



SECURITY INTELLIGENCE
REVIEW COMMITTEE

An Operational Audit of CSIS Activities

**Annual Report
1996 - 1997**

Canada

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

30 September 1997

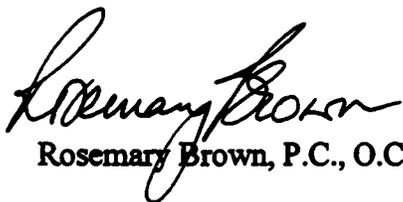
Dear Mr. Scott:

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 1996-97, for your submission to Parliament.

Yours sincerely,



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



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



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



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



James Andrews Grant, P.C., Q.C.

Introduction

This year's Annual Report is presented in a new format and its contents are organized so as to be accessible and readable. To reflect these changes and to more precisely describe the subject of the Report, the title now includes the phrase "An operational audit of CSIS activities." The revised Annual Report is but one of the initiatives undertaken by the Security Intelligence Review Committee in its continuing effort to meet a core strategic objective: to be the most trusted and widely used independent source of information about CSIS activities.

The Committee has set up a Web site¹ that includes its annual reports as well as a wealth of other information and relevant documents. A list of the Committee's classified reports is also available, and there are cross references to books, monographs, articles, and other Web sites that we believe would be worthwhile reading for those interested in security intelligence matters. The Web site, since its inception in October 1996, has already received over eighty-five thousand visits.

A third focus of the Committee's efforts is the ongoing professional working relationship with the Parliamentary Sub-Committee on National Security. The Chair and Members of the Review Committee will continue to make every effort to provide the Sub-Committee with the information it seeks, and to answer MP's questions as fully and forthrightly as

possible within the constraints of national security and without jeopardizing the safety of Canadians.

Finally, the Committee will place renewed emphasis on the practice of meeting academic experts and other well-informed individuals in every region of the country. Their views and assessments help guide Members' decisions when making judgements about complaints cases, Ministerial reports, or the appropriateness of particular CSIS activities. Clearly, the threat environment evolves and the circumstances of Canadians change; an action or policy appropriate at one time may no longer be acceptable. Only by staying in close touch with public and expert opinion can the Committee hope to make judgements that are consonant with prevailing standards.

The *CSIS Act*, though not flawless, established a governance structure for security intelligence matters that is being emulated in many other countries. Our senior officials are invited to describe Canada's system to the emerging democracies in Central and Eastern Europe, and foreign delegations visit Canada and the Committee for the same purpose. However, it sometimes seems that our accountability structure is less well-regarded here at home than it is abroad. The Committee hopes to change this perception by demonstrating to Canadians that it is fulfilling the role set out for it in the *CSIS Act* transparently and with considerable effectiveness. The Committee welcomes com-

... a core strategic objective: to be the most trusted and widely used independent source of information about CSIS activities

1. www.sirc-csars.gc.ca

ments on the format, utility, or any other aspect of its Annual Report or its Web site.

How SIRC's Annual Audit Report is Organized

Readers familiar with past SIRC annual reports will find all of the information presented in previous years. However, the material is presented in a new and, we believe, more functional format.

We have also attempted to make a clear differentiation between Committee comments, observations and recommendations bearing directly on our major task — reviewing CSIS and associated activities for a certain period of time — and the more general background material we are making available with the aim of assisting Canadians and other readers to understand the context in which security and intelligence work is carried on.

The latter category consists of shaded boxes set apart from the main text that address single topics the Committee believes will be of historical, background or technical interest to readers. Unlike the main body of the report, they do not reflect Committee opinion or conclusions as such and are intended to be strictly factual in nature.

In general, the report is organized to reflect the Committee's primary functions: first, to review CSIS intelligence activities, second, to investigate complaints about CSIS and associated matters, and third, to act in concert with other parts of the

governance system to protect Canada and Canadians from threats to security.

- **Section 1** presents the Committee's review and audit of what the Service does and how it does it. The subsections represent the different methods the Committee employs on an ongoing basis to make this assessment.
- **Section 2** deals with the Committee's role as a quasi-judicial tribunal with the power to investigate complaints of various kinds.
- **Section 3** brings together under a new heading — CSIS Accountability Structure — the Committee's review of the multiple administrative and legal mechanisms that hold the Service accountable to government, Parliament and the people of Canada.

