



SECURITY INTELLIGENCE
REVIEW COMMITTEE

Annual Report

1995-96

Canada

Security Intelligence Review Committee
122 Bank Street
P.O. Box 2430, Station D
Ottawa, Ontario
K1P 5W5

Tel: (613) 990-8441

Fax: (613) 990-5230

Web Site: <http://www.sirc-csars.gc.ca>

Collect calls are accepted, and the switchboard is open
from 7:30 a.m. to 5:00 p.m. Eastern Standard Time.

© Minister of Supply and Services Canada 1995

Cat. No. JS71-1/1995

ISBN 0-662-61343-0

The Honourable Herb Gray, P.C., M.P.
Solicitor General of Canada
House of Commons
Ottawa, Ontario
K1A 0A6

30 September 1996

Dear Mr. Gray:

As required by section 53 of the *Canadian Security Intelligence Service Act*, we transmit to you the Annual Report of the Security Intelligence Review Committee for the fiscal year 1995-96, for your submission to Parliament.

Yours sincerely,

Edwin A. Goodman, P.C., O.C., Q.C.
Chairman

Rosemary Brown, P.C., O.C., O.B.C.

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

George W. Vari, P.C., O.C., C.L.H.

Table of Contents

1.	INTRODUCTION	1
2.	CASE STUDIES	3
	(a) Alleged Interference with a Trial	3
	(b) Investigation of a Foreign State’s Intelligence Services	4
	(c) CSIS and an Alleged Terrorist	6
	(d) CSIS and a “Walk-In”	7
	(e) Foreign Interference with Democratic Processes	8
3.	CSIS OPERATIONS	9
	(a) Arrangements with Other Departments and Governments	9
	(i) Domestic Arrangements	9
	(ii) Foreign Arrangements	9
	(b) Exchanges of Information with Foreign and Domestic Agencies	10
	(i) Foreign Exchanges of Information	10
	(c) Warrants and Warrant Statistics	12
	(d) Counter Terrorism (CT) Branch	14
	(i) Threat Assessments	14
	(e) Counter Intelligence (CI) Branch	15
	(f) Analysis and Production Branch	15
	(i) Security Intelligence Reports	15
	(ii) Review of RAP Reports	16
	(g) File Management	16
	(h) Foreign Intelligence	17
	(i) Statistics on Operational Activities	18
4.	SECURITY SCREENING	19
	(a) Government Security Screening	19
	(i) Application of the “normally ten year rule”	20
	(ii) Incomplete Assessments	20
	(b) Immigration Screening	21
	(c) Citizenship Screening	22
	(d) Screening on behalf of Foreign Agencies	22
5.	COMPLAINTS	23
	(a) Statistics	23
	(b) Complaints Against the Service’s Activities	23
	(i) Prerequisite to the Committee’s Jurisdiction	23
	(ii) Examples of Complaints Against the Service	24
	(c) Security Clearance Complaints	27

(d)	Ministerial Reports by the Minister of Citizenship and Immigration Canada and the Solicitor General	28
(e)	Canadian Human Rights Commission Referral	28
6.	REGIONAL AUDITS	29
(a)	General	29
(b)	Targeting	29
(i)	The Counter Intelligence Investigations	29
(ii)	The Counter Terrorism Investigations	31
(c)	Sensitive Operations	32
(d)	Surveillance	32
(e)	Community Interviews	33
7.	REVIEW OF GENERAL MATTERS	37
(a)	Ministerial Direction	37
(b)	Changes in Instruction	37
(c)	Disclosures in the Public Interest	38
(d)	Regulations	38
(e)	Report of the Director and Certificate of the Inspector General	38
(f)	Reports of the Inspector General	39
(g)	Unlawful Conduct	39
(h)	SIRC Consultations and Inquiries	40
(i)	Formal Inquiries	40
(ii)	Briefings	40
(iii)	Beyond CSIS	40
(i)	Special Reports	41
8.	INSIDE CSIS	42
(a)	Recruitment	42
(b)	Finances	42
9.	INSIDE SIRC	44
(a)	Accounting to Parliament	44
(b)	Staying in Touch	44
(c)	Impact of Budget Changes	44
(d)	Personnel	46
A.	GLOSSARY	47
B.	SIRC REPORTS AND STUDIES SINCE 1984	49

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 and ears 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* (the *CSIS Act*). CSIS investigates terrorists, agents of hostile intelligence services, and others whose activities may be a “threat to the security of Canada.” CSIS must protect its sources and methods. Inevitably, therefore, much of its work remains secret. This makes it difficult for Members of Parliament 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 pre-empt these potential problems, the same law that created CSIS created SIRC.

The Committee is independent of the Government in its operations, but responsible to the Parliament of Canada. The *CSIS Act* provides that its members are appointed by the Governor General in Council, after consultation by the Prime Minister with 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 order of the Governor General in Council.

To the extent that national security permits, the Committee reports to Parliament through its Annual Report. This is available to the public. It constitutes an evaluation of 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 or revocations 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.

Third, 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.

1. Introduction

We present our twelfth Annual Report on a note of sadness. Our Chairman, the Honourable E. Jacques Courtois, P.C., Q.C., died after a short illness on 3 July 1996.

Mr. Courtois brought integrity, commitment, and a sense of fairness and justice to the service of the Review Committee. We will sorely miss his wisdom and good judgement.

As the following chapters illustrate, we have now returned to our usual area-by-area examination of CSIS' activities, following the disruption caused by the Heritage Front Affair. As is to be expected, our report includes some criticism and an occasional commendation, but, on the whole, it is a descriptive document.

Our aim is to provide a steadily broadening and deepening public base of information about what CSIS does, why those activities are necessary, and how well the Service carries them out. There is so much myth and legend surrounding the activities of intelligence services that the true picture of what they usually do: routine, mundane, and often boring hard work, is rarely described. We hope to give the Canadian Public a picture of what takes place in the Security Service they own and pay for.

Naturally, there are areas that we can discuss publicly in only the most general terms. CSIS' mandate is to deal with foreign intelligence agencies acting in our country, and with terrorist organizations wherever they are based. This work requires a considerable degree of secrecy if it is to be effective. As is evident from recent events, terrorists make no distinctions between the innocent and the guilty, or between soldiers and civilians; everyone is at risk at their hands. It is in every Canadian's best interest that CSIS conduct its affairs effectively, within the law, and with sufficient protection for its human sources and for operations that must be kept secret. It is our responsibility to review CSIS' activities and then to assure the public that we know what CSIS is doing, that we believe that those activities are necessary, and that they are being conducted in an appropriate and legal fashion.

In June 1996, the House of Commons Sub-Committee on National Security released its report on the Heritage Front Affair. We do not agree with much of what the Sub-Committee had to say. However, since we were given the opportunity to present our point of view during more than sixteen hours of testimony, but were unable to convince the members to change their minds, we do not intend to try to do so here. We now consider the matter closed.

On 1 August 1996, the Federal Court ruled that the Committee could not fulfil its statutory obligation pursuant to the *Citizenship Act, R.S.C. 1985, c.C-29*. The Court prohibited us from conducting an investigation into the denial of Mr. Ernst Zündel's application for Canadian Citizenship.

In his reasons, Mr. Justice Darrel V. Heald said, in effect, that the Committee had revealed its bias against Mr. Zündel by the way in which it referred to him in the Heritage Front Affair report. The Committee had referred to Mr. Zündel as a publisher of hate literature, a Holocaust denier, and a member of the radical right. The Judge said that it was apparent from The Heritage Front

Affair report that "... SIRC has had an opportunity to assess the credibility of Zündel and has found him, in several instances, to lack credibility."

Mr. Justice Heald also cited our statement that:

"Finally, we would like to put on the record our unshakeable conviction that the Government of Canada, through all means at its disposal, should continue to ensure that it is always aware of what is going on within extreme right wing racist and Neo-Nazi groups. Canadians should never again repeat the mistakes of the past by underestimating the potential for harm embodied in hate-driven organizations."

sentiments with which we hope most Canadians are in agreement.

We should add that being a member of the radical right, denying the Holocaust, or even publishing hate literature are not sufficient grounds for the denial of citizenship under current statutes. According to section 2(c) of the *CSIS Act*, only "activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political objective within Canada or a foreign state" would constitute sufficient grounds for the Committee to conclude that it should support a denial of citizenship. The Committee did not come to such a conclusion in its report on the Heritage Front Affair.

By the time this Annual Report is published, the Committee will be on the World Wide Web. We hope to provide a sufficient amount of information to make our "Home Page" a worthwhile place to visit for researchers or simply for those who have an interest in security intelligence affairs. The web site will include directions about how to contact us with suggestions about the site itself or any other matter. Our web address is <http://www.sirc-csars.gc.ca>

2. Case Studies

(a) Alleged Interference with a Trial

SIRC investigated a media allegation that CSIS may have been responsible for a witness in Canada refusing to testify in a United States trial of suspected supporters of a prominent overseas terrorist organization. The purpose of our review was to assess the Service's actions in this case.

The media articles quoted the American defence attorney representing one of the suspects. The Counsel stated that the witness from Canada initially agreed to cooperate, but later refused. The witness reportedly told the attorney that CSIS warned him that his status in Canada would be jeopardized if he testified at the United States trial.

Among those we sought to interview was the journalist who reported the allegations. He refused to meet with our staff, citing his editors' objections. We did interview the trial suspect's lawyer, and we communicated with the police and the counsel for the witness.

The media article reported that the witness was secretly taped by the police during a conversation with one of the trial suspects in Toronto. United States federal prosecutors alleged that the two men discussed the purchase of detonators and how to conceal those that they had already acquired. The surveillance tape was of poor quality and the defence lawyer wanted the witness in Canada to corroborate the defence's interpretation of the conversation. He claimed that the witness refused to assist in the case because of CSIS' interference.

Also according to the media, the suspect in the US trial was one of 14 men accused of conspiring to purchase explosive detonators and a Stinger surface-to-air missile for the terrorist organization. The prosecution's interpretation of the surveillance tape prompted the Assistant United States Attorney in the case, to refer to the possible witness from Canada, as an "unindicted co-conspirator."

The allegation about CSIS interference was first brought to the Service's attention when the police advised that they had learned of it from United States authorities. The police had served the witness with a subpoena on behalf of the American Attorney General, requesting that he testify on behalf of the prosecution.

We learned that CSIS interviewed the witness twice on a matter unrelated to the American investigation. The witness informed CSIS that he had declined the invitation from the American authorities to testify at the US trial. The Service did not pose additional questions about the trial during the interviews, nor did the investigators give advice regarding the matter.

The information we acquired from the police and the witness's attorney corroborated the Service's file information that CSIS investigators did not threaten the witness about his status

in Canada. We saw no evidence, furthermore, that the CSIS interviews deterred the witness from attending the trial.

Yet the witness did not go to the United States. Two plausible theories were advanced to us as to why the witness did not attend the trial, although neither could be substantiated. The witness may have feared being arrested for the alleged role he played in obtaining the detonators. This may also have contributed to his reluctance to cooperate with the defence. Or, the witness may have provided the American attorneys with the excuse that CSIS warned him not to go, rather than admit his apprehension, and possibly jeopardize his relationship with supporters of the extremist group.

Based on the information we obtained from intelligence, police, and other sources, we concluded that the Service did not warn the possible witness that his status in Canada would be jeopardized if he testified at the American trial.

(b) Investigation of a Foreign State’s Intelligence Services

On 14 May 1996, the Solicitor General told the House of Commons that “we play a prominent role in the world community, and we all know well that, in places, this world community is fraught with strife and unrest. In this environment, persistent threats must be dealt with and new ones emerge almost daily.”¹ We examined the intelligence services operated by one of those “persistent threats.”

