representatives also criticized the Director's statement to the Standing Committee that CSIS is entitled to be present when approved targets participate in demonstrations. The Federation explained this criticism by saying that the community believed that the presence of CSIS at demonstrations constituted surveillance of Arab-Canadians exercising their democratic rights. The Federation's legal adviser said that this had a chilling effect on the Arab-Canadian community.

The Federation President did not know whether formal complaints about alleged CSIS activities would be submitted to the Committee. To the first week of July, 1991, we have received no formal complaints by members of the Arab community in Canada about CSIS activities before, during or after the Gulf War.

We hope that our meeting with the Federation allayed many of its concerns. The Federation representatives explained that the chief fear of the community was that a complaint to this Committee was in effect a complaint to the Government and might have serious consequences for the complainants. Members of our staff were told, for example, that many Canadians of Arab descent questioned the effectiveness of the Committee, and feared that a complaint to SIRC would result in artificial delays in immigration procedures for their relatives.

The Committee now better understands the fears of Arab-Canadians. We would wish to reassure all Canadians that our investigations are conducted in strictest confidence and that we operate at arm's length from Government, protected by statute. We hope that we were able to persuade the Federation that security intelligence operations in Canada receive extraordinarily close external scrutiny. We certainly made it clear that complaints to SIRC will not result in vengeful actions by immigration or other Government officials.

(ii) Allegations about the University of Calgary

During the meeting with the Canadian Arab Federation, its President also complained about alleged CSIS activities in relation to the University of Calgary. He said that CSIS had interviewed a University of Calgary student during the Gulf crisis and asked him for a list of Arab student activists on campus. The President said that he would seek the student's permission to release his name. To date, we have not received that information.

The Committee reviewed this allegation in detail. In our investigation in Alberta, we reviewed all relevant documents and interviewed CSIS employees. We found that CSIS community interviews with members of the Arab community did take place in Calgary and elsewhere in Alberta, as they did in the rest of the country. But CSIS did not conduct any interviews or investigations concerning the University of Calgary. We found no evidence that CSIS officials knowingly interviewed Arab students from the university during the period in question. CSIS made no presentations to student groups or to clubs at the university. We also found no evidence that the Service photographed demonstrations in Calgary related to the Gulf crisis. No photographs of any kind, including those of demonstrations or vigils, were shown to persons who were

interviewed. We similarly found no evidence that CSIS interviewers asked about campus activists or requested student lists.

Our findings relate solely to CSIS activities in Calgary. We do not yet know if they apply to other universities in Canada.

(iii) Detained Iraqis

On January 9, 1991, two Iraqi nationals, identified publicly only as Joseph and Sarah Smith, landed at Pearson International Airport, carrying counterfeit Saudi passports. They applied for refugee status. The husband carried a notebook with a list of military weapons. He was an Iraqi national and had fought on Iran's side during the Iran-Iraq war. He was also a member of the Al Dawa party, a group suspected of terrorist acts. Both persons were detained.

Because CSIS was a key player in the case, we reviewed its role. We concluded that the CSIS investigation and the information collected fell within its mandate. We noted too that the Service did not make excessive or unnecessary use of its powers.

We believe that CSIS investigators seriously considered the explanations of the couple and made reasonable efforts to verify their statements. Although the Federal Court did not agree to continue the detention, we concluded that CSIS had acted in a fair and even-handed manner. The Iraqi nationals remain in Canada.

(c) Air India

Several developments have taken place during the past year in relation to the Air India and Narita Airport incidents. Six years ago, on June 23, 1985, a bomb exploded at Tokyo's Narita Airport, killing two baggage handlers. The Air India tragedy took place the same day. The flight containing the Narita bomb and the Air India flight both originated in Canada.

In December, 1988, we decided to undertake an inquiry into CSIS actions or lack of action before and after the Air India and Narita incidents. We made our decision in response to questions about whether CSIS could have done more to prevent these disasters and whether it helped the subsequent police investigation sufficiently. We established terms of reference for a limited but thorough inquiry.[2]

---

[2] See the 1988-89 Annual Report at pp. 19-20.

The inquiry did not proceed because the RCMP, the Deputy Solicitor General and the Deputy Attorney General said a SIRC inquiry could hinder the police investigation and the course of justice. The Deputy Attorney General asked us not to proceed at that time. After considerable deliberation, we placed the inquiry on hold.

Inderjit Singh Reyat was tried for the Narita bombing. On May 10, 1991, he was convicted of manslaughter for making the bomb or helping others to make it. Reyat has appealed his conviction.

In the wake of the Reyat conviction, we once again considered the possibility of convening an inquiry. We are discussing all aspects of this matter with the Solicitor General and the Minister of Justice. We would like their cooperation to conduct a thorough and rigorous investigation. These discussions are still under way. We expect to be in a position to make a final decision shortly after the tabling of this annual report in early October.

Counter-Intelligence Program

This year, we conducted a study of CSIS investigative activities involving East Bloc[3] targets. We also examined the adequacy of Service activities in one case about alleged transfers of military technology.

(a) East Bloc Investigations

In 1989, the East Bloc was beset with political changes, and a number of governments fell. The Committee followed the CSIS analysis of these changes. In particular, we were very interested in how these changes affected security threats against Canada.

In late 1990, the Committee decided to examine the CSIS response to the political changes in the East Bloc. We did so because we perceived a discrepancy between what the Service was saying to Government and the public about the ongoing intelligence activities of East Bloc nations and what these nations were in fact doing. We found that, whatever CSIS had said on the subject, it had made appropriate adjustments. We found no case where political changes had resulted in a CSIS investigation becoming unjustifiable, although we differed with CSIS about various aspects of some investigations -- for example, their duration.

The Service believes that the threat of theft of scientific and technological assets continues to be significant. Its concern with the former East Bloc now extends beyond protecting Canadian and allied military technology through COCOM[4]. Increasingly, the Service seeks to protect the

---

[3] Former Eastern European Soviet satellite states.

[4] Co-ordinating Committee for Multilateral Export Controls. This international body limits the flow of military and "dual use" technology to Soviet Bloc and other

Canadian economy and commercial assets. East Bloc nations, however, do not pose a significant economic challenge to Canada. Their trade with Canada is very limited, and their weakened economies have limited capacities to integrate modern technologies. The trading strength of many other countries poses a far greater risk to the Canadian economy.

We cannot say that all former East Bloc nations no longer represent a threat. Indeed, there seems to be some evidence of limited ongoing intelligence activity. The need for the East Bloc to engage in intelligence activity in Canada, however, is decreasing. With the easing of COCOM restrictions, East Bloc countries have less need to steal technology. The demise of hard-line communist regimes has meant that East Bloc countries have less and less reason to covertly manipulate ethnic communities or émigrés in Canada.

(b) Michel Bull, Space Research Corporation and Iraq

In November, 1990, a Canadian journalist,[5] citing a letter from External Affairs to CSIS, alleged that CSIS had been "tipped off" about possible activities linking Michel Bull and Space Research Corporation to military technology transfers to Iraq. The late Gerald Bull, his father, was involved in developing the Iraqi supergun and Iraqi long range artillery. The journalist also claimed that the case "raised doubts" about the capacity of CSIS to detect and investigate transfers of military technology.

Several agencies in Canada are involved in preventing illicit transfers of technology. By illicit transfers we mean transfers of restricted technology. Technology transfers are controlled in Canada by the *Export and Import Permits Act* and internationally by COCOM. Much of this restricted technology has military applications. Some involves state-of-the-art developments, such as missile guidance systems. Some is linked to conventional weapons -- guns, explosives and chemical and biological agents. The agencies involved include External Affairs, the RCMP, Revenue Canada, the Department of National Defence and CSIS. CSIS provides intelligence on illicit transfers as part of its duties under sections 2 and 12 of the *CSIS Act.*

We found no evidence that CSIS was negligent in its investigations. Nor did we find any indication that CSIS was unable to carry out its intelligence function with respect to technology transfers.