The Review Committee will continue to make every effort to provide the Sub-Committee with the information it seeks

Section 1: A Review of CSIS Intelligence Activities

A. Areas of Special Interest for 1996-1997

Titled “Case Studies” in past reports, this part of the audit report presents the results of major research and analysis carried out by the Committee in the course of the year. As the new title implies, these inquiries are in addition to, and are intended to complement and reinforce, the other forms of audit research the Committee undertakes.

The Committee’s selection of topics to be the subject of in-depth inquiry (this year there are five) is influenced by a number of factors including *inter alia*, shifts in the nature of the international threat environment, changes in technology, the need to monitor or follow up on past Committee recommendations, significant alterations in Government policy which the Committee believes could have implications for Service activities, changes in organizational structure or operational emphasis within the Service itself, and the interests of individual Committee Members.

This year, the subjects of the Committee’s special interest are CSIS activities in the investigations of emerging threats, the Service’s foreign liaison program, the means

by which the Service manages human sources, CSIS efforts in addressing economic espionage, and the Service’s activities concerning a particular homeland conflict.

Investigations of Emerging Threats

Since the end of the Cold War, many states and intelligence services of former foes have undergone a major transition. We reviewed how CSIS investigated the new and emerging threats to Canada’s national security posed by the intelligence agencies of these states.

The Service’s investigations of these threats were launched at the beginning of the decade. CSIS obtained information from foreign intelligence agencies and interviewed Canadians with a knowledge of developments in the states concerned.

After several years of monitoring the situation, CSIS terminated most of the targeting authorizations against the foreign states, owing to the absence of evidence that they were conducting intelligence activities against Canada. The Service retained, however, a general authorization to cover new threats which might arise. We concluded that the CSIS investigations were entirely appropriate, given the rapidly changing political environment at the time.

Below, we present our conclusions about certain of CSIS activities in this area. In most of the investigations that we examined, the Service’s actions were prudent.

We concluded that the CSIS investigations were entirely appropriate, given the rapidly changing political environment at the time

... foreign intelligence services were attempting to reactivate sources in Canada ...

In one case, however, we saw contradictory information about the seriousness of the threat and the Service's actions appeared to be excessive.

A foreign intelligence service investigation of note

In the case of one foreign state, CSIS conducted an extensive investigation. The Service believed that the foreign intelligence services continued to target ethnic Canadians at home and abroad. Furthermore, a foreign agency clandestinely collected information in Canada, some of which was economic, and attempted to sway Canadian government policies.

The Committee examined the Requests for Targeting Authority for this investigation.²

The Requests hypothesized that the new intelligence services were:

- establishing intelligence missions abroad, including Canada;
- continuing the predecessor agencies' practice of attempting to manipulate ethnic communities; and
- "...engaged in intelligence collection activities including the targeting of Canadians in Canada and abroad."

In addition, we examined the documentation that described how the new intelligence services were continuing the practices of their predecessors.

In our view, the evidence of these activities was equivocal. For example, we observed that CSIS

seemed to place a negative interpretation on one activity which taken in context seemed to us to be relatively benign. We found that the reports CSIS provided to consumers in other parts of the government suggested that most of the alleged intelligence activities were innocuous. Finally, we took note of the fact that an intelligence service allied to Canada decided not to pursue investigations of the foreign intelligence services in question.

The Committee did encounter some evidence that the foreign intelligence services were attempting to reactivate sources in Canada used by the previous regime. The Service's focus, however, was not so much on the current activities of the foreign services, but rather on their preparations for future intelligence activities.

Other emerging threat investigations of note

We noted several issues of concern in the other investigations that we reviewed:

- A CSIS official pressed a foreign diplomat posted in Canada for information although the diplomat, who was suspected of being a foreign intelligence asset, had clearly changed his mind about speaking with the Service. To the Committee, the officer's persistence was questionable in the circumstances.
- CSIS officers placed into the Service's computer banks extensive accounts about the internal politics of some states. The information was received by CSIS on an unsolicited basis.

2. For more information about targeting authority, see inset on page 17.

- CSIS investigators repeatedly questioned one target. To us, the questioning appeared confrontational and out of proportion to the threat he posed.
- The Service provided adverse information about a person to two Federal Government departments and to an allied intelligence agency. We noted that the Service described the target as a “witting agent” of a foreign intelligence service, a potentially damaging statement not substantiated by the documentary evidence we saw. In addition, the authority to investigate him was not properly approved; it did not take into account his immigration status, as required by policy. CSIS later rectified the error.