The state operating the intelligence services has a questionable human rights record, and reputedly has been involved in aiding terrorists. We wanted to determine whether CSIS assessments of the threats posed by the intelligence services were legitimate and whether the investigation complied with Ministerial Direction. We also examined the accuracy and adequacy of the advice concerning the intelligence services that CSIS provided to clients.

We examined all the files relating to CSIS investigations of the intelligence services covering a ten year period. We evaluated the following potential threats:

- ▶ support for Canadian extremists operating in a foreign country;
- ▶ covert associations with foreign extremists operating overseas;
- ▶ manipulation of ethnic communities and political interference; and
- ▶ the presence of undeclared intelligence officers in Canada.

¹ “Statement on National Security”, Honourable Herb Gray, 14 May 1996.

All the threats were well substantiated, although CSIS is still attempting to obtain some important additional information.

We examined the Target Approval and Review Committee (TARC) authorizations to ensure that investigations were justified and not excessive. All section 12 CSIS investigations require a TARC authorization. We verified statements in the “Request for Authority”, the application to TARC for an authority to investigate, to ensure that raw intelligence or other information supported the facts provided as the basis for the application. In one case, we came upon an instance in which supporting raw intelligence was not available. The documentation had been returned to the donor agency. The document in question appeared to be central to the authorization. We were told that as a matter of course, CSIS does not keep the documents themselves, but retains only a reference and a report number in the CSIS computer system. If need be, CSIS can recall the documents from the donor agency. Because the documents were not in the possession of CSIS, they were unavailable to SIRC for review. This issue is discussed further on page 6.

We noticed two other problems in the same “Request for Authority.”

The “Request” cited a deal offered to a terrorist by an agent of the foreign intelligence services. The involvement of the agent, according to CSIS, had been inferred from the context rather than being verified directly.

Under 2(b) of the *CSIS Act*, threat-related activities must be “foreign influenced”, “a detriment to the interests of Canada” and “clandestine or deceptive or involve a threat to any person.” In the “Request for Authority”, CSIS noted that information collected by the foreign intelligence services “can be used against persons in the community in the form of coercion and visa denials.” The “Request”, however, provides no intelligence to support this thesis. CSIS argued that one purpose of the investigation was to acquire the information in question.

We examined the extent of the investigations conducted against the intelligence services. The resources allocated to the investigations were not large, and CSIS officers frequently depended on information gathered in other investigations. We noted minor communication problems between desks in the Counter Intelligence (CI) and Counter Terrorism (CT) Branches. We also observed that the CT Branch had been given lead responsibility for the part of the investigations seeking to identify foreign intelligence officers in Canada, usually a job for the CI Branch. We were told that the CT Branch had been placed in charge to coordinate diverse, interlinked investigations, and to resolve communications problems.

We discovered that CSIS had exchanged security intelligence information in the absence of a section 17 agreement. Officers explained that they had mistakenly assumed that an agreement submitted to the Solicitor General had been approved. In addition, CSIS had not consulted with the Minister in a timely fashion concerning “threats posed by foreign representatives” as is required by Ministerial Direction. We were told that the problem arose from the

miscommunication of information within CSIS, and from CSIS to other departments. The Director of CSIS personally notified the Minister of both errors.

The investigations themselves were not problematic. In particular, we agreed with the procedures used in the investigation. These particular procedures are rarely used and are, in fact, prohibited in the case of Security Clearance interviews. However, in these circumstances there appeared to be legitimate reason for their use.

An important part of almost every Committee review is the examination of supporting documentation for “Requests for Authority” so as to determine the legitimacy of the decision to conduct investigations. In one “Request for Authority”, an important supporting document was unavailable for review. Thus, the Committee could not confirm crucial facts upon which the authorization was based, and could have been placed in the position of being unable to confirm the legitimacy of an authorization. By happenstance, other information from the donor agency was available so that the TARC “Request for Authority” could have been supported without reference to the missing documentation. This other information had been retained despite the policy that required its immediate return.

We strongly recommend that any supporting document or telex used as a reference in a TARC “Request for Authority” or a warrant affidavit be made available upon request to SIRC.

(c) CSIS and an Alleged Terrorist

When a person was arrested in Canada and was described as an alleged terrorist, based on erroneous information, SIRC reviewed the case to determine whether the Service was involved in this matter. In the course of the review, the Committee examined the nature of the information that CSIS received from or provided to foreign and domestic agencies.

We learned that during a major investigation, the Service received information that the person might be sought by other agencies. This and other information raised the possibility for CSIS that he might have been sent to Canada on behalf of a terrorist organization. Consequently, the Service sought information from other agencies about the individual.

The information that CSIS received indicated that the person had associated in the past with violence-prone groups, but the data did not support the allegation about his involvement in terrorism. CSIS notified other Canadian agencies about the information and added that the Service was not aware that the person was involved in any threat-related activity in Canada.

In further correspondence between CSIS and the other agencies, we noted that the Service stipulated that it had no interest in the person due to the criminal nature of his offences.

We concluded that CSIS placed the third party information in context when supplying the data to other agencies. Thus, the Service provided a fair and balanced assessment of the individual to its clients.

(d) CSIS and a “Walk-In”

Information provided by individuals plays a significant role in the Service’s collection of information concerning threats to the security of Canada. In one case, an individual provided unsolicited information to the Service and later complained that he had been lied to by CSIS. Subsequently he became a devoted follower of an individual he was associated with. His life changed dramatically, and he became estranged from family and friends. Some observers complained that CSIS had provided significant financial support to an extremist group and that the individual concerned was used inappropriately by the Service.

To conduct our review, we spoke to former employers, friends, and other individuals concerning the case. We examined all relevant CSIS files. We reviewed other reports that were prepared outside the Service regarding the individual concerned. We spoke to CSIS employees and managers, and, finally, we spoke to the individual. We pieced together the events surrounding the allegations and we reached the following conclusions.

CSIS had provided a very limited amount of assistance to the individual over the duration of a relationship that lasted six months. Initially, the individual appeared to be normal, intelligent and capable. Various outside observers said that they did not view the individual as being “troubled.”

CSIS officers did not withhold any information concerning potential danger to the individual, because they were not aware of any potential danger.

When the contact between the individual and CSIS ended, CSIS reevaluated the relationship. In the reevaluation, officers discovered problems concerning the individual that had not been readily evident at the commencement of the relationship, and were not recorded.

With the benefit of hindsight, everyone, including CSIS, recognized that a relationship with this individual was problematic. On the other hand, a number of allegations concerning the individual’s involvement with CSIS were totally untrue, particularly the allegation that CSIS spent thousands of dollars supporting domestic extremists.

We can find no neglect or malice in CSIS activities in relation to the individual in question. He offered information, and it was accepted. Officers assessed the individual to the extent required by policy.

(e) Foreign Interference with Democratic Processes

At the October 1995 Meeting, Committee Members directed staff to keep them “fully informed” of any activities, or any investigation of activities, relating to interference by foreign intelligence services in Canadian democratic processes, such as elections or referendums. This direction arose from a report discussed in last year’s Annual Report: “CSIS Investigations of Certain Intelligence Services.”

At a June 1996 meeting, the Committee examined the findings of a review of relevant operational reports and related documents covering 1995. It determined that CSIS had not conducted any investigations touching upon democratic processes and in fact had assiduously avoided any such investigation. There was a single report, unsolicited, of possible foreign interference, that the Service refused to pursue further. We are also of the view that the report was not credible.

3. CSIS Operations

(a) Arrangements with Other Departments and Governments

(i) Domestic Arrangements

To carry out its mandate, CSIS cooperates with police forces, and federal and provincial departments and agencies. The Service enters into agreements to cooperate with domestic agencies after having received the authorization of the Solicitor General. Cooperation includes exchanging information and intelligence and, less commonly, cooperating in operations.

In fiscal year 1995-96, CSIS did not sign any new agreements or make any amendments to existing agreements with domestic government institutions. According to CSIS, all the agreements are working well, including two signed the previous fiscal year with Environment Canada and Ports Canada Police.

In last year's annual report, we noted that CSIS was discussing with the Province of Alberta the impact of new provincial privacy and access to information legislation, the *Freedom of Information and Protection of Privacy Act*. According to CSIS, its agreement with the Province of Alberta remained unchanged because it has not noticed any negative impact due to the new legislation. CSIS continues to acquire information from some provincial institutions and Service information passed to the Alberta Government remains protected.

Under section 38, the Committee also monitors the exchanges of information between the Service and government organizations, and police forces. This review is presently underway and we will report the results in next year's annual report.

(ii) Foreign Arrangements

As of 31 March 1996, the Service had a total of 202 arrangements with 123 countries and three international organizations. During fiscal year 1995-96, CSIS established liaison arrangements with a number of foreign agencies in Europe and Africa.

In Europe, the Service has embarked on an active but cautious program to forge liaison arrangements with some former adversaries. These relationships are an attempt, at least in part, to show the foreign agencies that they could benefit more from cooperation with CSIS, than from resorting to espionage in Canada. The new arrangements with these agencies cover information exchanges pertaining to international terrorism, international criminal organizations and proliferation.

In Africa, the human rights records of the predecessors of two of the agencies were abysmal, and the two "replacement" agencies do not yet have a track record on which to assess their

erformance. The Service has been advised to exercise caution in the development of the relationships.

Another agency is located in a state that is embroiled in significant conflict. There are serious concerns about the potential for attacks against certain groups in a foreign country. One purpose of the arrangement is to prevent the entry of war criminals into Canada through the refugee or immigration process. The Service has established a limited arrangement for the purpose of immigration and visa vetting, and the agreement will be reviewed after a relatively short time. CSIS will not request information on prospective immigrants or refugees currently living in that country. Serious reservations have been expressed in Canadian government circles about the reliability of the organization. We will routinely “monitor the provision of information and intelligence pursuant to those arrangements.”²

(b) Exchanges of Information with Foreign and Domestic Agencies

(i) Foreign Exchanges of Information

The Service operates Security Liaison Officer (SLO) posts overseas that are responsible for liaising with the police, security and intelligence agencies in a large number of countries. Consequently, the authorities in the host countries are aware of the presence of the CSIS SLOs, a necessary precondition for cooperation.

SIRC has a mandate to review CSIS’ cooperation with foreign agencies under subparagraph 38 (a)(iii) of the *CSIS Act*. Each year, the Review Committee examines the activities of one or two SLO posts. In fiscal year 1995-96, we began the major task of auditing most of CSIS’ posts abroad. We are proceeding in stages and, for this Annual Report, we discuss our findings concerning two CSIS foreign posts in a large and economically important region.

The two posts we reviewed are located in an area of great economic interest to Canada. One issue facing the Service, is what level of representation is required in the region. Since 1990, the Service has closed most of the SLO posts in the area and moved most of the liaison responsibilities to one of the two remaining posts in that region. We found that the distribution of responsibilities between the two posts was unbalanced. One post liaised with twenty-four foreign agencies, while the second post covered only five. CSIS informed us that it intends to redistribute responsibilities between the two posts in order to produce a more balanced workload. We will review the Service’s progress in this area.

² Section 38(a)(iii) of the *CSIS Act*.

The Committee reviewed all of the correspondence that CSIS exchanged during 1994-95 with the foreign agencies covered by the two posts. We conducted the examination of the material with several key questions in mind:

- ▶ were the disclosures to foreign agencies properly authorized?
- ▶ did the disclosures comply with the conditions of the arrangements that CSIS has with the foreign agencies?
- ▶ were the requests for information from the foreign agencies justified under the Service's mandate?
- ▶ did CSIS consider the potential end-use of the Service's information, particularly regarding Canadians?