---

states.

[5] Dave Todd, *The Ottawa Citizen,* November 21, 1990, p. A1.

Analysis and Production Branch (RAP)

In our previous annual reports, we noted that the Analysis and Production Branch (RAP) had not yet received a full complement of staff. In 1990-91, all positions were filled and overall intelligence production increased by approximately 30 per cent.

(a) Strategic Analysis

In previous years we criticized CSIS for not putting enough emphasis on strategic analysis. In fiscal year 1990-91, the Service introduced a new format of reporting intelligence: *CSIS Studies. CSIS Studies* are longer, more in-depth and longer term analyses than the *CSIS Reports. CSIS Reports* are the primary means of disseminating advice to Government from the Analysis and Production Branch (RAP). In general, *CSIS Studies* represent the work of senior strategic specialists in RAP who, during their research, have amassed considerable knowledge about the Middle East, the Soviet Union and the former East Bloc countries. This new format represents a valuable addition to the efforts of the Service to provide long range, strategic analysis.

The Branch has produced two classified studies dealing with changes in the Soviet Union. The reader will not find in these studies the operational information usually distributed by the Service. The product is similar to what one finds in specialized open literature such as *International Security and Foreign Affairs.*

The Analysis and Production Branch also published eight issues of *Commentary* during the fiscal year. This unclassified publication addresses broad concepts and strategic situations. We commend RAP for these publications and hope they will receive wide distribution. The topics covered in *Commentary* are:

1 . Gorbachev's Manifesto;
2. KGB Glasnost: Soviet Press Interviews with KGB Officials;
3. Mikhail Gorbachev: Reformer, Revolutionary or Reactionary?;
4. Future of ex-Eastern Bloc Intelligence Personnel;
5. De Klerk and "Law and Order" in South Africa;
6. Historical and Cultural Dimensions to the Gulf Crisis of 1990;
7. Variants of Violence in South Africa; and
8. Post-war Iraq, Gulf Security and a "New World Order".

(b) Gulf Crisis

RAP contributed to Service efforts during the Gulf crisis by issuing several intelligence summaries. These addressed the crisis from different perspectives: evaluations of terrorist activities in Canada and abroad, intelligence activities, and the geostrategic situation. We were pleased to note the timely production of these summaries.

(c) Science and Technology

In the 1989-90 fiscal year, the majority of RAP's consumers asked for more information on science and technology. This year, RAP increased its production of *CSIS Reports* on science and technology by 40 per cent. In our opinion, the intelligence products have increased in their relevance and their depth of analysis.

(d) East Bloc

We took RAP to task last year for the delay we perceived in the intelligence products of the Branch in assessing the rapid and unexpected political developments in Eastern Europe. The *CSIS Reports* did catch up to the remarkable changes in the East Bloc.

(e) Executive Intelligence Production Committee

Two years ago we expressed serious concern that the Executive Intelligence Production Committee (Executive IPC) rarely met. The Executive IPC is responsible for providing overall direction to RAP. During the 1990-91 fiscal year, the Executive IPC met six times, a substantial improvement.

(f) Clients and Operational Branches

We take a special interest in the requests RAP receives from clients for special reports. Most of these requests are channelled through the Interdepartmental Intelligence Advisory Committee or through senior management in the Service. Issues such as domestic terrorism, Middle East developments and conflicts in Central Asia represent a cross-section of the requests received by RAP. We will report on a forthcoming client survey in our next annual report.

Cooperation between RAP and its sister operational branches in the Service is crucial for maintaining the quality of intelligence products and advice to Government. We note that an arrangement was completed between RAP and the Counter-Terrorism Branch to expedite the approval process for intelligence reports.

Campus Operations

Last November, the Committee met with representatives of the Canadian Association of University Teachers (CAUT). SIRC members at the meeting explained that the Committee shared many CAUT concerns and had already conducted studies on some of the issues CAUT raised. Committee members noted, for example, that in 1989-90 the Committee did three studies touching on campus operations.

This fiscal year, the Committee studied a potential blind spot in its earlier studies -- investigations, not necessarily occurring on campus, but involving academic employees.

One goal of the study was to determine if CSIS was conducting intrusive investigations on campus that were not permitted by the Ministerial direction, "Security Investigations on University Campuses". We found that the Service was not. In general, CSIS investigations on campuses were not numerous. Where investigations did occur, CSIS took care to avoid reporting on academic activities.

Another goal of our study was to examine any effect of CSIS activities on the free exchange of ideas. We found no evidence of any direct effect. However, in one case we concluded that the focus of investigations pertaining to paragraph 2(b) targets might have strayed from "foreign influence" to legitimate political activities. We understand that CSIS has taken measures to focus more precisely on the foreign influenced activities of targets.

We briefly examined less intrusive investigative activities -- in particular, interviews by CSIS officers on campus. There is at present no means of identifying all such interviews (we have recommended a logging system for such visits). Those interviews we reviewed, however, were not part of broader-investigations, and all "investigations" were brief, often involving only a single interview.

Our study reassured us. Investigations on campus are limited. There is no indication of general surveillance. We will continue to keep a close eye on campus operations approved under Ministerial direction and on any campus activity we encounter elsewhere. We also hope to begin an annual audit of on-campus interviews.

Files

(a) File Management

In fiscal year 1990-91, CSIS reviewed 271,914 files, destroyed over 200,000 of them and has sent several thousand files of historical value to the National Archives of Canada. Access to 24,612 files is restricted while they await review. Special procedures are in place to ensure that senior management approval is obtained before intelligence officers are permitted to review the restricted material.

In 1990-91, CSIS opened nearly 130,000 new files. The vast majority are screening files. These pertain to immigration, citizenship, Government checks, and checks for foreign agencies.

(b) The Special Case of Files Inherited from the RCMP Security Service

In 1984, CSIS inherited 510,000 files from the RCMP. CSIS established a unit to review the files and destroy information not meeting the requirements of sections 2 and 12 of the *CSIS Act.* To date, slightly more than half of the 510,000 files have been reviewed. Of these, 93 per cent have been destroyed, almost five per cent transferred to National Archives and less than two per cent retained.

In his report on the management by CSIS of information inherited from the RCMP Security Service, the Inspector General revealed several deficiencies in policies and procedures. These included the absence of documented standards which would lead to consistency in identifying and disposing of information about matters that did not fall within the mandate of CSIS. As well, at the time of the Inspector General's review, a substantial number of unreviewed files were accessible to CSIS personnel, even though the files may have contained information which could not have been collected lawfully under the Act. Though some controls existed on the use of inherited hard copy files, they were weak. For computer files, no specific controls existed.

Despite concerns about some aspects of the management of inherited files, the Inspector General was generally satisfied with the progress made by CSIS in reviewing and disposing of the files. As well, he was generally satisfied with the review and disposal process itself. He concluded that controls over the storage, handling and incineration of files destined for destruction were sound. This conclusion was consistent with our findings in our previous reports.

(c) The Counter-Subversion Residue: An Update

In last year's annual report, we recommended that CSIS continue to reduce the number of active files in the counter-subversion residue. The residue consists of files on the investigations of groups and individuals under section 12 and paragraph 2(d) of the *CSIS Act.*

Most of these investigations were first conducted by the RCMP Security Service. They were also investigated by the former Counter-Subversion Branch of CSIS. A special passive level of investigation was developed for these targets. The Analysis and Production Branch (RAP) was given the responsibility to monitor the residue at that low level of investigation. RAP would also alert the operational branches of the Service if the threat to national security arising from these targets increased and thus fell within their respective mandates.

Our review showed that the special passive level of investigation did not work. We recommended that the files representing suspected threats that were properly documented be given to the Cl and CT Branches. The recommendation sought to end "targeting by category".

At a press conference following the tabling of our annual report last year, the Director of CSIS announced that the Service was reviewing the residue files (there were 1,416 of them[6]). Months later, the number in the residue had been reduced to 562. The other 854 files of the 1,416 total were disposed of according to CSIS and National Archives requirements.