CSIS Liaison Program with Foreign Agencies

SIRC’s reviews of the Service’s foreign liaison activities were conducted pursuant to section 38(a)(iii) of the *CSIS Act*.³ We reviewed the foreign liaison program in general, and the exchanges of information with foreign agencies at nine posts abroad in particular. The audits focused on the accountability procedures and controls in place, and examined whether CSIS had placed restrictions on the dissemination of certain types of information to foreign agencies. We also inquired into CSIS relations with foreign agencies as carried out by its Security Liaison Officers (SLOs) as well as the SLOs’ relations with Canadian Federal officials.

The reviews had several objectives:

- to ascertain the status of several issues that repeatedly arose in past reviews;
- to ensure that there was no excessive or unnecessary use of powers by the Service;
- to review the effectiveness of the Service’s tracking systems for information exchanges; and
- to learn if there were systemic problems that impacted on the Service’s foreign liaison program that had not already been identified.

Methodology of the current review

The Service operates Security Liaison Officer (SLO) posts overseas responsible for liaising with police, security and intelligence agencies in a large number of countries. The authorities in the host countries concerned are aware of the Service’s officers presence and functions, a necessary pre-condition for inter-agency cooperation.

In fiscal years 1995-96 and 1996-97, SIRC undertook a series of reviews of the CSIS SLO posts abroad. We conducted these audits as a result of our review of the documentation from one post in 1994-95.⁴ That study sought to audit the exchanges of information with other agencies conducted through the post solely from the documents available at CSIS Headquarters. The findings prompted concern that the numerous problems we found might be systemic in nature. We then undertook to review additional SLO posts.

... The audits focused on the accountability procedures and controls in place

3. “...to review arrangements entered into by the Service pursuant to subsections 13(2) and (3) and 17(1) [mandating CSIS to enter into arrangements with foreign powers, agencies and international organizations] and to monitor the provision of information and intelligence pursuant to those arrangements.”

4. SIRC *Annual Report* 1994-95, Chapter 4(ii), page 28.

The major focus of the reviews was to examine the documentation retained at CSIS Headquarters for nine SLO posts. On-site reviews at three of these posts were conducted to ascertain whether the material sampled at CSIS Headquarters from the same posts was representative of the information provided by the Service to foreign agencies. In addition, at CSIS Headquarters we examined the correspondence from six other posts. For purposes of comparison, we audited the information disclosures to foreign agencies for the same period of time.

To supplement this information, we interviewed Service staff at CSIS Headquarters and at selected posts, and we examined open information from other sources (human rights groups, for example). In addition, we conducted a special audit of “direct

exchanges” — information that CSIS provides to foreign agencies via telecommunications circuits — in order to determine if important information was bypassing the controls associated with the SLO posts.

Information exchanges with foreign agencies were examined with the following questions in mind:

- did they conform to the statutory guidelines for the retention, dissemination or receipt of the information?
- were they in conformity with the arrangements Canada entered into with the agency in question?
- was the information provided by CSIS to the foreign agency accurate and was the potential for damage to the person weighed against the importance of the investigation?

Background to the Service’s Foreign Liaison Program

From the inception of CSIS in July 1984, until 1989, CSIS had a Foreign Liaison Branch. In 1990, the Service replaced the Branch with a new system for communicating with and coordinating the efforts of the SLOs. At the time, SIRC expressed its concern about the disbanding of the Foreign Liaison Branch. The Committee regretted the loss of what it described as “An intermediary... [that could] ‘blow the whistle’ on the inappropriate dissemination of information abroad.”⁵

In its place, CSIS created a new unit under a Coordinator, to provide administration and support services to the SLOs. The Coordinator reported to one CSIS executive member, while the SLOs reported directly to another. The Foreign Liaison Advisors reported to their respective operational branches, and were to monitor the correspondence exchanges and ensure that the SLOs were informed about new developments.

In a previous Annual Report,⁶ we expressed concern about the number of SLO posts CSIS was closing and were of the opinion that, “the foreign liaison program would benefit from more attention from the Service, not less, as seems to be the trend in terms of representation overseas.”