We found that the information exchanged at the two posts was, in general, balanced and accurate. We raised one concern, however, about a direct exchange between a foreign agency and CSIS Headquarters. In that exchange, CSIS provided information to a foreign agency about the family members of a person who was of interest to the Service. Furthermore, the information that CSIS gave to the foreign agency appeared to violate a restriction on the types of data being provided to services in the foreign country. In another exchange, one that involved open information, we concluded that the Service was justified in releasing the material to a foreign agency in a different country.

One of the SLO posts that we reviewed exchanged little information with the foreign agencies in the host country. A significant factor here was that the foreign agencies did not provide the information that CSIS requested from them. Some of the mutual difficulties arose from the language barrier. The Committee agrees with the Service's 1995 decision that all SLOs sent to this post should undergo extensive language training.

We believe that SLOs should be fluent in the language and the customs of the host country.

As part of the accountability and management process, all Security Liaison Officers are to send CSIS Headquarters an annual assessment of the foreign agencies with which the Service cooperates. These Agency Assessments are intended to ensure that CSIS HQ has current information, including those factors that could affect Service decisions on whether to disseminate information to the foreign agencies.

The Committee was not satisfied with the Agency Assessments prepared at one post. We found that:

-
-
- ▶ the assessment for one agency did not refer to vital CSIS information that cast doubt on the reliability of the agency;
 - ▶ many of the assessments contained little current information; and
 - ▶ some assessments failed to comment on factors influencing the dissemination of information, such as the human rights situation in the country and the protection of CSIS information.

One of the posts dealt with the foreign agencies in a country undergoing significant political changes. The political developments there had implications for CSIS' cooperation with the main security agency. We noted the discussions within CSIS concerning the impact of the changes on both the security of Service information and the reliability of the foreign service. As the country is a major source of immigration to Canada, we expressed our concern about the lack of effective immigration vetting for that country. The Service is satisfied that the arrangements currently in place at this location effectively meet its obligations with respect to immigration vetting.

Nonetheless, this and other similar issues will be dealt with in the forthcoming SIRC review of immigration screening.

(c) Warrants and Warrant Statistics

Warrant powers enable the Service to collect information not accessible by other investigative means. As a result, warrant powers also tend to be very intrusive. Section 21 of the *CSIS Act* allows the Service to submit an application for warrants to the Federal Court. The Service may request such powers as the interception of communications, the opening of mail, and the acquisition of financial information.

The Service provides us with basic statistics concerning the number of new warrants and renewed warrants in a fiscal year. Table 1 below, compares the number of new and renewed/replaced warrants in three consecutive fiscal years.

Table 1
New and Renewed Warrants

	1993-94	1994-95	1995-96
New Warrants Granted	85	85	32
Warrants Renewed/Replaced	103	130	180
Total	188	215	212

According to the Service, the number of warrants is levelling off. For the first time since 1991, the number of new warrants has decreased significantly. CSIS states that the decrease is the result of the Service's "more rigorous" approach to warrant acquisitions. Warrants are acquired only as a last resort when other methods of investigation might not succeed.

The warrant statistics are, by their nature, misleading. They do not reflect how many persons are being affected by CSIS warrant powers. For example, a single warrant can involve many individuals. As well, an increase in the number of warrants does not always mean an increase in the number of individuals affected by the warrant powers.

CSIS did not request any warrant powers in new areas of investigation in fiscal year 1995-96; all "new warrants" are in established areas of CSIS investigation. The number of individuals affected by CSIS warrant powers remains approximately constant. Foreign Nationals continue to constitute the majority of individuals subject to warrant powers. The number of Canadians and Landed Immigrants affected has not increased.

There were no regulations issued in fiscal year 1995-96 pursuant to section 28 of the *CSIS Act*. This section of the *Act* allows the Governor in Council to issue regulations concerning the forms of warrants that may be issued, the procedures, practices, and security requirements for hearing warrant applications, and the places where hearings may be held.

Warrants can contain one or more conditions specified by a Federal Court Judge. These conditions are generic and use standardized wording. The Service must follow the conditions in the execution of the warrant powers. In 1995-96, there were no new conditions, or revisions made to existing conditions in the warrants.

There have been no recent court decisions that have substantially affected the authorization or execution of warrants.

(d) Counter Terrorism (CT) Branch

The Service's Counter Terrorism Program is the major player in the battle to provide early warning to the government about individuals and groups that threaten the use of, or support the use of, serious violence to achieve their political goals. The CT Branch describes its program as striving to maintain the capability to provide timely forewarning of emerging threats and to provide accurate advice with respect to evolving security intelligence requirements.

For 1995-96, we were informed that there were no significant changes to the Counter Terrorism Program. The situation was not static, however, in that the Service internally reviews the functions and investigations in the CT Branch in the light of the budget reductions arising from the government-wide fiscal restraint program.

We noted that the CT Branch has placed increased emphasis on the coordination function for the collection and authorized disclosure of foreign intelligence pursuant to sections 16(1) and 19(2) of the *CSIS Act*.

In past years, we have remarked on the research documents or functional analyses issued by the Briefing Unit in the CT Branch. We had commented that these analyses were quite useful in that they allowed CSIS analysts an opportunity to stand back after an important operation and prepare a detailed, often technical, analysis of an important operation that took place in Canada or overseas.

We note with regret that the 1995-96 Counter Terrorism Program no longer requires the preparation of Functional Analysis Studies. We believe that both CSIS and SIRC benefitted from the insights in these retrospective analyses.

(i) Threat Assessments

CSIS employs threat assessments to warn Federal Government departments and agencies about imminent and potential threats to national security. In fiscal year 1995-96, the Threat Assessment Unit in the CT Branch produced 602 threat assessments. A comparison with the two previous years, 691 in 1994-95, and 843 in 1993-94, reveals a decline in the threat assessment numbers.

The Service was unable to point to any specific reason for the reduction. CSIS did note, however, that the production of these documents is governed by the "threat environment", and the varying requirements of the Service's clients.

(e) Counter Intelligence (CI) Branch

The CI Branch continues to focus on traditional espionage threats, but has had to respond to a changing international environment. Externally, CSIS encourages relationships with former adversaries; domestically, the CI Branch promotes positive relationships with Federal departments and agencies. Internally, the CI Branch responds to the changing environment by developing a smaller, but more focused organizational structure.

In 1995-96, the CI Branch set up a Transnational Criminal Activity Unit. According to CSIS, “the Service recognized the threat posed by the ‘transnational’ nature of organized crime and its connection to hostile intelligence services.” The CI Branch’s primary role in the transnational crime area is to provide “timely strategic intelligence” concerning the threat to government consumers and policy-makers, and specific “incidental/tactical criminal information” to Canadian law enforcement authorities. Investigation of transnational crime is linked to the development of relationships with former Warsaw Pact adversaries.

(f) Analysis and Production Branch

Few changes took place during 1995-96 in the Analysis and Production Branch (RAP). The Branch is comprised of two general areas, and its mission is to advise government decision-makers about important issues. Its advice is based on the evaluation of publicly available, as well as classified, information. The Strategic Analysis Unit is responsible for developing “comprehensive, policy-relevant intelligence assessments, covering a wide range of vital Canadian interests and future policies.”³ The second area deals with operational analysis and combines “tactically assessed intelligence with information from other sources, including government agencies and other intelligence services. The result is a finished evaluation which lends context to and weighs the significance of the original raw information.”⁴

In 1995-96, the Branch made a modest change by adding an operational analyst with expertise in transnational crime and information warfare to the Strategic Analysis Unit.

(i) Security Intelligence Reports

The Analysis and Production Branch produces a range of reports, studies, and briefs to aid government decision-makers. In fiscal year 1995-96, Branch staff were responsible for spearheading the preparation of six reports that were disseminated by the Intelligence Advisory Committee of the Privy Council Office. One of these reports dealt with the global terrorism situation and two others focused attention on states that have been plagued by terrorist incidents.

³ Canadian Security Intelligence Service. 1994 Public Report and Program Outlook. Ministry of Supply and Services, 1995.

⁴ *Ibid.*

The remaining reports assessed political developments in a state that has been historically hostile to Canada.

During 1995-96, the Branch published 57 CSIS Intelligence Briefs, the majority of which assessed the potential for terrorist activities emanating from foreign states. The studies also reviewed the threat to national security posed by groups in Canada.

(ii) Review of RAP Reports

The Committee does not read and critique all RAP reports in any given year. Rather, we assess those reports that are relevant to the reviews that we undertake in that year, and that would add to our knowledge in these specific areas.

In 1995-96, we reviewed the RAP products associated with the investigation of a foreign intelligence agency's activities in Canada. We were satisfied that the studies produced by RAP were consistent with the information and intelligence amassed during the investigation of the agency.

During our reviews, we have frequently observed that foreign agencies have complimented CSIS about the RAP reports and, indeed, have sought more of them. We will undertake a comprehensive review of RAP reports in the future.

(g) File Management

In our 1994-95 Annual Report, we described the end of the almost seven year odyssey during which the Service reviewed and disposed of the approximately one-half million files that it had inherited from the RCMP Security Service. During fiscal year 1995-96, the CSIS team that conducted the review of the inherited files, the National Archives Requirements Unit (NARU), turned to routine functions.

When we first received the file statistics for 1995-96, we noticed several anomalies in the data and we requested explanations from the Service. CSIS responded that our query had revealed errors in the file count; that discovery prompted an extensive review of the file holdings. The Service found that at the end of their review of the files inherited from the RCMP, errors were made when the file data was transferred to a new automated system. CSIS has implemented a more rigorous monitoring procedure to prevent a recurrence of the problem.

All files held by CSIS are subject to approved retention and disposal schedules. That is, when a file becomes inactive, a clock starts ticking and, after a predetermined period, the file must be reviewed for disposition. NARU decides whether to retain the file, destroy it, or add it to the National Archives' holdings.

For the year under review, NARU examined over 115,000 files whose retention periods were about to expire. As a result of the reviews, ninety-seven percent (97%) of the files were destroyed, almost three percent (3%) were retained, and just over one half of one percent (.6%) were released to the National Archives, based on their historical value.

In contrasting the file statistics for 1994-95 and 1995-96, we observed some interesting developments. We emphasize that a decrease in the number of files does not necessarily presage a reduced threat to national security. It may instead reflect changes in memberships or affiliation, or the Service's concentration on the most dangerous elements in various movements.

A similar caveat applies to the opening of more files on possible threats to national security. Here, the scope may be wider due to the changing nature of the threat or where higher demands for security screening are placed on the government. We noted:

- ▶ that there were no changes from the last fiscal year in the number of files pertaining to operational exchanges between the Service, federal and provincial institutions, and law enforcement agencies;
- ▶ an increase in the files concerning destabilizing technologies. The change represents a reorganization of the files by specifying the type of technology, such as weapons of mass destruction; and,
- ▶ major increases in the number of files on screening, particularly in the categories of citizenship, foreign checks and immigration, though refugee screening files decreased.

(h) Foreign Intelligence

Each year, the Committee examines CSIS assistance to the Departments of National Defence and Foreign Affairs for the collection of foreign intelligence; that is, information concerning foreign states and persons. We review the number of requests, and conduct an annual audit. In the annual audit, we examine requests from Ministers for CSIS assistance, the retention of information by CSIS from section 16 investigations and, specifically, the retention of information concerning Canadian persons or companies. In addition, we scrutinise the retention by CSIS of intelligence provided by Communications Security Establishment (CSE), and any cooperation between CSIS and CSE in the collection of information.