We have learned that a special task force in Records Management evaluated the remaining 562 files. The task force review followed new criteria set by the operational branches of the Service and by RAP itself. All 562 files were ultimately selected for disposal.

If selected for disposal, files are returned to Records Management for reclassification to other file categories, transferred to the National Archives or destroyed. When destruction is chosen, hard copies are physically destroyed and computer copies are erased from the computer data base.

We will continue to monitor the residue program.

Internal Security

In May, 1991, the Solicitor General confirmed that an ex-RCMP officer was investigated in the 1980s as a suspected Soviet agent. The Committee reviewed this case almost a year ago. Both the investigation by the Solicitor General and our own investigation were inconclusive. Too much time had passed, and the individual in question had died. The Committee has decided to examine CSIS internal security measures further.

---

[6] Last year we used the CSIS estimate of 1,400 files.

4. Review of CSIS Activities Regarding Native Canadians

Introduction

In October, 1990, the Committee reviewed the activities of CSIS in relation to native Canadians. The review covered the period from March, 1989 to July, 1990, when the violence began at Oka. The review followed an earlier Committee review of the "native extremism" investigation undertaken by the Service in late 1988 and early 1989. We report the conclusions of our reviews here.

SIRC Review of the CSIS "Native Extremism" Investigation (December, 1988 to March, 1989)

One-and-a-half years before the Oka incidents, on December 14, 1988, the Service approved a nation-wide investigation into "native extremism". The investigation was non-intrusive. The object was to prepare a detailed assessment of any potential threat to the federal government. CSIS stated that it would immediately end the investigation if it found no threat.

The targeting authorization in this case allowed the regions to interview persons who may have had pertinent information. However, CSIS Headquarters did not allow the field to use intrusive methods of investigation.

CSIS interviewed police and Government officials. It did not use its most intrusive powers, nor did it conduct community interviews. Service analysts reviewed newspaper articles and selected documents from Government agencies.

During this national investigation, CSIS requested little information from the RCMP through the primary liaison channel established for that purpose. We were told that, in large part, the RCMP viewed the incidents as criminal and not related to security. Our review of Headquarters and regional documents confirmed that this was the RCMP position.

However, some information was provided to the Service both at the regional and Headquarters levels. Our review revealed that the Service sought details about events which may have been related to national security. Under its mandate contained in paragraph 2(b) of the *CSIS Act*, the Service also examined possible foreign involvement.

The Service gave the Government its assessment of radical native activities. The advice dealt with issues such as the potential for violence.

The Committee's review of CSIS activities concluded that the inquiry was non intrusive. We did not detect any Service improprieties. Our review of documents from this period revealed no evidence of political violence posing a threat to national security. Specifically, the Committee report on the CSIS "native extremism" investigation stated that:

1. the targeting decision was in compliance with CSIS policy;
2. there was a basis for investigation under paragraph 2(c) of the *CSIS Act;*
3. the investigation was broadly-based, even though the violent and criminal activities were confined to a few reserves;
4. the investigation was non-intrusive -- a "fact finding" exercise;
5. gaps in the intelligence available to the Service resulted in a general rather than a focused targeting authorization; and
6. even though the Director was aware of this broad investigation, CSIS should have sought approval from the targeting committee chaired by the Director.

Second SIRC Review (March, 1989 to July, 1990)

Violence and threatened violence in native communities characterized the period between March, 1989 and July, 1990 -- the period immediately following the CSIS "native extremism" investigation. Also evident was violence (though largely threatened) towards non-native society. These incidents occurred mostly on a few reserves in Ontario and Quebec.

The Committee authorized its research staff to examine CSIS activities during this period. The review focused on three broad questions:

1. Did the Service receive information which showed a serious or potentially serious threat to national security from extremist elements in native communities?
2. Were CSIS activities within the law and were they based on reasonable grounds about the potential threat posed by extremist elements in native communities?
3. Based on the available information and intelligence, did the Government of Canada receive notification of any potential threat from extremist elements in native communities?

The Committee found no evidence of information collection or the use of intrusive measures. Interviews and documents revealed that CSIS senior management considered the violent events involving native Canadians during 1989 and prior to the 1990 Oka confrontation to be outside the mandate of the Service.

We noted one case where a CSIS regional office requested Headquarters permission to forward intelligence data collected during the 1988-89 CSIS "native extremism" investigation to a unit in the RCMP. However, we concluded that both CSIS and the RCMP generally viewed native incidents during the review period as criminal activities that were not related to threats to the security of Canada.

The documents the Committee examined during its second review revealed minimal interaction about native activities between CSIS and other Government departments and agencies. However, we were told that there was considerable interaction between the police and certain other Government agencies. A mass of information was exchanged among Government departments and agencies, but CSIS was not a party to these exchanges; they did not pertain to threats to the security of Canada.

CSIS advice to Government was largely based on the "native extremism" investigation. The Service focused on whether native actions presented a security threat to Canada. It is worth noting that the CSIS analysis was a general overview. It contained few, if any, details which would interest a law enforcement agency.

CSIS did not seek targeting authorization because it suspected no threat to national security. The Committee was told that the Government received a continuous flow of information on native activities. Indeed, departments received a surfeit of material from the agencies on the scene. CSIS was generally not a contributor to this information flow.

Committee Comments and Conclusions about the "Native Extremism" Investigation and Subsequent CSIS Activities

(i) General Conclusions

The Committee believes that the Service conducted a restrained and appropriate investigation between December, 1988 and March, 1989 -- the "native extremism" investigation -- into the possibility of threats to national security arising from native Canadian grievances.

After the Service presented its conclusions to the Government in mid-1989, a series of violent events occurred. The Government viewed this violence as criminal in nature. CSIS does not have a mandate to investigate or concern itself with criminal activities, even when those activities give rise to widespread violence.

(ii) Specific Conclusions

1. Between March, 1989 and July, 1990, the Service was not in receipt of reliable information that there were reasonable grounds to suspect a serious or potentially serious threat to national security from extremist elements in native communities;
2. CSIS activities were within the law, Ministerial direction and CSIS policy;
3. In 1989, the Government received information from CSIS about the potential threat from extremist elements in native communities. The information was derived largely from the "native extremism" investigation.

5. Security Screening

The Security Screening Branch of CSIS is responsible for carrying out investigations and responding to Government requests for screening for security clearances, immigration and citizenship. For two years, beginning in 1989, the Security Screening Branch was given the highest priority for receiving developmental resources. By the fall of 1991, the Service will have upgraded its automated information system, which is dedicated solely to security screening.

Role of the Service in Security Screening

The Service provides a security screening service to Government institutions under the Government Security Policy (GSP). Clearances may be needed for public sector employees or for private sector contractors. CSIS performs this function for all departments and Government institutions except the RCMP and the Department of National Defence.

Many Government employees require only a "reliability assessment". Some, however, may also require a security clearance. If so, the employee's department or agency must perform a basic or enhanced reliability assessment before requesting a security assessment from CSIS. As soon as the person is "administratively" granted basic or enhanced reliability status, the departmental security officer sends CSIS the request for a security assessment.

Security Clearances

The CSIS security assessment consists of an assessment of a person's loyalty to Canada and his or her reliability as it relates to loyalty. CSIS then recommends granting or denying a specific level of security clearance.

In performing security assessments, CSIS is not concerned about reliability in the sense of an individual's good or bad work habits. Section 2 of the *CSIS Act* defines a security assessment in part as an appraisal of *loyalty* to Canada. Section 2 therefore envisages an appraisal of the reliability of a person *only* as that reliability relates to loyalty.

Distinguishing between reliability that is relevant to loyalty and that which is not can be exceedingly difficult. Financial pressures, for example, may affect a person's reliability. However, this is not always so. If they do affect reliability, the Service must in turn judge whether this will have an impact on his or her loyalty. It must judge whether certain features of character may make an individual vulnerable to coercion to act to Canada's detriment. Also, the Service tries to determine whether the individual will engage in activities representing a threat to the security of Canada.