For a number of years, there were few changes to the Service’s posts abroad, save for the post closings, but the mid-1990s saw a major reworking of the Service’s foreign liaison strategy. Decisions to open as well as close selected Security Liaison Officer posts resulted, as did changes to the management structure of the foreign liaison program as a whole.

In 1994-95, the reporting relationships and responsibilities changed for both the unit and the SLOs, as a result of an internal management study. Most notably, the overall management of the program was once again centralized under the direction of a senior manager. We understand that in 1997, to a certain extent, history will repeat itself. The foreign liaison program will be raised to Branch level once again, an initiative the Committee will report on in our next Annual Report.

5. A SIRC Review of CSIS’ SLO Posts (London & Paris), 12 January 1993.

6. SIRC 1993-94 Annual Report, page 26.

- were the control provisions, including recording methods, for the information provided by CSIS properly observed?

Results of the review: CSIS' organizational initiatives

In 1995, the first meeting of a new CSIS committee took place, the establishment of which arose from an internal CSIS program review. Chaired by the Chief of the foreign liaison program, the committee was established to serve as a coordinating and information sharing body between CSIS Headquarters' branches and the overseas posts. The purpose was also to provide strategic direction for the management of the Service's foreign liaison program. We believe the initiative is a positive one.

As well, the Committee regards the re-establishment of a Foreign Liaison Branch as a constructive decision. With the increasing interdependence of the global intelligence community, the liaison responsibilities of the foreign liaison program will also expand and a branch-level infrastructure will likely help the Service manage the increasing work load.

In previous SLO post reviews, we have commented on the adequacy of the Service's Procedures Manual for SLOs. In 1993, the Field and Liaison Unit at CSIS Headquarters published a Foreign Liaison Procedures Manual to replace an outdated manual. The new manual deals primarily with administrative matters and instructs SLOs to maintain a log of all incoming and outgoing correspondence on a specific form.

We noted that because of the relative isolation of the SLOs from CSIS Headquarters, the existence of a document containing basic procedures to assist them is more important than it would be for Canada-based CSIS staff. We observed that whereas in the 1980s, the Service provided the SLOs with a rather comprehensive body of instruction specifically for the posts, the "new" Procedures Manual is already out of date and contains only information on routine administrative procedures.

We recommend, therefore, that the Procedures Manual be brought up to date, and that it cover important post issues that are not addressed elsewhere.

The Service informed us that it concurs with the need to update the Procedures Manual on a priority basis.

In the course of the Committee's liaison post audits, we learned that the Chief of the foreign liaison program had conducted a management review of one SLO Post, and intended to conduct others where warranted. We regard this as a sensible initiative.

Results of the review: CSIS foreign communications tracking procedures

The Service's foreign liaison program must be able to respond to information demands from within the Service, as well as from domestic and foreign agencies. However, the Committee has in the past been critical of the Service about its unreliable system for

The Committee regards the re-establishment of a Foreign Liaison Branch as a constructive decision

The Committee has in the past been critical of the Service about its unreliable system for tracking the information it provides to foreign agencies

tracking the information it provides to foreign agencies. This problem, as well as others that arose due to communications deficiencies the Committee identified within the Service, were unresolved.

Logging and data tracking

In 1985, CSIS developed a form it said was intended “to assist SIRC in its duty under section 38(a)(iii) to ‘monitor the provision of information and intelligence pursuant to ... arrangements.’”

The written log that the Service implemented at that time was complicated and difficult to interpret, so in subsequent years, CSIS Headquarters sent out memoranda and telexes to help SLOs understand how to complete the form.

During the course of our SLO reviews, we repeatedly attempted to use the logs of information exchanges with foreign agencies created by SLO posts (and held at CSIS Headquarters). These attempts were thwarted by the difficulty in locating the documents at Headquarters referred to in the logs compiled at the posts. The only reliable way to find and examine the documents listed was to visit the SLO post itself.

In recent years, the Service introduced an electronic tracking system. SIRC staff have since attempted to check the data in the new system against the information in the logs so as to ensure that the audit samples were representative of the messages sent abroad. Our current audits establish conclusively that it is not possible to correlate the log and electronic tracking systems. In

commenting on these difficulties, the Service informed SIRC that “at least part of the problem is that the post logs contain more than just section 12 [intelligence] information. Cooperation and administration tasks are also recorded.”