This year, we noted no dramatic increase in the number of approved section 16 operations, though there has been a significant growth over the last few years. The annual audit for fiscal 1995-96 began in June of this year, and will not be finalized until October 1996. We will be reporting on that audit in next year's Annual Report.

(i) Statistics on Operational Activities

Under section 38(a)(vii) of the *CSIS Act*, the Committee is to “compile and analyse statistics on the operational activities of the Service.” We retain and update a small computerized data base of various types of statistics. This includes such areas as warrants, targets, security screenings, person-year usage, and various financial matters. We analyse the statistics using multi-year comparisons, and breakdowns by operational region, Intelligence Requirement, and other categories. We seek an explanation from CSIS about any significant change revealed by the statistical analyses.

The statistics compiled are used in our studies. In the planning stage of reports, representative samples are selected for audits using the section 38 database. In the reports themselves, the statistics provide an evaluation of the extent of resource-use against specific targets. Thus, we can assess whether the extent of an investigation is justified by the severity of the threat posed by a group or individual.

Last year, we mentioned an agreement with CSIS for the provision of information on the number of people subject to investigation, by targeted group. This data had been included in *CSIS Annual Reports* predating 1992-93 to the Minister. CSIS has now begun publishing classified information on authorized investigations in two charts: a listing of authorized investigations by levels, but with no reference to targets, and a listing of authorizations by Intelligence Requirements (in general the targeted group), but with no indication of investigative level. We will move to a procedure whereby we will receive the detailed information on which the charts are based. This data will be more useful for our review function.

A few years ago, the Service’s CI area stopped publishing composite statistics on known and suspected intelligence officers in Canada. Individual desks in CSIS now retain statistics for their own use. In our view, these statistics provided a useful measure of the threat posed to national security by various hostile intelligence services.

We recommend that CSIS begin publishing statistics again on a regular basis.

4. Security Screening

In the course of performing screening enquiries, the Service's investigators come into daily contact with the public, thus making the Security Screening Program the Service's most visible function.

The Service's security screening activities fall under sections 13, 14, and 15 of the *CSIS Act*, supplemented by Ministerial Direction and Service policy. The Service may conduct such investigations as are required for the purpose of providing security assessments to departments of the government, and security advice to the responsible Minister in the area of citizenship and immigration.

This year, the Minister issued a Ministerial Direction to the Director on security screening and assessments, and, in conformity with subsection 6(2) of the *CSIS Act*, we received a copy. This Direction identifies the prevailing Government Security Policy (GSP) as the minimum standard required of the Service, and sets out general principles and guidelines to govern the provision of security assessments. It states that security assessments should be timely, accurate, and complete. Where there are reasonable grounds to doubt the loyalty or reliability of an individual, the concerned person should be given an opportunity to resolve such doubts. It also emphasizes that it is of paramount concern that the Service ensure the accuracy of the information contained in security assessments.

We noted that the Ministerial Direction leaves the collection, reporting, handling, and separate retention of information pursuant to security assessments, to be governed in accordance with approved Service operational policies and procedures.

(a) Government Security Screening

Upon request by a government department or agency, the Service conducts screening investigations in order to provide security assessments for these employees of the Public Service who require a security clearance, except those employed by the Department of National Defence (DND), and the Royal Canadian Mounted Police (RCMP). These two agencies conduct their own field investigations. Security assessments are also provided for persons in the private sector under contract to government institutions.

A security assessment is required in all instances where a person's duties require access to classified information or assets.

The *CSIS Act* defines a security assessment as an appraisal of an individual's loyalty to Canada and, insofar as it relates thereto, the reliability of that individual. Therefore, a clear causal relationship between loyalty and reliability must be seen to exist before reliability becomes a concern of the Service.

For the year under review, CSIS processed a total of 56,886 government security assessments. The time required to process government screening Levels 1 (confidential), 2 (secret), and 3 (top secret) were: one, forty-two, and one hundred and thirteen days respectively. For the 1994-95 fiscal year, the Service provided 39 information briefs⁵ and three rejection briefs to its clients.

The Government Security Policy and the Ministerial Directive on the provision of security assessments establish the “evidentiary standards, tests, and rejection criteria” by which a person can be denied a security clearance. Upon completion of its screening investigations, the Service provides not only information but also an assessment of the individual’s loyalty to Canada, and a clear recommendation to the requesting department advising whether the clearance should be granted.

(i) Application of the “normally ten year rule”

A decision to grant or deny a security clearance must be based upon adequate information in terms of both quantity and quality covering the last five continuous years (or to age 16) for restricted site access, or the last ten continuous years (or to age 16) for all three levels of security clearances. In the majority of the Canadian Human Rights referrals we have had to investigate over the years, we commented on the fact that, in our opinion, there was sufficient flexibility under the “ten year rule” to allow applicants with less than 10 years of Canadian residence to provide alternative means of verification, such as personal interviews or the provision of references. We concluded these cases with a recommendation that “departments apply the government security policy in a flexible and humane manner, bearing in mind the intent and purpose of the policy relating to protecting security.” Therefore, we were pleased that in late August 1995, Treasury Board issued a security policy implementation notice to all security coordinators indicating that the number of years for background coverage should be considered flexible, with the emphasis being placed on adequate quantity and quality of information. The policy also reminded them of the assistance the Service could provide in evaluating security assessment information.

(ii) Incomplete Assessments

Under the revised GSP, when the Service is unable to obtain sufficient information to renew a security assessment, an “incomplete assessment” is issued to the department. In these cases, and in keeping with the fact that the authority to revoke or to deny a security clearance remains with Deputy Heads, the department is responsible for determining if there are any security concerns and for making the final decision with respect to the clearance renewal. If the department has any

⁵ The Service defines an information brief as “a detailed assessment outlining the threat or potential threat to national security posed by individuals in the areas of government security screening pursuant to the Government Security Policy.” The information contained in such a brief addresses the loyalty to Canada and, as it relates thereto, the reliability of an individual, or any relevant matter uncovered during verifications and investigations.

security concerns, the Service can be further consulted.

The majority of “incomplete assessments” last year were provided to four principal departments or agencies: Transport Canada, Foreign Affairs and International Trade (DFAIT), Canadian International Development Agency (CIDA), and Citizenship and Immigration Canada (C & IC).

Almost all Transport Canada’s “incomplete assessments” are in the site access program of the Airport Restricted Area Access Clearance Program (ARAACP). Under this program, the Service conducts background checks for only the past five years. Out-of-country security and police checks are not conducted under the ARAACP. In cases where the individual has lived in Canada for the past five years, CSIS is able to obtain adequate information to make a security assessment in almost every case. Where an individual has not resided in Canada for the full period and because the five year period is a minimum period on which to base a security assessment, an “incomplete assessment” is returned to the department.

The “incomplete assessments” that CSIS issues to the other three departments, DFAIT, CIDA and C & IC are predominantly security clearance updates on personnel who are serving, or have served, abroad for most or all of the past five years. The GSP requires that CSIS conduct indices checks and out-of-country checks, when an applicant has resided outside Canada. Security and police checks with foreign agencies are not conducted on Canadian personnel as part of the update process, because it would be inappropriate to request a foreign agency to investigate a Canadian. CSIS indices checks are conducted but these checks rarely indicate anything, because the individual was living abroad. Under the revised GSP, subject interviews, which are the responsibility of individual departments, are recommended for Level 3 updates in such circumstances, and are mandatory for Signals Intelligence (SIGINT) access.

(b) Immigration Screening

With the acceptance of the concept of risk management in the processing of security checks on possible immigrants, the Service’s role focuses on those applicants who, on the basis of analysis and experience, are most likely to present a security risk. The advice provided by the Service assists the Department of Citizenship and Immigration in determining whether prospective immigrants are inadmissible persons under the *Immigration Act*. In the coming year we will devote considerable research resources to the Service’s role in immigrant security screening and the degree to which it cooperates with other agencies in the assessment of potential immigrants. Various posts abroad will be visited to provide the most accurate possible basis for this study.

In 1995-96, the Service received 51,010 applications from the department of Citizenship and Immigration. Of these, 2,769 were applications for citizenship, 9,585 were under the Refugee Determination Program (RDP ongoing), and 129 requests were under the RDP backlog program.

The Service's average processing time for such requests is 62 days; fifty-one percent of all cases were completed within this time frame. The remaining forty-nine percent of requests averaged 110 days to complete. Less than one percent of all cases took longer than twelve months as compared to a little more than one percent of all cases in 1994-95. In the Fall of 1995, the Service's screening branch introduced a greater degree of automation which should be reflected in next year's processing times.

(c) Citizenship Screening

The Department of Citizenship and Immigration Canada maintains a registry, called the Security Flag System, with the names and biographical data of permanent residents about whom the Service has identified security concerns. This registry triggers an in-depth review by the Service at the time of an individual's application for citizenship. Of the cases so far referred to the Service for such an in-depth investigation, very few are still unresolved.

(d) Screening on behalf of Foreign Agencies

The Service, with the approval of the Solicitor General who must, in turn, consult the Minister of Foreign Affairs, may enter into an arrangement with the government of a foreign state, a foreign agency, or an international organization, to provide security assessments.

In this fiscal year, the Service processed 779 such requests by foreign agencies. Of these, 179 required a field investigation, resulting in 19 detailed information briefs.

5. Complaints

As an independent investigatory agency established under the *Canadian Security Intelligence Service Act*⁶, we conduct investigations into the activities of the Canadian Security Intelligence Service (the “Service”) (section 41 of the *CSIS Act*), into denials of security clearances (section 42 of the *CSIS Act*) and render reports under the *Immigration Act*⁷, the *Citizenship Act*⁸ and the *Canadian Human Rights Act*⁹.

(a) Statistics

During the 1995-96 fiscal year, we received 29 new complaints, one Ministerial report and one referral from the Canadian Human Rights Commission.

Table 2
Complaints (1 April 1995 to 31 March 1996)

	New Complaints	Carried Over from 1994-95	Closed in 1995-96	Carried to 1996-97
CSIS Activities	29	4	30	3
Security Clearances	0	0	0	0
Immigration	1	0	0	1
Citizenship	1	0	0	1
Human Rights	1	0	1	0

(b) Complaints Against the Service's Activities

(i) Prerequisite to the Committee's Jurisdiction

Any person may make a complaint to the Committee with respect to “any act or thing” done by the Service and we must investigate such a complaint as long as we are satisfied that it is

⁶ R.S.C. 1985, c. C-23.

⁷ R.S.C. 1985, c. I-2.

⁸ R.S.C. 1985, c. C-29.

⁹ R.S.C. 1985, c. H-6.

not trivial, frivolous, vexatious or made in bad faith, and that the complainant has first submitted his or her complaint to the Director of CSIS.

If, after having submitted the complaint to the Director, the complainant is not satisfied by the Director's response, or if there has not been a response within a reasonable period of time, the complainant can bring the matter to our attention for an independent review.

We are precluded from investigating a complaint in respect of which the complainant is entitled to seek redress by means of a grievance procedure established either pursuant to the *CSIS Act* or the *Public Service Staff Relations Act*. For the year under review, we declined to investigate four such complaints from ex-employees of the Service.

(ii) Examples of Complaints Against the Service

Is CSIS bugging you?

As in previous years, we received fourteen complaints from individuals who believed that: they were the subject of undue surveillance, the Service had provided negative comments to their employers, their mail or telephone was censored, or that the Service had performed medical experiments on them by implanting a device. In such cases, we usually neither confirm nor deny that a person is a target. However, we thoroughly investigate the allegations to ensure that the Service has not used and is not using its powers unreasonably. After having ascertained that the Service is performing its duties and functions effectively, efficiently, and legally, we try to convey that assurance to the complainant.