The different types and levels of screening and the levels of access they permit are shown in Table 2.

Table 2. Types of Personnel Screening

Screening Type	Level	Information or Asset Access
Reliability Check	Basic	Non classified or non designated
	Enhanced	Designated
Security Assessment	Level I	Confidential
		Site Access (Airports, Restricted Work Site or Facilities Programs)
	Level II	Secret
	Level III	Top Secret (10 year history) Special Access (20 year history)

A special simplified Level I (Confidential) clearance was introduced as part of the Airport Restricted Area Access Clearance Program (ARAACP) implemented in 1987. The Service performed checks on the subject and spouse only, looked back only 5 years and did no out-of-country checks. In each of the three years of the program's operation, CSIS received about 30,000 requests for ARAACP clearances.

On February 9, 1990, the Federal Court ruled the ARAACP program illegal after a union challenged its validity. Madame Justice Reed ruled that the Minister of Transport did not have sufficient delegated authority under the *Aeronautics Act* to implement the program.

CSIS immediately halted all activity on the ARAACP. On February 15, 1990, Cabinet, by Governor-in-Council decision, authorized resumption of the program. The necessary legislative changes to the *Aeronautics Act* followed.

Section 42 of the *CSIS Act* gives public servants and those contracting directly with the Government a recourse to SIRC if they are denied a security clearance. Persons employed by contracting companies, such as those under the ARAACP program, have no such right. The lack of a right to complain to SIRC for non-governmental employees (and candidates) and persons not in a direct contractual relationship with the Government constitutes a great injustice. (See chapter 8 for a more detailed discussion of this problem.)

Delays

CSIS turnaround time for security screening requests has improved noticeably. Significantly greater automation has been one reason. In addition, Government institutions are now required to perform some duties, such as processing fingerprint checks through the RCMP, before sending requests to CSIS. Also, since Level I and II clearances now remain in effect for ten years, not five, renewal requests have been halved. CSIS believes that it will meet its goals in fiscal year 1991-92.

Table 3. Mean Turnaround Time (calendar days) 1989-1991

	1989-1990	1990-1991	CSIS Goals
Level I	110	25	30
Level II	110	65	30
Level III	200	198	120

During fiscal year 1990-91, the Service received approximately 65,000 requests for Levels I, II and III security assessments. For Levels I and II, where no traces of negative information are uncovered from an indices check, the Service issues a standard form indicating the Service's recommendation to grant a clearance at the level requested, and lists the checks on which the assessment is based.

Since September, 1990 and January, 1991 respectively, the Service has issued only a recommendation for Level III clearances involving 10-year background checks and Level III clearances involving 20-year background checks. In the past, it had routinely provided information briefs. The Service defines information briefs as detailed security assessments sent to a department or federal institution and which contain information deemed to have a potential impact on the security status of an individual. Information briefs are recommendations that a security clearance be granted. Rejection briefs are recommendations that a person not be granted the level of security clearance requested. The information contained in information briefs addresses loyalty to Canada and, as it relates thereto, the reliability of an individual, or any relevant matter uncovered during verifications and investigations.

This new regime of recommendations instead of information briefs does not apply, however, to requests from External Affairs, the Communications Security Establishment and CSIS. For these institutions, any trace of potentially negative information continues to be reported in an information brief.

CSIS issued 703 information briefs in the 1990-91 fiscal year. Of these, 229 were Levels I, II or III briefs containing adverse information. CSIS issued only one rejection brief during the period.

We examined the information and rejection briefs issued to institutions accounting together for about 95 per cent of the screening requests handled by CSIS. We reviewed all briefs sent to the following institutions between April, 1989 and December, 1990:

External Affairs
Public Works
Employment and Immigration
CSIS
Finance/Treasury Board
Justice
Communications
Revenue/Taxation
Revenue/Customs and Excise
Privy Council Office.

We found that departments remain reluctant to provide CSIS with information about certain reliability issues that need to be addressed when determining basic or enhanced reliability status, even though the Government Security Policy (GSP) clearly sets out the obligation to do so. Government institutions must transmit a record of decision about any reliability issues that have been decided in favor of the individual. CSIS therefore often rediscovers negative information already known to department officials because the departments have not provided this information to CSIS in the first place. This causes unnecessary delays. In such instances, the Service puts the investigation on hold. It advises the department of the reliability issues uncovered and requests a decision from the department.

If the department, while fully aware of these reliability concerns, still wants to proceed with the security clearance, CSIS will proceed with its assessment. However, it will place less emphasis on the reliability issues that it discussed with the department. The security assessment will be affected if, and only if, this negative information can be linked to loyalty to Canada and the reliability of the individual as it relates to loyalty.

One concern we raise about this process is that negative information uncovered by CSIS could be used by departments to circumvent the complaint process provided by section 42 of the *CSIS Act*. However, the GSP should prevent this from happening. The GSP states that "if an individual has been granted basic or enhanced reliability status and adverse information is uncovered as a result of a check *not authorized for reliability* the decision on reliability status is not to be reversed".

Table 4 contains a slightly modified version of the relevant GSP document showing the responsibilities of CSIS and the departments requesting security assessments.

The security assessments we reviewed normally contained a CSIS recommendation about granting or denying a security clearance. The briefs appeared to contain objective and fair assessments. They also identified adequate grounds for drawing certain conclusions. Finally, the briefs highlighted the subtleties of deciding whether adverse characteristics affecting reliability also relate to the person's loyalty to Canada.

Most evident to us was that the Service adopts an extremely strict interpretation of the criteria that it must apply when doing security assessments. We believe that this strict interpretation is a response to a Ministerial direction of June 28, 1989. The direction requires the Director to approve all recommendations to deny a security clearance. Advice from CSIS Legal Services might also have had an impact.

Table 4. Personnel Screening Process

	Government Institution's Responsibility						CSIS Responsibilty			
	Initial Process						Initial and Update Process			
	Personal Data	Education/ professional qualifications	Employment data and reference checks	CRNC	Fingerprint check	Credit Check	Personal Character Reference	CSIS Indices Check	Field invest. of normally 10 Years background or to age 16 (whichever comes first)	Subject Interview
Reliability										
Basic	X	X	X	X[1]	X[2]					
Enhanced	X	X	X	X	X[2.3.4.5]	X[6]				
Security Clearance										
Level 1	7	7	7	X	X[2.3.5]	X	For cause	X	For cause	Pilot Project
Level 2	7	7	7		X[5]	X	For cause	X	For cause	Pilot Project
Level 3*	7	7	7		X[5]	X	X[8]	X	X[9]	Pilot Project

1 Optional, except when conducted as a prerequisite for a security clearance.
2 May be required where the results of the CRNC indicate that a criminal record may exist.
3 Optional.
4 For "current employees", may be replaced by a criminal records name check at the discretion of the deputy head.
5 For updates, the initial fingerprint check may be replaced by a CRNC.
6 Only when the duties or tasks to be performed require it.
7 Basic or enhanced reliability status must be granted prior to the request for a security clearance.
8 Mandatory for initial screening process; for cause for updates.
9 Field investigation should cover a minimum of 10 years for Level 3 clearance, and 20 years or back to age 16 (whichever comes first) for access to special material in accordance with international agreements.

Immigration Screening

Sections 14 and *15 of the CSIS Act* authorize CSIS to investigate and provide advice to the Minister of Employment and Immigration about prospective immigrants. The advice given by the Service relates to the security rejection criteria contained in paragraphs 19(l)(e), (f) and (g) of the *Immigration Act*. On average, CSIS takes 90 calendar days to perform the security screening of an immigrant.

External Affairs, Employment and Immigration, the RCMP, and CSIS conducted a pilot project to streamline immigration processing outside Canada ("profiling"). The experiment was successful, and the profiling program has been in operation in all posts abroad since June 1, 1991.