Linked to this problem was a deficiency the Committee found in the Service’s system for reporting reliable statistics on the volume of information exchanges carried out by Security Liaison Officers.

Subsequently, and at the invitation of the Service, SIRC identified problems perceived to exist within the Service’s information recording and reporting system. Thus, beginning in late 1996, the Service implemented a new automated system for use at SLO Posts. The system is designed to streamline reporting procedures and address SIRC accountability requirements.

We appreciate the fact that the Committee’s input was requested and, at first glance, it appears that the Service has attempted to address our concerns in this area. Future audits will test the success of the new system.

Distinctions between exchanges of “open” and “classified” information

One of the recurring issues for SIRC in its review of CSIS information exchanges with foreign agencies, is the extent to which SLOs can provide open information to foreign agencies. We observed that the Service’s *Operational Policy Manual* makes no distinction between the treatment to be afforded open and classified information.

CSIS has made a distinction, however, between open information collected as part of a section 12 investigation, for example, and open information to which SLOs have access, but is not collected or retained as part of the “corporate record.”

For open information that is collected as part of an investigation, the Service’s position is that the same rules governing the disclosure of classified information to foreign agencies apply to open information collected and held on Service files under a section 12-mandated investigation. Open information which comes to the attention of SLOs via other means, however, such as newspapers, magazines, and the like, may be passed at the SLO’s discretion providing it meets the Service’s criteria for what is appropriate.

We were concerned about the impact of adverse open information that SLOs can release to foreign agencies. We noted one case where the provision of open information to a foreign agency triggered a foreign agency investigation.

The Committee has noted the efforts of the foreign liaison program to deal with our concerns regarding the provision of open information to foreign agencies. We consider it a positive move that the unit has attempted to achieve an understanding in this area.

We recommend, however, that when an SLO decides to disclose adverse open information about Canadians to a foreign agency, the

SLO be required to first consult with management at CSIS Headquarters.

Information exchanges not passing through SLO posts

Our reviews of “direct (telecommunications) exchanges” described the importance of direct links between the Service and several allies for Canadian security interests. For the period under review, we found that the SLOs were always notified when a direct exchange occurred; that all CSIS requests or responses were made under a valid authorization; and that the exchanges were captured in the Service’s electronic tracking system. We were satisfied with the Service’s use of the telecommunications links.

Results of the review: CSIS assessments of other agencies

Each year, SLOs provide CSIS Headquarters with assessments of the foreign agencies that cooperate with the Service for the purpose of aiding the operational branches to decide what should and should not be disseminated to these agencies. With the introduction of SLO ratings several years ago, SIRC had welcomed the Service’s initiative because it held out the prospect for better informing CSIS operational staff about the various factors that might influence decisions about such dissemination. Recent audits have given the Committee reason to reconsider its initial enthusiasm.

As noted above, the current series of SLO audits was prompted by an earlier SIRC evaluation where we saw that agency assessments were

We were concerned about the impact of adverse open information that SLOs can release to foreign agencies

Some SLO agency assessments did not contain information on human rights

of uneven quality and that the human rights situations in several countries were not adequately described. CSIS maintains that human rights considerations are taken into account.

For this latest series of reviews, we conducted an on-site audit at the same post that prompted the broader SLO review. We found that despite poor human rights situations and political instability generally in many of the countries in the region covered by the post – in addition to high levels of corruption in some cooperating agencies – these organizations continued to receive favourable SLO ratings.

Our survey of the foreign agency ratings procedures identified specific concerns:

Attributing the information source

The ratings are set by the SLOs on the basis of the information collected *en post*. The assessments represent the perceptions of the SLOs based upon their day-to-day dealings with the foreign agencies, what they read in the media and elsewhere, and information shared with SLOs by other staff at Canada's missions abroad.

It is the Committee's view that where the reliability ratings reflect the experience of other Government of Canada sources available to the SLO — Foreign Affairs or Immigration department staff, for example — and in the absence of sufficient information held by the SLO itself, agency assessments should attribute the ratings to the other parties.

Definitions of reliability

We believe the current operational definitions employed in the reliability

ratings system are ambiguous and thus open to a level of individual interpretation that reduces the system's effectiveness as an operational tool. With the emergence of the new democracies and with the expanding number of foreign arrangements, the need for a well-defined system of rating the reliability of the foreign agencies is essential.