How long is too long?

For the year under scrutiny, we received 9 complaints with respect to the Service's activities in providing security assessments and/or advice to the Minister of Citizenship and Immigration Canada (C & IC). In accordance with section 15 of the *CSIS Act*, the Service may conduct such investigations as are required for the purpose of providing security assessments to the Minister as to whether an applicant for permanent residence is a member of an inadmissible class of persons under section 19 of the *Immigration Act*. The actual decision to grant or refuse an application rests with the Minister.

In the first of these investigations, we dealt with an application that had been sent to the Service in the Fall of 1990. Though it was a complex case and the Service needed considerable time to ensure that it provided complete and accurate advice to C & IC, we concluded that taking 46 months to process an application was unacceptable and that the complaint was justified. There was an undue administrative delay in the Service's handling of the case that was not reasonable in the circumstances.

In other cases dealing with applications arising before 1992, we concluded that the overall administrative system for processing security screening applications within the Service was inefficient. The Service acknowledged that, for the period between 1989 and 1991, it was faced with a physical environment of inadequate resources and technology while dealing with an increasing level of work. We sought and received the Service's assurance that these inadequacies were corrected. In 1992, the Service introduced new measures which have enabled it to deal with applications in a more timely fashion.

In one instance, our investigation revealed that the complexity of the case was increased by a lack of forthrightness on the applicant's part. In light of the fact that the Committee was not in a position to comment on the six months period it took to schedule an interview, since this is always done by C & IC, and because we found that the Service had completed its enquiries and reported its conclusions to the department of C & IC within a month, we concluded that the complaint was not justified. The Committee also found that it was good policy for the Service not to proceed with the applicant's partner's application in light of the concerns identified in the main application. There was an administrative delay in the Service's handling of the two applications but that delay was justified by the seriousness of the concerns identified and the lack of forthrightness on the part of the applicant.

In another instance, we were in a position to confirm that, in the midst of our investigation, the Service's advice was sent to C & IC. We informed the complainant of that development. Nevertheless, the complainant asked us to pursue our review of the time taken by the Service to process the application for permanent residence status. We will be reviewing and commenting on that issue.

Press Allegations

We investigated the concerns raised by a Member of Parliament regarding the alleged investigations by CSIS of a medical doctor and a businessperson because of their relationships with Cuba, and their travels to that country. The Service can interview individuals to solicit information, views, and opinions, in order to become better informed on issues within the investigative mandate of the Service. Without infringing on privacy considerations we can indicate that we determined that the concerned individuals were not targets of the Service and that the Service should have given them specific assurances in that regard.

Allegations of bias on the part of the Service

We investigated a complaint regarding the Service's activities in the conduct of a security screening enquiry and its ensuing recommendation to a government department.

In summary, the complainant had indicated that the conduct of the Service's investigator had revealed bias. The complainant said that the reasons for the security screening investigation were not provided, nor had he been informed that allegations had been made against him, and that

damaging letters had been sent to the department where he worked. He also complained that he had not been provided with a copy of the final report or even an opportunity to review it.

Concerning the investigator's reports, we found that the information could have been reported in a more professional manner by distinguishing clearly between what was actually said by the source of the information, and the investigator's own comments. The investigator's use of generalizations and subjective characterizations may have presented a more negative view of the complainant than the actual information from the sources warranted.

According to the GSP, a critical function of the Subject Interview is to allow the subject to respond to the allegations against him or her. We concluded that the complainant had not been given such an opportunity and that the investigator's failure to confront the complainant with the allegations should have been noted in his report.

However, the process by which an investigator's report is reviewed and processed before the Service reaches a final conclusion provides some allowance for an investigator's potential bias. Furthermore, the actual Subject Interview Report is not sent, as a matter of practice, to the Government department. We confirmed that it had not been sent in this particular case. The Service's final recommendation to the Government department was much more temperate than the investigator's observations.

Beyond the complaint itself, we were greatly disturbed by the department's restricting the complainant's access to information to a level lower than the level specified by the complainant's security clearance, without formally revoking that security clearance. A course of action that, if it became widespread, could seriously undermine both the integrity of the security clearance process and the integrity of the review mechanism established by Parliament in the *CSIS Act*.

An Alleged Spy

In our Annual Report for 1993-94, we reported on a case heard by the Chairman of the Committee. The case received considerable publicity this year.

The case dealt with a complaint received from an ex-contractual employee of the Service who had been involved in the security screening investigation of another Service employee. According to the complainant, the security screening investigation had revealed problems that had not been addressed, and he questioned the impartiality and objectivity of a senior employee of the Service, whose intervention had had the effect of terminating the investigation.

Section 41 of the *CSIS Act* provides for an investigation by the Committee where a complaint has been received from “any person with respect to any act or thing done by the Service.”

Because the complainant was an ex-contractual employee, the complaint involved the disclosure of sensitive information that had come to his knowledge in the course of his duties and functions as an employee of the Service. An important consideration was the protection of personal information concerning the Service employee who was the subject of the security screening investigation. We were also conscious of the fact that the case could come back to the Committee as a section 42 complaint in the event that the case was re-opened.

After hearing evidence from all of the parties concerned, we had serious reservations about the Service’s security screening investigation in this case. Some important matters had not been adequately resolved.

We recommended that:

- ▶ the security screening investigation of that particular employee be re-opened and that several specific concerns mentioned be re-addressed;
- ▶ the employee be re-interviewed by objective and experienced interviewers with a view to resolving any remaining concerns; and,
- ▶ where possible, interviewers be selected who do not know the individual concerned.

We are satisfied with the actions taken by the Service.

(c) Security Clearance Complaints

Section 42 of the *CSIS Act* provides a right of complaint to the Committee for individuals who have been denied employment, or have been dismissed, demoted or transferred because of the denial of a security clearance.

We did not receive any complaints under this section this year.

(d) Ministerial Reports by the Minister of Citizenship and Immigration Canada and the Solicitor General

Citizenship Refusal¹⁰

The Minister of Citizenship and Immigration Canada may make a report to the Committee when the Minister is of the opinion that a person should not be granted citizenship because there are reasonable grounds to believe that the person will engage in an activity that constitutes a threat to the security of Canada, or that is part of a pattern of criminal activity involved in the commission of an offense punishable by way of indictment.

We received one Ministerial report pursuant to this section this year, but our jurisdiction was successfully challenged in the Federal Court. We comment upon this case in Chapter 1.

Deportation Order¹¹

We did not receive any Ministerial Reports under this section this year.

(e) Canadian Human Rights Commission Referral¹²

When, at any stage after the filing of a complaint and prior to the commencement of a hearing before a Human Rights Tribunal, the Commission receives written notice from a Minister of the Crown that the practice to which the complaint relates was based on considerations relating to the security of Canada, the Commission may refer the matter to the Review Committee.

For the year under review, the Commission referred one case to us.

After examining the circumstances of the case, the Committee concluded that the practice about which the individual complained was not related to matters affecting the national security of Canada. The Committee nevertheless offered to act as a facilitator in the unlikely event that information requested by the Commission, or information necessary for the Service to respond to the allegations of the Complainant, involved the disclosure of sensitive and classified information.

¹⁰ See the *Citizenship Act* (s.19.1 onward).

¹¹ See the *Immigration Act* (s.30 onward).

¹² See section 45. (1) of the *Canadian Human Rights Act*.

6. Regional Audits

(a) General

To obtain a field-level perspective on how well the Service's systems are working, we audit the investigative activities in one region of Canada each year. During 1995-96 for example, we reviewed targeting approvals, surveillance, sensitive operations and, for the first time, community relations in a region. The Service's operations took place in fiscal year 1994-95.

The information we collect through these regional audits allows us to see how CSIS operations have evolved since the last audit in a wide range of areas. The impact of new Ministerial Direction and new operational policies, for example, can be ascertained through this regional audit process.

(b) Targeting

During each regional audit, we review the Service's performance of its primary mandate: the investigations authorized pursuant to sections 2 and 12 of the *CSIS Act*. The Committee randomly selected 11 investigations conducted by the Region: five from the CI Branch and six from the CT Branch.

In each case that we examined, the Committee attempted to answer four questions:

- ▶ did CSIS have reasonable grounds to suspect a threat to national security?
- ▶ was the level of investigation proportionate to the seriousness and imminence of the threat?
- ▶ was the investigation authorized in accordance with the Service's internal rules and the directives in force?
- ▶ did the Service collect only the information that was strictly necessary in order to advise the Government about threats to national security?

(i) The Counter Intelligence Investigations

The first case concerned a person who CSIS suspected of cooperating with a foreign intelligence service. We found that the targeting proposal was weak in demonstrating reasonable grounds to suspect that the individual posed a threat to national security. The Service told SIRC that the targeting documents did not mention that a foreign intelligence officer was seen using clandestine techniques prior to meeting with the target.

An internal memorandum from CSIS' Legal Services stated that there were no reasonable grounds to believe or suspect that the person posed a threat to the security of Canada. The Service added

that the legal opinion was a comment on the “viability of obtaining a warrant” and that the case did not meet the threshold needed to obtain a warrant pursuant to section 21 of the *CSIS Act*. Moreover, the Service noted that Legal Services would not have recommended that it proceed with other investigative techniques if it believed that the investigation was not justified. The Service terminated the investigation in the Fall of 1995.

We agreed with the initial targeting decision and also supported the decision to terminate the investigation.

In the course of this investigation, the Service collected personal financial information without a warrant from a private institution. The Service stated that provincial legislation allowed the disclosure of such information in the absence of a warrant. In other provinces, a warrant is necessary to obtain the information. Our research confirmed that the legislation in the province does give the Service access to personal financial information without a warrant.

In the same investigation, we noticed that some operational reports did not identify the information source. This procedure makes it difficult, if not impossible from an audit perspective, for both SIRC and CSIS to identify and assess the source of the information. The regional investigators interpreted the new operational practices as preventing the identification of casual contacts, even if these contacts did not object to being identified. The Committee believes that it is essential that both the Service and SIRC be able to identify all information sources.

The second case involved a person suspected of supervising the overseas operations of a foreign intelligence service. According to the targeting authorization, the individual travelled frequently to Canada and other countries, had contacts with known intelligence officers, and seemed to be in a position of authority over the diplomats of his country.

We noted that the Region obtained information about the individual from a private institution in the absence of a warrant. The Committee questioned the Service about the collection effort and we concluded that the information met the test of “strictly necessary.” The Service informed SIRC that it had acquired a legal opinion on the matter to the effect that there was no requirement for a warrant in this situation. Based on the specific facts in this case, we agreed.

The third case also pertained to a foreign intelligence service. Whereas we had no difficulty with the Service’s targeting of the long-term adversary, the Committee did find that the 1994 targeting document provided little information about the extent of the foreign intelligence service’s activities in Canada.

In the opinion of the Committee, the remaining two cases posed no problems with regard to either the decisions to investigate or the information that the Service collected.

(ii) The Counter Terrorism Investigations

The first CT Branch investigation involved a purported plot to overthrow a foreign government. An emergency targeting authorization was obtained and the decision was later ratified by TARC.

We reviewed the content of the targeting request submitted to TARC and we found that some aspects of the request did not accurately reflect the information collected. For instance, the request stated that the principal conspirators were apparently influential individuals. The Committee learned that a representative from a federal agency told CSIS that the alleged principal conspirators were not influential in their community, and that they did not necessarily have the resources to carry out the threat. The Service informed SIRC that it did not agree with the agency's assessment.