All the departments involved understand that "profiling" is an exercise in risk management. They accept it as offering the best balance between satisfying security screening interests and meeting immigration goals quickly and efficiently.

The new program entails a shift to visa officers of responsibilities previously shared by CSIS and the RCMP. Visa officers (Social Affairs Officers) are employed by External Affairs. Their duties include issuing visas and selecting immigrants under the *Immigration Act*. CSIS and the RCMP are providing them with profiles and interview guidelines. We will closely monitor the progress of the project.

With the implementation of the profiling program, visa officers now have the primary responsibility for initial security and criminality screening. This should permit CSIS to concentrate on higher risk cases.

6. Domestic Terrorism

Background

The Committee examined Service operations conducted under section 12 and paragraphs 2(b) and (c) of the *CSIS Act* against persons engaged in politically motivated violence within Canada. We specifically reviewed the CSIS investigations of national security threats from racist extremists and single issue political violence.

Racist extremists are committed to using violence to achieve their political objectives. In single issue political violence, persons or groups focus on a single, highly controversial issue. They are prepared to engage in serious political violence to attain their goals. The Service labels the activities of racist extremists and those of groups involved in single issue political violence as "domestic terrorism".

The Domestic Terrorism Program

Since 1984, many aspects of CSIS domestic terrorism operations have changed, Until 1988, the Counter-Terrorism and Counter-Subversion Branches shared responsibility for domestic terrorism investigations. In 1988, the Counter-Subversion Branch was disbanded. All domestic terrorism cases were transferred to the Counter-Terrorism Branch.

In counter-terrorism activities, targets can change frequently in response to new developments at home and abroad. In domestic terrorism, however, targets have remained somewhat static until recently.

Our Review of CSIS Investigations

We reviewed current and recent CSIS investigations, focusing on racist extremists and single issue political violence.

(a) Racist Extremists

Racist extremist groups in Canada have not always been highly organized. However, they share a common philosophy which involves an irrational fear or hatred of minority groups. To further their cause, they capitalize on a range of the public's fears about immigration, constitutional issues, native land claims and the stagnating economy.

We looked at whether the federal government should consider the investigation of these groups as solely a criminal matter. This is admittedly a "grey" area for an intelligence agency. The efforts of police and the Service may overlap and they may sometimes have the potential to

jeopardize each other's operations. We concluded that there is a limited role for CSIS, but that its role must be circumscribed by well-defined criteria.

CSIS efforts in the past have enabled it to advise the Government about the threats posed by such extremist groups in this country. Our review showed that the Service has engaged in an effective investigation of racist extremists. The Service has shifted its attention from people who exhibit little propensity for violence and has instead concentrated on the most potentially violent groups.

We have concerns about the length of three investigations. These three represent a small minority of the cases we examined. In two of the three cases, the Service started investigating individuals who had previously been targeted by the RCMP Security Service. Our review of the files from recent years did not substantiate the continuation of targeting. During our review, the Counter-Terrorism Branch dropped two of the three investigations we were concerned about and reduced the intensity of its investigation of the third target.

(b) Single Issue Political Violence

Towards the end of the 1980's, a series of acts of violence and mischief occurred. These were related to political objectives. To evaluate the extent of the threat of domestic terrorism and to determine the relationship between certain acts of violence and possible political objectives of the perpetrators, the Service conducted several non-intrusive investigations. The investigators were limited to the collection of open source information and liaison with several police forces. In two investigations, both recently terminated, CSIS monitored the activities of potentially violent figures.

We also reviewed a case where the Service targeted a person who had engaged in political violence decades ago. The Service justified its decision by stating that the individual still advocated violence to achieve a political objective. CSIS targeted the individual at the highest level of investigation for several years.

The files showed, after two years of investigation, that the individual had become isolated from the milieu which he sought to mobilize for violent action, and had lost all credibility there. The investigation then continued for two more years. Although we had reservations about the length of the investigation, we believe on balance that the Service acted reasonably at the time.

In view of the concerns we identified in these single issue political violence investigations, we were pleased to see that the Service had ended them all by early 1991.

Conclusion

The interpretation by CSIS of the "threat or use of acts of serious violence against persons or property" for political purposes (paragraph 2(c)) sometimes did not seem to correspond to the nature of the information which the Service collected. We concluded that the Service did not operate beyond its mandate, but we also found that a few investigations may have been unduly lengthy in that they continued in the absence of discernible threats to national security. Again, these cases did not represent the majority.

We are satisfied that CSIS is now more focused and selective than in the past in deciding on domestic terrorism targets.

7. Three Case Studies

The Association of New Canadians

On December 18, 1990, *The Fifth Estate* aired a program on Bulgarian refugees in Newfoundland. The program reported that the then Executive Director of the Association of New Canadians (ANC), a refugee settlement group, had provided CSIS with information. The reporter alleged that the Executive Director had breached the trust of the refugees by helping CSIS.

The ANC was formed in 1979 to deal with Vietnamese "boat people". It is a private concern, a non-governmental organization, but is largely funded by the federal and provincial governments. The ANC looks after most needs of refugees landing in Newfoundland. At one point in 1990, the ANC was dealing with 2,600 persons. Everyone was scrambling, including refugee lawyers and CSIS, to deal with this extraordinary influx.

We found that ANC employees had given CSIS the current addresses of refugees -- probably about 80 to 100. In a few instances, employees had provided information that they felt had national security implications. In some instances, they had also phoned CSIS at the behest of fearful refugee clients. We do not know in all cases what information was exchanged, because CSIS did not document all exchanges.

Some ANC employees felt that, because they were funded by the Government, they were obliged to provide information to CSIS. Others in the community, however, felt that the ANC's sole obligation was to its clientele.

Our review did not determine whether a breach of trust had occurred. We did say that CSIS was party to a *perceived* breach of trust. A climate of distrust had been created, and rumors were circulating. To the extent possible, we investigated the rumours and any possible inappropriate acts by the Service. We found no improprieties by CSIS. We also found that CSIS and ANC employees had acted without malice.

The Committee believes that there is nothing improper about the Service accepting volunteered information. Nor is it improper for Canadians to volunteer information. To be accepted and retained, however, the information must meet the tests of sections 2 and 12 of the *CSIS Act*.

We explored the issue of CSIS using information that has been obtained in actual or possible situations of trust. The Committee believes that CSIS cannot be expected to investigate the origins of all information. When the information comes from a confidential source, however, the Service has additional obligations flowing from its relationship with the source. In principle, information that may have been obtained in trust is not sacrosanct. Still, the Service should carefully weigh the threat it is investigating against the potential detriment caused by accepting confidential information.

Victor Ostrovsky

During September 1990, headlines appeared when Canadian-born author Victor Ostrovsky told the media that he had been visited at his home near Ottawa by agents of Israel's foreign intelligence agency, the Mossad. Mr. Ostrovsky stated that Mossad officers demanded he stop the release of his book, *By Way of Deception*, which allegedly reveals the activities of the Israeli agency.[1] We reviewed the affair, and now consider the matter closed.

Mohammed Al Mashat

The immigration to Canada of Iraq's ex-ambassador to the United States, Mohammed Al Mashat, gave rise to much public speculation about the role of CSIS. We investigated and sent a complete report of our findings to the Solicitor General under section 54 of the *CSIS Act.*

We found that on February 28, 1991, CSIS attended a Defectors Committee meeting chaired by External Affairs. CSIS was asked if Al Mashat would be of any intelligence value to Canada. CSIS contacted allied agencies and conducted its own evaluation. The next day, March 1, 1991, CSIS told the Committee that Al Mashat was of no intelligence value to Canada. The Defectors Committee decided that Al Mashat probably did not qualify as a defector.

On March 4, 1991, Al Mashat contacted the Canadian Embassy in Vienna to ask for an immigrant visa to Canada. CSIS then conducted the security check that is used for certain categories of potential immigrants. CSIS contacted several allied agencies and conducted a further evaluation of Al Mashat's history and activities. CSIS also arranged for a CSIS officer to interview Al Mashat in Vienna on March 5, 1991.