Moreover, on the day that TARC met to approve the request, the Region sent Headquarters a preliminary assessment that cast doubt on the plot theory. The regional assessment was not provided to TARC. The Service said that the Regional report was preliminary and was not consistent with other reports. We informed CSIS that CT Branch should have drawn TARC's attention to the conclusions of the regional assessment.

Notwithstanding these concerns, the Committee supported the investigation. The volatile political and social situation in the foreign country justified the Service's interest in the possible conspiracy.

The second investigation focused on the activities of a young adult involved in a domestic extremist group. The Region learned that the person was the leader of the group and the Service increased the level of the investigation. We observed that the Region subsequently informed CSIS Headquarters that the target was no longer the leader and, indeed, that the group had disbanded. The Service did not actively investigate the person during the last few months of the specific authorization against him, and then terminated the investigation.

In the course of the investigation, CSIS learned that the target might have been involved in an attempted firebombing. The Service did not find information to show that the target was in fact involved in this criminal matter.

In the remaining four cases, we found that the decisions to investigate were appropriate and that the Region collected only the information that was strictly necessary for the purpose of the investigation. We also noted that the Region was particularly alert to and complied with CSIS policies concerning sensitive institutions in these investigations.

(c) **Sensitive Operations**

Sensitive operations are subject to the requirements set out in Ministerial Direction and the CSIS *Operational Policy Manual*, and must be approved by senior CSIS managers or the Solicitor General. These operations might touch on “sensitive institutions” such as churches or universities. We examine the Service’s decisions each year to determine if they are “strictly necessary” and whether they comply with policy.

For 1995-96, we noted that a source was directed to attend and collect information at a religious institution without the required approval of a senior manager. We found that no information was collected concerning religious matters. In another operation, we noted that an expenditure which, in the Committee’s view, required Headquarters approval had not been appropriately authorized.

CSIS documents revealed that a Federal Government official was asked to provide information to Service officers after, in the course of his duties, he had interviewed an individual. The Service told us that it could not explain the documentary reference. We found that the official did not provide the information to CSIS.

We reviewed a number of other operations approved pursuant to Ministerial Direction and the Service’s *Operational Policy Manual* during the fiscal year. We saw no problems in the approvals, or in the subsequent operations. We found, however, that there was no central file listing all the decisions concerning activities that could touch upon lawful advocacy, protest or dissent. Consequently, these decisions, scattered in numerous operational files, might not be seen during periodic audits.

We recommended to CSIS that records of senior management decisions regarding activities touching upon lawful advocacy, protest or dissent be retained on a central file.

(d) **Surveillance**

CSIS uses surveillance to provide details on the behaviour patterns, associations, movements, and “trade-craft” of groups or individuals targeted for investigation. Large amounts of personal information can be gathered and stored in the course of surveillance operations.

We examined all of the applications in the Region for the use of surveillance during a six month period. We observed that the majority of requests came from the CT Branch and we found no anomalies or problems with the applications.

Emergency surveillance is used “when an unanticipated threat to the security of Canada is suspected.” In these cases, the TARC authorization for the investigation is sought after the

fact. We intended to examine the use of emergency surveillance, but we found that the Region had never used this surveillance provision.

We found few issues in the surveillance operations that we randomly selected for detailed audit. All of the operations were clearly justified, with individual targets linked either to terrorist groups or to hostile intelligence services. We questioned the Service about:

- ▶ the collection of significant amounts of incidental information on individuals in the vicinity of targets;
- ▶ the retention by surveillants of working files containing personal information about the targets; and
- ▶ the use of cameras in the context of a “reasonable expectation of privacy.”

We were satisfied with the Service’s responses.

One surveillance report revealed that the Service intended to collect information on a person’s movements and contacts. The person in question, however, was not an authorized target and thus, surveillance could only be properly used for identification purposes. CSIS attributed the reference to faulty report writing, and we found no indication that information on the individual’s movements and contacts had been collected.

(e) Community Interviews

We have previously reported on the interview programs that CSIS has conducted in ethnic communities. The Committee examined, for example, the first Service-wide community interview program that took place among the Arab community during the Gulf War. Our 1991-92 Annual Report observed that whereas the program was carried out in a lawful manner, it nevertheless elicited fear and controversy in the ethnic community.

We returned to the issue again in our 1993-94 Annual Report. At that time, we found that CSIS had instituted several Community Interview Programs. We concluded that the Service had learned a great deal from its actions during the Gulf War and, in the main, did not repeat the mistakes of the earlier program.

We believe that the potential impact of CSIS on ethnic communities is extremely important. As we noted in 1993-94, “some emigré communities have lived through disagreeable experiences with security services in their homelands. In most of these communities, a knock

on the door from a local security service can impact massively and adversely on the individual.”¹³

The Service employs community interview programs to a significant extent, as a consequence of overseas “homelands” conflicts. Consequently, we concluded that we should establish an ongoing review of such programs. We have, therefore, incorporated the review of Community Interview Programs into our regional audits.

Community Interview Programs are duly authorized investigations and are used to sensitize ethnic communities to the Service and allow CSIS, in turn, to collect information on the potential for threats to national security. The voluntary cooperation of interviewees is sought by the Service.

When SIRC began the current review, we learned that the Region had also developed a unique and ongoing liaison program with ethnic communities, designed to be completely separate from the section 12 community interviews. We examined both the Community Interview Program and the Ethnic Communities Liaison Program in this study, as they involved the relations between the Service and the ethnic communities in the Region.

For the two types of programs, we sought to ascertain their scope, whether the programs were properly authorized, whether information from the community interview program was collected and retained on a strictly necessary basis, and if the Region collected personal information on those interviewed. We also wanted to see how the Region isolated the information in the Ethnic Community Liaison Program from the operational sector.

Committee Researchers reviewed the Regional and CSIS Headquarters (HQ) correspondence concerning the community interviews and the ethnic community liaison programs. We interviewed the key Regional personnel and we received a community liaison presentation that significantly aided our understanding of the differences between the two programs.

During our review, we saw no Ministerial Direction to address the special concerns dealing with the possible impact on ethnic communities of Service investigations. But we were pleased to see that the Service’s operational policies were sensitive to the issues associated with investigating persons from countries where the security and police authorities had brutalized the civilian populations.

Our review of a January 1993 memorandum from the then Director General CT found that it provided guidelines for community interviews, though the definition was ambiguous.

¹³ 1993-94 SIRC Annual Report, p. 14.

We recommended, therefore, that the memorandum be more precise as to the definition of the program and that it either be included in the *Operational Policy Manual* or that it be updated and re-issued to all operational branches.

The Service informed us that our recommendation will be given full consideration, as CSIS was “reviewing other operational policies, changes to which may affect the policy governing community interviews.” We will monitor the Service’s activities in this regard.

For the period under review, fiscal year 1994-95, we learned that the Region had conducted a small number of community interview programs in the counter terrorism area. The Region had interviewed the leaders and knowledgeable members of the ethnic communities. The CI Branch informed us that it did not conduct any community interviews in the Region during this time.

We observed that even the few interviews in one ethnic community highlighted that group’s fear of people in Canada who were associated with overseas enemies. We saw no problems in the Service’s community interviews for the period under review. The interviews in another community were also conducted responsibly and we did not see any abuse of the process. We commented, however, on the occasional violations of the requirement to electronically track the information exchanged with other agencies.

The small number of community interviews in a third ethnic population were similarly not of concern. As in the previous interviews, it was evident that people in the ethnic communities were fearful of retribution by their homeland enemies. We noted too, that the Region conducted interviews in a fourth community, but CSIS did not consider these actions to comprise a Community Interview Program per se, and no special authorization was sought, although the general targeting authorization remained in force. The ambiguity associated with whether a special authorization was required, again pointed to a policy vacuum in this area.

In late 1992, Regional staff proposed an innovative Ethnic Communities Liaison Program as a means to approach ethnic communities, to complement the Service’s communications strategy, and to demonstrate the Service’s openness to multiculturalism. The proposal was inspired by CSIS’ first public report in 1991, the Osbaldeston Report, and SIRC’s recommendation that ethnic communities be sensitized to the role of CSIS in order to earn their respect and ease the unfounded fears in these communities.

One outcome of the program was the receipt of requests for assistance from the ethnic communities. Although the majority of these requests were not within the Service’s mandate, the contacts, said the Region, served to encourage a certain level of confidence in CSIS from the ethnic communities. These results could not completely dispel, however, the general fear in some ethnic communities concerning all intelligence services.

We concluded that the initiative taken by the Region in its Ethnic Community Liaison Program was impressive. The program was well-structured and the objectives were particularly praiseworthy in reaching out to the ethnic communities and focusing on multiculturalism issues for CSIS employees.

We found cases where there were strong links from the liaison to the operational sectors. When liaison officers met with a possible source, we were concerned that the line that separates the liaison program from its operational counterpart was breached. As well, one liaison interview appeared to blur the differences between liaison meetings and community interviews. The Service stated that the liaison staff were present solely to facilitate the meetings.

We noted that the community and liaison programs were duly authorized. As we stated earlier, we believe that clearer policy guidelines are required to better define community interviews.

We also concluded that the Region did not collect personal information on those interviewed for the liaison program. Further, the information from community interviews was amassed on a strictly necessary basis. Finally, we expressed some misgivings about the participation of liaison staff in meetings of an operational nature with members of ethnic communities.

7. Review of General Matters

(a) Ministerial Direction

Under subsection 6(2) of the *CSIS Act* the Solicitor General may issue direction to the Service. The Committee reviews all new directions issued, examines how well they work, and audits how well they are being followed. In 1995-96 we received three new Ministerial Directions.

“Security Screening and Assessments” is a consolidation of the general principles contained in the six previous directions on the subject, and was issued due to “changing circumstances” and the “significant operational resources dedicated by the Service to security screening.”

The “National Requirements for 1994-95” contains general direction from Cabinet as to how CSIS should focus its investigative efforts. In particular, CSIS is directed to pass to the RCMP all relevant intelligence received from foreign intelligence and security services dealing with international organized crime. CSIS is also cautioned to ensure that section 16 activities are not undertaken to the detriment of the Service’s primary mandate under section 12 of the *CSIS Act*. The “National Requirements for 1994-95” was issued to the Service in September 1995, six months after the end of the fiscal year. To avoid such gaps in the future, each issue of “National Requirements” will be valid for two years, though the document will still be updated annually as a general rule.

The “Management of Human Sources” tightens up certain aspects of human source direction. A new senior manager, the Assistant Director - Intelligence is to oversee operational support and will report to the Director. Other changes concern questionable source behaviour and “agent provocateur” activities.

In the *Heritage Front Affair* study, the Committee noted that “the level of policy guidance available to CSIS” in the human source area “is ... seriously deficient,” and that “Direction and Policy in this area should be re-examined.” We believe that the new direction on human source management is a step in the right direction but that some further clarification is still required.

(b) Changes in Instruction

The *CSIS Operational Policy Manual* contains policies which are based, in part, on the Service’s interpretation of Ministerial Direction. The *Operational Policy Manual* provides general guidance, principles, and a framework to enable CSIS officers to make decisions. In 1995-96 the Service produced six new policy instructions.

One outlines general principles, roles and responsibilities for the acquisition of warrants under part II of the *CSIS Act*. One covers cooperation with Canadian government institutions in the form of exchanges of information, joint operations, operational assistance and technical assistance. Another provides direction for section 16 operations, and includes approval procedures and the delineation of responsibilities. Two of them allocate duties and responsibilities with respect to Service transportation, and one covers CSIS involvement in

“Special Events.” The latter formalizes existing procedures followed by the Service in preparing for VIP visits and similar special events.