On March 13, 1991, CSIS informed the immigration officer in Vienna that CSIS had no evidence on which to base a recommendation under paragraphs 19(l)(e), (f) or (g) of the *Immigration Act* for rejecting Al Mashat as an immigrant. On March 28, 1991, the Canadian Embassy in Vienna issued visas to Al Mashat and his wife.

When CSIS is asked by Employment and Immigration Canada to conduct a security check on a potential immigrant, it usually takes about 90 days to complete the task. Al Mashat's check took much less time. There are good reasons for this. First, Al Mashat was well-known. It took no time in Canada or abroad to verify his identity. Also, rumors about his possible defection, though not specifically to Canada, had been circulating in European capitals for some time. This considerably speeded responses to CSIS queries. Finally, because of the Gulf War and related threats of terrorism, CSIS was completely up to date on the status of Iraqi expatriates. In fact, Canada had only recently expelled several Iraqi diplomats.

---

[1] The Ottawa Citizen, September 8, 1990.

Although the security check was completed more quickly than usual, we believe that CSIS acted responsibly and professionally. CSIS made no deals with foreign agencies or governments, and it had no interest of its own in ensuring Al Mashat's speedy entry into Canada. The speed of the security check was not the result of using special or unusual methods. It was the understandable consequence of unusually rapid responses from allied agencies and the up-to-date knowledge of CSIS itself.

8. Complaints

Complaints in 1990-91

During the 1990-91 fiscal year, we received 35 new complaints, five fewer than the year before. As Table 5 shows, most (32) were made under section 41 of the *CSIS Act* -- complaints about "any act or thing done by the Service". The Committee has not yet resolved four of the complaints; they have been carried over to 1991-92.

Table 5. Complaints Record, April 1, 1990 to March 31, 1991

	New Complaints	Carried over from 1989-90	Closed in 1990-91	Carried over 1991-92
Security Clearances	3	6	9	0
CSIS	1	0	1	0
DND	2	6	8	0
Citizenship	0	0	0	0
Immigration	0	0	0	0
Human rights	0	0	0	0
Section 41	32	0	28	4
Total	35	6	37	4

There has been a significant drop in complaints from persons refused a security clearance by the Department of National Defence (DND). In fiscal year 1989-90, we received ten complaints; in 1990-91, we received only two. Furthermore, our preliminary investigation showed that DND did not deny any security clearances in 1990-91. The two complainants had been refused contract extensions because administrative reorganization and technological change had resulted in their positions being abolished.

We have in the past strongly criticized DND's tendency to confuse concerns about reliability with concerns about national security. We have also criticized its willingness to base conclusions on inadequate evidence and to place undue emphasis on sexual orientation. Accordingly, we could not ignore the reduction of complaints involving DND. A number of factors could have contributed to a reduction in complaints to us:

- low attrition rates and force reductions leading to a low intake of new recruits into the Canadian Forces;

- the implementation of the reliability screening process within the Department (this process is also discussed in Chapter 5);
- changes in departmental personnel policies; and
- the impact of the recommendations of the Honourable René Marin in his report, *External Review of the Canadian Forces Special Investigation Unit*. The recommendations of Judge Marin undoubtedly provided considerable assistance in instituting more effective checks and balances in the security screening process.

A working group consisting of representatives from DND and other investigative bodies (CSIS and RCMP), in conjunction with Treasury Board, is still working on the establishment of clear standards with respect to investigation and related decisions. We understand that the working group has not yet presented its findings and recommendations to the Department of National Defence.

Only one new security clearance complaint involved CSIS. A preliminary investigation showed that no decision about granting a security clearance had yet been made. The delay in granting the clearance was caused by delays within Government, and not through any action or inaction by CSIS.

Accordingly, the three complaints about security clearances proved without foundation. Chapter 5 offers a more in-depth look at the role of CSIS in departmental decisions to grant or refuse security clearances.

As with the last two fiscal years, we received no complaints in 1990-91 about refusals of citizenship or rejections of persons as inadmissible under the *Immigration Act.*

Table 6. Cases Reviewed by the Committee, All Categories, 1984-1991

Categories	Received	Supported	Not Supported*	Recommendation Accepted by Departments	Recommendation Not Accepted by Departments
Section 41	179	2	177	2	0
Section 42	102	23	79	19	4***
Immigration	10	1	9	1	0
Citizenship	12	6	6	6	0
Human Rights**	3	0	3	0	0
Total	306	32	274	28	4

* "Not Supported" includes all cases which fell outside the Committee's jurisdiction.

** Referrals from the Canadian Human Rights Commission.

*** All are still before the courts on appeal.

Redress for Denial of Security Clearance

Section 42 of the *CSIS Act* allows some Canadians or landed immigrants who are denied a security clearance to complain about the denial to us. Others have no right to complain to the Committee.[1] For example, persons working on the "air side" of Canadian airports require a security clearance. Yet they have no right of complaint to us under the *CSIS Act* if they are denied a security clearance and lose employment opportunities.

This differential treatment is unwarranted and unfair. The denial of a security clearance greatly reduces employment opportunities, both in the public and private sectors -- hence, the importance of a complaints mechanism for all such denials.

In our submission to the Thacker Committee, we argued that no category of Canadians or landed immigrants should lack the right to complain to SIRC about the denial of a security clearance. Unfortunately, the Government has decided not to amend the Act to correct this deficiency.

To reduce the unfairness of the present provisions of the Act, Cabinet should instruct all departments and agencies to treat any denial of a security clearance fairly and equitably. Each person should be informed of a denial of security clearance within ten days of the denial. The person should also be informed that he or she has the right to complain to SIRC. Such a policy would give anyone denied a security clearance the right to have a third party -- this Committee -- fully investigate the denial.

---

[1] For a more complete description of this situation, see Security Intelligence Review Committee, *Amending the CSIS Act: Proposals for the Special Committee of the House of Commons 1989* (1989) at pp. 10-12.

9. Inside CSIS

Polygraph Testing

CSIS polygraph examinations fall into two general categories -- recruit screening and operations.

Since our 1985-86 Annual Report, we have inveighed against the use of the polygraph by CSIS to screen potential employees and test the loyalty of serving employees. We have noted the absence of generally accepted scientific studies establishing the validity of polygraph examinations in mass employment and security screening programs. We have pointed out that many defenders of the device admit an error rate of ten per cent or more.

We observed the lack of confidence in the use of the polygraph in security screening of the British Psychological Association and the American Psychological Association. Most courts in Canada have ruled against admitting polygraph evidence. The United Kingdom decided not to introduce the polygraph due to problems of inaccuracy and unreliability. The Government of Ontario prohibits such tests in personnel screening.

We acknowledge that CSIS has reduced the scope of its polygraph program. Participation is voluntary. The polygraph is used only to assess loyalty, not lifestyle issues. For those who wish to join CSIS, however, the polygraph is a mandatory part of the screening process.

The Service states that the polygraph examination is only one of a series of assessment procedures and is never the determining factor. Our position remains that CSIS is likely to give polygraph results more weight than they deserve. Based on the test results for recruit screening, however, we are unable to draw firm conclusions about the importance actually attributed by the Service to polygraph data.

Last year we were told that the Service had hired an external consultant to evaluate the CSIS polygraph program. We thought this an excellent idea. The Service had tested employees for some years, and a considerable data base existed for evaluation.

Late in fiscal year 1990-91 we received the consultant's report. The report surprised us. If the consultant evaluated the test data, the results were not described in the classified report we received. The report acknowledged the absence of standards or criteria covering the use of the polygraph on applicants. Much of the report centered on a Department of Justice review of issues pertaining to the *Canadian Charter of Rights and Freedoms.* The report then proposed standards for polygraph administration to meet the legal requirements.