CSIS also produced four amendments to sections of the *CSIS Operational Policy Manual*. Three amendments concern the authorized disclosure of information, and focus on the protection of intelligence in light of Access to Information legislation. The other amendment deals with changes in human source use, and reflects in large part the new Ministerial Direction on source management.

All policies written by members of the RCMP Security Service (and predating 1984) have now been removed from, or revised in, the current *CSIS Operational Policy Manual*.

(c) Disclosures in the Public Interest

Under section 19(2)(d) of the *CSIS Act*, the Solicitor General can direct the Service to disclose information to government officials or Ministers when the public interest outweighs any invasion of privacy that might result. We are to be notified of such disclosures. We received no such notifications in 1995-96.

Section 19 of the *CSIS Act* prohibits the Service from disclosing operational information, except in certain circumstances. It does not address disclosure by the Solicitor General. The Service may make disclosures outside of the Government of Canada when warranted by “the national interest.” The Service does so on the authority of the Solicitor General, and acting as his agent. There were no “special disclosures” made in 1995-96.

(d) Regulations

Under section 8(4) of the *CSIS Act*, the Governor in Council may make regulations concerning appointments and other personnel matters. No such regulations were issued in 1995-96.

(e) Report of the Director and Certificate of the Inspector General

Under section 33 of the *CSIS Act*, CSIS must provide the Minister with an annual report on the Service’s “operational activities.” The Inspector General is to review the Annual Report, and to provide a Certificate indicating whether any operational activities in the period reviewed by the Annual Report contravened the *Act* or Ministerial Direction, or involved an “unreasonable or unnecessary exercise by the Service of any of its powers.” We are to review both the Annual Report and the Certificate.

In general, we receive both too late for inclusion in our current Annual Report. This results in our commenting on them in the following year's report.

According to the 1994-95 *CSIS Annual Report*, public safety remains the Service's principal concern. The Director indicates that, in the fight against terrorism, CSIS has achieved success against persons who support terrorist causes or perpetrate terrorist acts by helping the government deny them sanctuary and the use of Canada as a base of operations. In the area of economic security, CSIS believes that investigations have reaffirmed that foreign interests are using clandestine, deceptive, coercive or illegal methods to acquire information and technology of economic value. Also, counter-intelligence investigations have revealed a link between a number of foreign intelligence services and international organized crime.

The 1994-95 *CSIS Annual Report* provides a useful overview of all investigations. The Report contains much relevant statistical information; however, the way some of the numbers are aggregated occasionally undermines their value. In addition, the Report does not contain any significant discussion of the problems and challenges facing CSIS.

The Certificate of the Inspector General was not issued when we finalized our current annual report. We were informed by the Inspector General that, as a basis for the upcoming certificate, he has examined aspects of CSIS targeting practices under section 12 of the *Act*, the conduct of joint operations with various allied agencies, the accuracy of affidavits prepared by the Service in support of selected warrant applications, as well as other issues related to CSIS' observance of Ministerial directions and its own operational policy.

(f) Reports of the Inspector General

Under section 40 of the *CSIS Act*, SIRC can ask the Inspector General to formally conduct a study. Last year, we made no formal requests for assistance, but staff did meet frequently to discuss work and to coordinate research.

In 1995-96, the Inspector General himself issued one report. The report, "CSIS Handling of Confidential Sources", was discussed in last year's annual report. The Inspector General may, from time to time, issue special studies, but the Certificate is his primary reporting vehicle.

(g) Unlawful Conduct

Under section 20(2) of the *CSIS Act*, the Director is to submit a report to the Minister on any employee who has "acted unlawfully in the purported performance of the duties and functions of the Service." The Minister is to forward the report, with comments, to the Attorney General of Canada for possible prosecution. Under section 20(4) of the *CSIS Act*, we are provided with a copy of "anything given to the Attorney General of Canada."

In fiscal 1995-96, as in 1994-95, we received no notifications concerning illegal activities. As part of our database, we retain a record of all the section 20 cases received by SIRC, and the disposition of those cases. As of 31 March 1996, we had received copies of a total of 13 referrals to the Attorney General. No action has been undertaken by the Attorney General against CSIS employees pursuant to those referrals. In two cases, the Service dismissed employees. As of 31 March 1996, there were no cases pending before the Attorney General of Canada.

(h) SIRC Consultations and Inquiries

(i) Formal Inquiries

In our review function, not counting inquiries arising out of complaints, we directed 148 formal inquiries to the Service in the 1995-96 fiscal year (1 April 1995 to 31 March 1996). The average time CSIS took to answer a formal inquiry was 53 days, a significant increase from last year's average of 40 days.

We were told that the increase was caused by temporary problems within the Service. The Committee does not believe that the numbers are indicative of a trend.

(ii) Briefings

We continued with our regular meetings with the Director of CSIS during fiscal year 1995-96. These meetings are over and above the constant contact that our staff maintains with the Service.

We regularly visit the regional offices of the Service so as to keep current with their particular operations and problems. This year we met with Officials from CSIS Regional Headquarters in Toronto, Vancouver, Montréal, and Halifax.

We also met with the Solicitor General of Canada, the Honourable Herb Gray, P.C., M.P., and the Commissioner of the RCMP, Mr. J.P.R. Murray.

(iii) Beyond CSIS

Visiting dignitaries from other countries often ask to meet Members of the Review Committee. In 1995-96 we met with the British Intelligence and Security (Oversight) Committee; and, the Joint Standing Committee on Intelligence of the Parliament of South Africa.

(i) 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 1995-96, we submitted the following study to the Minister under section 54 of the *CSIS Act*:

- ▶ *An Ongoing Counter-Intelligence Investigation*, May 1995 (TOP SECRET) (CI 93-07)

A list of all SIRC studies can be found in Appendix B of this report.

8. Inside CSIS

(a) Recruitment

There were two Intelligence Officer (IO) Entry Training Classes held during the 1995-96 fiscal year, with a total of 32 participants. Four of the trainees were conversions from other positions within the Service.

The female to male recruitment ratio was 10 females to 22 males, down from last year's ratio of 13 females to 11 males.

All students met the bilingualism criteria by acquiring level BBB in reading, writing, and oral conversation, and all successfully completed the Entry Training Course.

In the IO category, the percentage of female employees dropped slightly from the previous year: from 24.5 percent to 23.7 percent.

In the senior management level, the percentage of men increased slightly from 87.3 to 90.5 percent; women represented 9.5 percent of Senior Management, down from 12.7 percent last year. The Committee hopes that the decrease in female representation is not indicative of a trend.

The representation of visible minorities within Senior Management remains at 1.3 percent. A satisfactory explanation has not been given as to why there has been no progress in this area for so long. We will continue to press for better balanced representation in every area of the Service's operations.

(b) Finances

Each year, we receive a summary of CSIS expenditures, which includes a breakdown of spending by Standard Object (standard government accounting categories) and a separate breakdown for covert expenditures, covering such items as source expenditures. We examine these against historical data, and question the Director on any significant variations.

Table 3 shows expenditures for the last six years.

Table 3
Actual Expenditures (\$000)

	Personnel	Other Expenditures	Capital	Total
1991-92	120,956	69,200	15,294	205,450
1992-93	124,926	72,591	27,833	225,350
1993-94	118,819	77,282	48,190	244,291
1994-95	115,579	71,715	18,381	205,675
1995-96	110,723	69,048	4,383	184,154
1996-97 ¹⁴	102,801	62,753	0	165,554

“Other Expenditures” includes some expenses under “Construction and Acquisition of Land, Buildings and Works” and “Machinery and Equipment”, but does not include expenditures for the new CSIS Headquarters building which are included under “Capital”.

CSIS expenditures have decreased because of the completion of the new Headquarters Building and staff cutbacks. In 1995-96, CSIS received \$2 million in supplementary funding for the Early Departure Incentive Program. The Service’s spending on computers and software remains strong, but funding for one significant engineering and development area is being reduced.

This year, we received information on covert expenditures in a different format than in prior years, in part due to the reclassification of some items. We will evaluate whether additional information is needed for future financial reviews.

¹⁴ Main Estimates.

9. Inside SIRC

(a) Accounting to Parliament

On 16 October 1995, the Solicitor General tabled the Committee's 1994-95 Annual Report.

The Committee appeared before the Sub-Committee on National Security on 15 May 1996 to answer questions about its 1995-96 Main Estimates.

(b) Staying in Touch

In the past, the Committee has made extensive use of seminars to obtain invaluable advice from outside experts. Since September 1992, when SIRC held its last seminar in Montréal, budget constraints continue to limit our ability to hold any further seminars. Efforts are being made to seek more cost-effective means of maintaining these links within the reality of a limited budget.

(c) Impact of Budget Changes

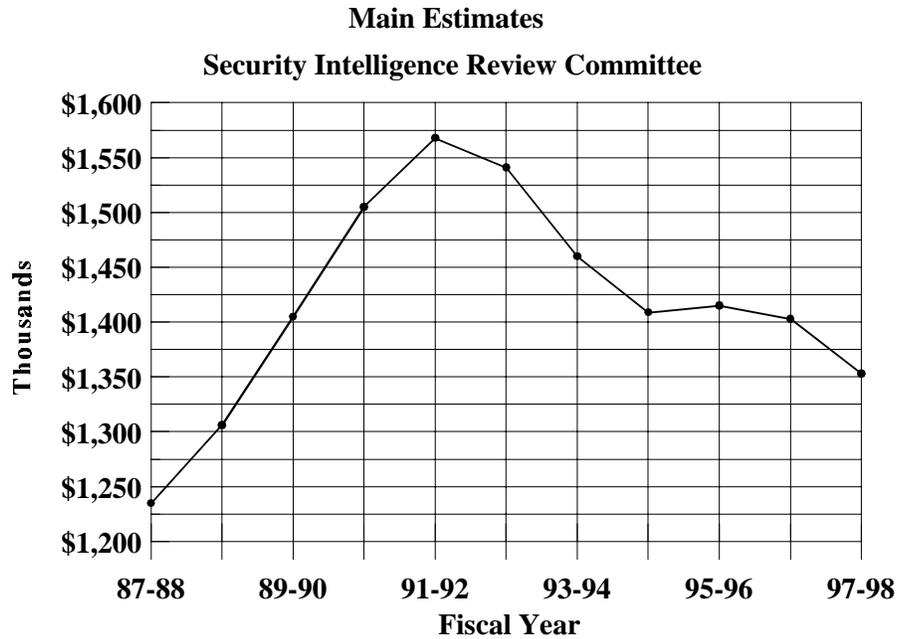
The Committee's budget has been declining since fiscal 1991-92, and although the cuts have not been large in absolute terms, they are significant for a small organization with little budget flexibility. The following graph understates the degree to which the Committee's budget has been reduced because translation services (\$50,000) which used to be provided off-budget are now included in SIRC's Main Estimates.

Table 4
SIRC Budget 1995-96

	1995-96	1994-95
Personnel	799,000	807,000
Good and Services	616,000	602,000
Total Operating Expenses	1,415,000	1,409,000

Source: 1995-96 Estimates, Part III, Section II, Figure 7

Figure 1



The investigation of complaints is the most expensive area of operation for the Committee, and must, therefore, bear the brunt of the budget cuts. To deal with the reductions, this year again the Committee is doing more work “in house”, and using outside lawyers less. More pre-hearing meetings are being conducted by Committee staff to better focus the issues to be dealt with in hearings. While undertaking such measures, the Committee is determined to avoid increasing the time required to handle complaints, and to maintain the quality of its investigations.