The consultant's report offered no evaluation as such of polygraph examinations as part of the security screening process. There was no evaluation of the polygraph test results collected by the Service. Alternatives to polygraph testing were not discussed. We can only conclude that the terms of reference prevented a rigorous evaluation of the use of the polygraph as a general employment screening mechanism.

SIRC has for six years stressed that CSIS should abandon polygraph testing. We believe that the polygraph should no longer be used for general screening purposes. SIRC will continue to press this view publicly. Neither CSIS nor the Solicitor General have advanced any compelling arguments refuting our position on the abolition of polygraph screening.

Finances

One issue raised in Parliament and by the media is the growth in CSIS funding. The total of Main Estimates and Supplementary Estimates, approved by Parliament, look like this:

Total Estimates (in thousands)

1985-86	$115,908
1986-87	$132,844
1987-88	$136,861
1988-89	$157,852
1989-90	$165,417
1990-91	$205,325
1991-92	$213,951 (Main Estimates only)

Funding requirements for 1990-91 and 1991-92 have grown significantly over the 1989-90 funding level -- about 25 per cent. A large portion of this growth, over $15 million per year, is attributable to capital construction -- facilities to house the Service, including its computers. There are certain other reasons for the increases that we cannot discuss, except to say that they do not represent higher operational costs and are not linked to an increase in the level of CSIS investigations.

Fiscal year 1985-86 was a transition year. From 1986-87 to 1991-92, funding jumped by over $80 million. Some of this increase (estimated conservatively at $25 million) is related to inflation. Some relates to the recommendations of the independent Advisory Team (the Osbaldeston Committee), and some to Government-wide initiatives, such as increased airport security.

10. Inside SIRC

Staying in Touch

On February 14, 1991, we held a seminar in Vancouver. We invited academics, lawyers and other experts to exchange views on "CSIS After the Thacker Committee Report: Where to From Here?". We are grateful to those who spent the day with us to discuss this issue. Their names are listed in Appendix C.

On January 23, 1991, the Chairman, Mr. John Bassett, spoke in Toronto to the Institute of Corporate Directors in Canada. Ms. Paule Gauthier addressed the New Brunswick Branch of the Canadian Bar Association on February 2, 1991, and Mr. Saul Cherniack spoke to a meeting of Saskatchewan Provincial Judges on May 30, 1991.

Accounting to Parliament

We appeared before the House of Commons Standing Committee on Justice and Solicitor General on June 4, 1991, to answer questions on a variety of issues. We were asked specifically about relations between CSIS and other domestic and foreign agencies and whether CSIS has "tasked" any agency with which it does not have a memorandum of understanding. Concern was expressed in particular about information passing from CSE, an agency with no statutory mandate, to CSIS. We explained that we were awaiting a report from the Inspector General on the relationship between CSIS and CSE (We reported the Inspector General's findings in Chapter 2.).

Spending

Our 1990-91 budget is set out in Table 7. At $1,505,000, it represents an increase of 7.6 per cent from actual spending of $1,399,000 in 1989-90. The increase was largely due to the addition of research positions. Our 1991-92 estimate of $1,568,000 represents an increase of 4.2 per cent over the 1990-91 budget.

During the 1990-91 fiscal year, our budget was reduced by $25,000 as a contribution to the financing of the Gulf War. In addition, we handed back $43,000 to the Government due to a surplus. Accordingly, of our planned 1990-91 budget of $1,505,000, we returned a total of $68,000 to the Government.

Table 7. SIRC Budget 1990-91

Personnel		$728,000
Salaries and wages	$630,000	
Contributions to employee benefit plans	$98,000	
Goods and services		$768,000
Professional and special services	$611,000	
Other	$157,000	
Total operating expenditures		$1,496,000
Capital expenditures		$9,000
Total		$1,505,000

Source: 1991-92 Estimates, Part III, figure 7

Personnel

The Committee has a staff of fourteen: the Executive Director handles the day-today operations of the office; the Senior Complaints Officer handles complaints and ministerial reports; the Director of Research (Counter-Terrorism), the Director of Research (Counter-Intelligence) and four Research Officers; an Executive Assistant co-ordinates activities on behalf of the Chairman, conducts all media liaison, co-ordinates the production of the annual report, and undertakes research projects; an administrative officer who is also the Committee registrar for hearings; and an administrative support staff of four.

At its monthly meetings the Committee decides the research and other activities it wishes to pursue and sets priorities for the staff.

Appendices

A. SIRC Reports and Studies since 1984

(Section 54 reports -- special reports the Committee makes to the Minister -- are indicated with an asterisk)

Eighteen Months after Separation: An Assessment of CSIS' Approach to Staffing Training and Related Issues, April 1986 (139 pages/SECRET) *

Report on a Review of Security Screening for Applicants and Employees of the Federal Public Service, May 1986 (SECRET) *

Ottawa Airport Security Alert, March 1987 (SECRET)*

The Security and Intelligence Network in the Government of Canada: A Description, January 1987 (61 pages/SECRET) *

Report to the Solicitor General of Canada Concerning CSIS' Performance of its Functions, May 1987 (SECRET)

Closing the Gaps: Official Languages and Staff Relations in the CSIS, June 1987 (60 pages/UNCLASSIFIED)*

Counter-Subversion: SIRC Staff Report, August 1987 (350 pages/SECRET)

SIRC Report on Immigration Screening, January 1988 (32 pages/SECRET) *

Report to the Solicitor General of Canada on CSIS' Use of Its Investigative Powers with Respect to the Labour Movement, March 1988 (18 pages/PUBLIC VERSION) *

The Intelligence Assessment Branch: A SIRC Review of the Production Process, September 1988 (80+ pages/SECRET) *

SIRC Review of the Counter- Terrorism Program in the CSIS, November 1988 (300+ pages/TOP SECRET) *

Report to the Solicitor General of Canada on Protecting Scientific and Technological Assets in Canada: The Role of CSIS, April 1989 (35-40 pages/SECRET) *

SIRC Report on CSIS Activities Regarding the Canadian Peace Movement, June 1989 (540 pages/SECRET) *

A Review of CSIS Policy and Practices Relating to Unauthorized Disclosures of Classified Information, August 1989 (SECRET) *

Report to the Solicitor General of Canada on Citizenship/Third Party Information, September 1989 (SECRET) *

Amending the CSIS Act: Proposals for the Special Committee o the House of Commons, September 1989 (UNCLASSIFIED)

Supplement to *SIRC Report on Immigration Screening* (January 1988), November 1989 (SECRET) *

A Review of the Counter-Intelligence Program in the CSIS, November 1989 (700 pages/TOP SECRET) *

SIRC Report on the Innu Interview and the Native Extremism Investigation, November 1989 (SECRET) *

Section 2(d) Targets -- A SIRC Study of the Counter-Subversion Branch Residue, September 1990 (SECRET)

Domestic Exchanges of Information, September 1990 (SECRET)*

Regional Studies (six studies relating to one region), October 1990 (TOP SECRET)

Investigations, Source Tasking and Information Reporting on 2(b) Targets, November 1990 (TOP SECRET)

Security investigations on University Campuses, February 1991 (TOP SECRET)*

Release of Information to Foreign Agencies, January 1991 (TOP SECRET)*

CSIS Activities Regarding Native Canadians -- A SIRC Review, January 1991 (SECRET)*

Report on Multiple Targeting, February 1991 (SECRET)

Review of the Investigation of Bull, Space Research Corporation and Iraq, May 1991 (SECRET)

Report on Al Mashat's Immigration to Canada, May 1991 (SECRET)*

B. Complaints Case Histories

Following are brief outlines of complaints on which SIRC reached decisions in 1990-91. Complaints that were withdrawn or resolved before the Committee completed its investigations, or that were beyond the Committee's jurisdiction, are not reviewed here.

Department of National Defence (DND) - Case 1

The individual complained about the Department's denial of any level of security clearance. In March, 1987, the complainant had graduated first in the class and was promoted to the rank of Second Lieutenant. In May 1987, the complainant received a Level III security clearance. From November, 1987 to May, 1988, the complainant was enrolled in Basic Security Officer Training, and again graduated first in the class.