The review area is also being affected by budget reductions. As with Complaints, more work is being done “in house”, and the Committee is no longer using contract Research consultants.

Through automation, the Committee has been able to reduce some costs over the last few years. It has installed personal computers and a local area network. This has resulted in a cutback of secretarial staff from three persons to two, and has reduced the time required to prepare and release documents. Automation has also allowed more effective tracking of correspondence, classified records, and the Committee's budget.

The Committee is also taking some measures to reduce general administrative costs. In past years, the Committee used an outside Editor to assist in the preparation of the Annual Report. This year again, the Executive Director and the Executive Assistant will share the task. The Committee is no longer hosting seminars and conferences. Rather, it is dealing with more experts and opinion-makers on a one-to-one basis at, for example, Committee meetings. The Committee is developing an Internet web site. Through this venue, a wider public will have access to SIRC's publications, and in so doing, reduce printing and mailing costs.

The Committee believes that the steps outlined above, together with a continuing effort to improve efficiency, will allow SIRC to maintain or improve the performance of its responsibilities to Parliament and the public at lower cost.

(d) Personnel

The Committee has a small staff of 14 in total: an Executive Director; a Senior Complaints Officer to handle complaints and ministerial reports; a Director of Research Counter Terrorism; a Director of Research Counter Intelligence; and four Research Officers; an Executive Assistant who coordinates activities on behalf of the Chairman, conducts all media liaison, coordinates the production of the Annual Report, and undertakes research projects; an Administrative Officer who is also the Committee registrar for hearings, and undertakes research projects; and an administrative support staff of four. There is a particular burden on the Committee's administrative support because the material handled by the Committee is sensitive and highly classified, and must be dealt with using special security procedures.

At its monthly meetings, the Committee decides about the research and other activities it wishes to pursue, and sets priorities for the staff. Day-to-day operations are handled by the Executive Director with direction, where necessary, from the Chairman in his role as the Chief Executive Officer of the organization.

A. Glossary

ARAACP	-	Airport Restricted Area Access Clearance Program
C & IC	-	Department of Citizenship & Immigration
CI	-	Counter Intelligence
CIDA	-	Canadian International Development Agency
COMMITTEE	-	Security Intelligence Review Committee (SIRC)
CSE	-	Communications Security Establishment
CSIS	-	Canadian Security Intelligence Service
CT	-	Counter Terrorism
DFAIT	-	Department of Foreign Affairs & International Trade
DIRECTOR	-	the Director of CSIS
GSP	-	Government Security Policy
HQ	-	Headquarters
IO	-	Intelligence Officer
MINISTER	-	the Solicitor General of Canada, unless otherwise stated
MOU	-	Memorandum of Understanding
NARU	-	National Archives Requirements Unit
NHQ	-	CSIS National Headquarters
RAP	-	Analysis and Production Branch
RDP	-	Refugee Determination Program
SERVICE	-	Canadian Security Intelligence Service (CSIS)
SIGINT	-	Signals Intelligence
SIRC	-	Security Intelligence Review Committee

SLO - Security Liaison Officer
TARC - Target Approval and Review Committee

B. SIRC Reports and Studies Since 1984

(Section 54 reports — special reports the Committee makes to the Minister — are indicated with an *)

Eighteen Months After Separation: An Assessment of CSIS' Approach to Staffing Training and Related Issues, April 14, 1986 (139 pages/SECRET) * (86/87-01)

Report on a Review of Security Screening for Applicants and Employees of the Federal Public Service, May 1986 (SECRET) * (86/87-02)

The Security and Intelligence Network in the Government of Canada: A Description, January 1987 (61 pages/SECRET) * (86/87-03)

Closing the Gaps: Official Languages and Staff Relations in the CSIS, June 1987 (60 pages/UNCLASSIFIED) * (86/87-04)

Ottawa Airport Security Alert, February 1987 (SECRET) * (86/87-05)

Report to the Solicitor General of Canada Concerning CSIS' Performance of its Functions, May 1987 (SECRET) * (87/88-01)

Counter-Subversion: SIRC Staff Report, August 1987 (350 pages/SECRET) (87/88-02)

SIRC Report on Immigration Screening, January 1988 (32 pages/SECRET) * (87/88-03)

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) * (87/88-04)

The Intelligence Assessment Branch: A SIRC Review of the Production Process, September 1988 (80 pages/SECRET) * (88/89-01)

SIRC Review of the Counter-Terrorism Program in the CSIS, November 1988 (300 pages/ TOP SECRET) * (88/89-02)

Supplement to the Committee's Report on Immigration Screening of January 18, 1988, 15 November 1989 (SECRET) * (89/90-01)

Report to the Solicitor General of Canada on Protecting Scientific and Technological Assets in Canada: The Role of CSIS, April 1989 (40 pages/SECRET) * (89/90-02)

SIRC Report on CSIS Activities Regarding the Canadian Peace Movement, June 1989 (540 pages/SECRET) * (89/90-03)

A Review of CSIS Policy and Practices Relating to Unauthorized Disclosure of Classified

Information, August 1989 (SECRET) (89/90-04)

Report to the Solicitor General of Canada on Citizenship/Third Party Information, September 1989 (SECRET) * (89/90-05)

Amending the CSIS Act: Proposals for the Special Committee of the House of Commons, September 1989 (UNCLASSIFIED) (89/90-06)

SIRC Report on the Innu Interview and the Native Extremism Investigation, November 1989 (SECRET) * (89/90-07)

A Review of the Counter-Intelligence Program in the CSIS, November 1989 (700 pages/ TOP SECRET) * (89/90-08)

Security Investigations on University Campuses, February 1991 (TOP SECRET) * (90/91-01)

Release of Information to Foreign Agencies, January 1991 (TOP SECRET) * (90/91-02)

Domestic Exchanges of Information, September 1990 (SECRET) * (90/91-03)

Regional Studies (six studies relating to one region), October 1990 (TOP SECRET) (90/91-04)

Investigations, Source Tasking and Information Reporting on 2(b) Targets, November 1990 (TOP SECRET) (90/91-05)

Section 2(d) Targets — A SIRC Study of the Counter-Subversion Branch Residue, September 1990 (SECRET) (90/91-06)

CSIS Activities Regarding Native Canadians — A SIRC Review, January 1991 (SECRET) * (90/91-07)

Report on Multiple Targeting, February 1991 (SECRET) (90/91-08)

Study of CSIS' Policy Branch, October 1990 (CONFIDENTIAL) (90/91-09)

Review of the Investigation of Bull, Space Research Corporation and Iraq, May 1991 (SECRET) (91/92-01)

Report on Al Mashat's Immigration to Canada, May 1991 (SECRET) * (91/92-02)

CSIS and the Association for New Canadians, October 1991 (SECRET) (91/92-03)

Exchange of Information and Intelligence between CSIS & CSE, Section 40 Study, October

1991 (TOP SECRET) * (91/92-04)

Victor Ostrovsky, October 1991 (TOP SECRET) (91/92-05)

Report on Two Iraqis — Ministerial Certificate Case, November 1991 (SECRET) (91/92-06)

Threat Assessments, Section 40 Study, January 1992 (SECRET) * (91/92-07)

East Bloc Investigations, August 1991 (TOP SECRET) (91/92-08)

Review of CSIS Activities Regarding Sensitive Institutions, August 1991 (TOP SECRET) (91/92-10)

A SIRC Review of CSIS' SLO Posts (London & Paris), September 1993 (SECRET) (91/92-11)

The Attack on the Iranian Embassy in Ottawa, May 1992 (TOP SECRET) * (92/93-01)

Domestic Terrorism Targets — A SIRC Review, July 92 (TOP SECRET) * (90/91-13)

Review of CSIS Investigation of a Latin American Illegal, November 92 (TOP SECRET) * (90/91-10)

CSIS Activities in regard to the Destruction of Air India Flight 182 on June 23, 1985 — A SIRC Review, November 92 (TOP SECRET) * (91/92-14)

Prairie Region — Report on Targeting Authorizations (Chapter 1), November 92 (TOP SECRET) * (90/91-11)

CSIS Activities during the Gulf War: Community Interviews, September 92 (SECRET) (90/91-12)

The Audit of Section 16 Investigations, September 92 (TOP SECRET) (91/92-18)

Prairie Region Audit, January 93 (TOP SECRET) (90/91-11)

“STUDYNT” The Second CSIS Internal Security Case, May 92 (TOP SECRET) (91/92-15)

The Assault on Dr. Hassan Al-Turabi, November 92 (SECRET) (92/93-07)

CSIS Activities with respect to Citizenship Security Screening, July 92 (SECRET) (91/92-12)

Domestic Exchanges of Information (A SIRC Review — 1991/92), November 92 (SECRET) (91/92-16)

Regional Audit, September 1993 (TOP SECRET)

Middle East Movements, December 1993 (SECRET)(CT 93-01)

Domestic Investigations (1), December 1993 (SECRET)(CT 93-02)

The Asian Homeland Conflict, September 1993 (SECRET) (CT 93-03)

Domestic Investigations (2), December 1993 (TOP SECRET) (CT 93-04)

A Review of CSIS' SLO Posts (1992-93), December 1993 (SECRET) (CT 93-05)

Sheik Rahman's Alleged Visit to Ottawa, May 1993 (SECRET) (CT 93-06)

The Proliferation Threat, December 1994 (SECRET) (CT 93-07)

A Review of CSIS' SLO Posts (1993-94), January 1995 (SECRET) (CT 93-09)

Potential for Political Violence in a Region, June 1995 (SECRET) (CT 93-10)

Community Interviews, March 1995 (SECRET) (CT 93-11)

Review of Traditional CI Threats, December 1993 (TOP SECRET) (CI 93-01)

Regional Audit, July 1994 (TOP SECRET) (CI 93-02)

Intelligence - Source Confidentiality, November 1993 (TOP SECRET) (CI 93-03)

Protecting Science, Technology and Economic Interests, December 1993 (SECRET) (CI 93-04)

Domestic Exchanges of Information, December 1993 (SECRET) (CI 93-05)

Foreign Intelligence Service for Canada, January 1994 (SECRET) (CI 93-06)

An Ongoing Counter-Intelligence Investigation, May 1995 (TOP SECRET) (CI 93-07)*

Domestic Exchanges of Information (A SIRC Review 1993-94), January 1995 (SECRET) (CI 93-08)

Sources in Government, June 1994 (TOP SECRET) (CI 93-09)

Regional Audit, October 1995 (TOP SECRET) (CI 93-10)

The Audit of Section 16 Investigations and Foreign Intelligence Reports, May 1994
(TOP SECRET) (CI 93-11)

The Heritage Front Affair. Report to the Solicitor General of Canada, December 1994
(SECRET) (CT 94-02)*

Terrorism and a Foreign Government, October 1995 (TOP SECRET) (CT 94-03)

The Proliferation Threat - Case Examination, January 1995 (SECRET) (CT 94-04)

The Audit of Section 16 Investigations and Foreign Intelligence Reports, February 1996
(TOP SECRET) (CI 94-01)

Review of Certain Foreign Intelligence Services, January 1996 (TOP SECRET) (CI 94-02)

Domestic Exchanges of Information (A SIRC Review 1994-95), February 1996 (SECRET)
(CI 94-03)

Visit of Boutros Boutros-Ghali to Canada, November 1995 (SECRET) (CI 94-04)

A SIRC Review of CSIS' SLO Posts (1994-95), September 1995 (SECRET) (CT 95-01)

CSIS and a "Walk-In", March 1996 (TOP SECRET) (CI 95-04)