The complainant was to be promoted on graduation from security training in May, 1988. In June, 1988, the complainant was assigned to the Central Detachment of the Special Investigation Unit (SIU) of the Military Police. When the complainant received the promotion message, she was the subject of an SIU investigation initiated in May, 1988. The promotion was consequently held in abeyance.

The SIU was investigating allegations that the complainant was engaged in a homosexual liaison. The decision to deny any level of security clearance was made in April, 1989. The complainant submitted her complaint to the Committee in August, 1989.

The Department challenged the Committee's jurisdiction to hear the case. DND counsel argued that the Committee could investigate complaints as long as the loss of a security clearance was the *only* reason for any action taken, such as dismissal, demotion or transfer. The Department argued that the complainant's homosexuality brought her within the "Canadian Forces Interim Policy CFAO 19-20", which permits administrative release.

An "administrative release" requires either an acknowledgment that a member is a homosexual, or that DND considers the member to be a homosexual; and that the member desires to be released, or the member does not object to being released according to the Regulations. If the member does not agree to be released, the member will be retained with career restrictions (no promotion, no career courses).

On October 24, 1989, the Chairman of the Committee rendered a decision that the Committee had jurisdiction to investigate. DND applied to the Trial Division of the Federal Court to prevent the Committee from investigating the complaint. On March 30, 1990, Mr. Justice Cullen dismissed DND's application and decided that the Committee had jurisdiction to investigate:

> What is quite clear however is that a decision was made to transfer [the complainant] from a sensitive post calling for a high security clearance to one where a lesser degree of security clearance was required. I agree with counsel for the respondent ... that Section 42(l) of the Canadian Security Intelligence Service Act, has only 2 requirements, namely a decision be made to dismiss or transfer, and by reason only of a denial of a security clearance. The document -- Change of Circumstances leaves no room for doubt that security clearance was the basis for the transfer to another job.
>
> Also SIRC, following the procedures outlined in the Act determined it had jurisdiction. I cannot find any error in law, or that the decision was so patently unreasonable that gives the Court authority to sign an Order prohibiting the review.

The Committee accordingly investigated. The Committee rendered a report recommending that the complainant be granted a Top Secret security clearance retroactive to April 17, 1989, and that her employment be reinstated.

Not believing that the Committee had the mandate or the authority to decide the constitutional validity of departmental policies bearing on the security clearance cases coming before the Committee, the presiding member commented that, in the Committee's opinion, such a policy was inconsistent with the *Constitution Act, 1982,* as it violated subsection 15(l) of the *Charter.*

On August 24, 1990, the Minister of National Defence asked the Federal Court to review the Committee's report. The case has not yet been heard.

Department of National Defence - Case 2

The complainant had allegedly been involved in a theft. As a result, the Department reduced the complainant's security clearance from Level III (Top Secret) to Level II (Secret). The complainant contended that the reduction in his security clearance had resulted in his being denied a transfer in that he could not attend a year-long career course in the United States.

The Department argued that the change in security clearance level had not caused the complainant to be "dismissed, demoted or denied a promotion", as would be required before he could complain under section 42 of the *CSIS Act.* In fact, only three months after the downgrading in security clearance, the individual was promoted. However, the reduction in security clearance level meant the complainant was not qualified for approximately 80 per cent of the positions available at his rank.

The Committee concluded that it could not offer appropriate redress for persons denied a security clearance if it interpreted the word "transfer" in section 42 as did DND. The presiding Committee member took into consideration *Blacks Law Dictionary, the American Heritage Dictionary of the*

English Language and the *Shorter Oxford English Dictionary*. The member also considered the rules for interpreting statutes, the object and purpose of the review mechanism of the *CSIS Act* and the effect of the change in the complainant's security clearance level. The presiding member concluded that the Committee had jurisdiction to investigate the complaint.

The presiding member further concluded that it was not the Committee's role to decide whether the complainant was guilty of a charge for which he had received a court discharge. The important issue was to assess whether the complainant was a security risk.

The Committee concluded that DND could not have been convinced that the cornplainant was truly a security risk. The downgrading of the individual's security clearance from Level III (Top Secret) to Level II (Secret) with a provision that the individual would soon have his Level III clearance restored was accompanied by a promotion, three months after the downgrading. The presiding member concluded that the downgrading constituted more of a slap on the wrist than a true response to concerns about national security. A recommendation that the Level III security clearance be restored to the complainant was issued.

DND accepted our recommendation.

Department of National Defence - Case 3

DND notified the complainant that his Level II (Secret) security clearance for employment with the Canadian Forces was being denied and that a review would not be conducted until 24 months had passed. The Department felt that the complainant was not reliable because he used drugs and was dishonest in not admitting this.

The Committee investigated and found that the complainant's late admission to using drugs, and the extent of the use, clearly indicated some dishonesty. This raised questions of reliability as it related to loyalty.

The complainant accepted that the Department's decision to deny a Level 11 security clearance was correct at the time. He maintained that a review of that decision was nonetheless warranted because he had changed for the better.

The Committee saw clear indications of a change in lifestyle. Accordingly, it recommended reducing the length of time that must pass before a review of the denial of the clearance.

DND accepted our recommendation.

C. Vancouver Seminar (February 14, 1991)

On February 14, 1991, the lawyers and scholars listed here accepted the Committee's invitation to attend a seminar on "CSIS After the Thacker Committee Report: Where to From Here?". They did so without fee. The Committee is grateful to them for their contribution to its thinking on the topics discussed.

Professor Phillip Bryden
Faculty of Law
University of British Columbia
Vancouver

Karen Busby
Assistant Professor
Faculty of Law
University of Manitoba
Winnipeg

Michael De Rosenroll
Assistant Inspector General
Ottawa

Stuart Farson
Ganges
B. C.

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

Georges A. Goyer
Barrister and Solicitor
Vancouver

George Gould
Barrister and Solicitor
Vancouver

Ted Hughes
B.C. Police Commission
Victoria

Mark Hillford
Barrister and Solicitor
Vancouver

Craig Patterson
Barrister and Solicitor
Vancouver

Art Lee
Barrister and Solicitor
Vancouver

Professor Patrick Smith
Department of Political Science
Simon Fraser University
Burnaby

Professor Murray Rankin
Faculty of Law
University of Victoria
Victoria

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

Don Stewart
MacLeod's Books
Vancouver

John Westwood
B.C. Civil Liberties Association
Vancouver

Maurice Tugwell
President
Mackenzie Institute
Toronto

D. SIRC Counsel

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

Gina S. Brannan, Toronto

Pierre-C. Gagnon, Quebec City

Gordon Hilliker, Vancouver

Robert E. Houston, Q.C., Ottawa

Jack R. London, Q.C., Winnipeg

Robert W. MacQuarrie, Q.C., Ottawa

Mel Myers, Q.C., Winnipeg

Christopher J. Roper, Toronto

Perry W. Schulman, Q.C., Winnipeg

Jacques Shore, Ottawa

Leslie Vandor, Ottawa

Grant Kenneth Weaver, Vancouver

David L. Zifkin, Toronto

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

Edward L. Gladu, Q.C., Ottawa

William G. Horton, Toronto

John B. Laskin, Toronto

Allan Lutfy, Q.C., Ottawa

Eva E. Marszewski, Toronto

Simon Noel, Hull

Mary E. Saunders, Vancouver

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

John M. Sibley, Toronto

J. Peter Vice, Q.C., Ottawa

Alan Whiteley, Toronto

E. SIRC Staff Directory

Following is a directory of the SIRC staff as of August 31, 1991, when this report went to the printers.

Maurice Archdeacon, Executive Director	(613)990-6839
Pierrette Chenier, 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	990-8051
Elaine Grant, Research Officer	991-9112
Sylvia MacKenzie, 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