We recommend that the Service revise, or at least better define, its system of evaluating the reliability of foreign agencies.

Agency assessments and human rights concerns

According to Ministerial Direction, CSIS must consider the human rights conditions in those countries with which it is considering sharing information. Our recent reviews have found, however, that some SLO agency assessments did not contain information on the human rights situations for countries where we would consider the discussion warranted.

Earlier SIRC audits in the current series indicated that references to human rights in assessments were only sporadic, notwithstanding the fact that human rights is an issue SLOs are obliged to comment on. In the aftermath of our earlier reports, agency assessments we saw did document the human rights situation in a number of countries, but there is room for improvement still. Current audits identified a number of assessments which failed to provide current information on recent important events and others that have not been updated for several years.

The Committee regards CSIS' agency assessment process as an opportunity that has yet to be fully exploited. We believe that this problem can be remedied by the Service, as evidenced by some of the most recent assessments.

Defining types of liaison

A principal Ministerial Direction to the Service sets out the various types and levels of liaison Canada has with foreign agencies. Cooperation with other agencies can range from routine immigration vetting all the way to personnel exchanges. In a number of SIRC studies conducted in the series examining foreign agency cooperation, we found that the decision as to which sort of activity falls under what liaison arrangement is subject to varying interpretation.

SIRC identified one exchange with a foreign agency which we considered to be inappropriate in light of existing Direction. CSIS had never asked the Solicitor General to approve this type of exchange with this particular foreign agency. CSIS did not agree with our interpretation, maintaining that the type of assistance rendered was in accordance with an existing, Minister-approved arrangement.

We also observed that the Service's definitions for the scope of arrangements appear in neither Ministerial Direction nor in CSIS policy documents. The Committee would like to see the Service provide clear definitions for the various exchange arrangements it manages.

On the policy front, a Ministerial Direction that pre-dates CSIS has outlived its usefulness in a number of areas. We hope that a new Ministerial Direction forthcoming will remove the ambiguity as regards the definitions of foreign arrangements.

Logging of oral directions and information exchanges

In two past reviews, we have noted that SLOs or staff at CSIS Headquarters sometimes failed to log certain kinds of oral exchanges, specifically conversations with persons in foreign agencies and important instructions relayed to the SLO by CSIS Headquarters personnel. We were also concerned about a statement to us by one SLO that there was no policy direction requiring that such oral exchanges be logged. The *CSIS Operational Policy Manual* clearly states otherwise. The Service notes that these incidents were isolated cases.

For the purpose of accountability, we believe that all meetings with foreign agencies where operational information is exchanged, whether orally or in writing, should be documented. All CSIS Headquarters personnel should document the instructions they provide to SLOs, regardless of the means of communication. The Committee is also of the view that Headquarters branches should remind staff of the existing requirement to document operational instructions conveyed orally to SLOs.

Our disagreement with CSIS in this area appears to focus on whether operational information has or has not been recorded. We have found some examples of where this was

The Committee would like to see the Service provide clear definitions for the various exchange arrangements it manages

unequivocally the case. We expect to find more in the future if the Service does not reiterate the existing policy to its employees in the ways suggested above.

Altering or transferring existing liaison arrangements

A long-standing Ministerial Direction requires CSIS to obtain the Minister's approval to establish a liaison arrangement or alter the scope of an existing one. However, SIRC found cases where the Service transferred agreements from one agency to another in the absence of Ministerial approval. CSIS had instead sought and obtained authorization from senior officials in the Ministry of the Solicitor General.

Where the transfer takes place because an agency undergoes a name change or has received expanded responsibilities, we do not object. Sometimes, however, the proposal is to transfer existing arrangements to a new agency with its own new mandate and personnel.

We believe that Ministerial approval, not just that of Ministry officials, is necessary to comply with the Direction when a liaison arrangement is to be transferred to another agency, regardless of whether the scope has changed.

Management of Human Sources

Human sources function at the direction of CSIS to collect and provide information to the Service. The rules which govern their management stem from Ministerial Direction and written CSIS policies. Following the events involving the Heritage Front in 1994, the Direction and the concomitant policies were amended. In the period following the dissemination of the new directions, the Committee wanted to see if the revisions to the rules had resolved the concerns we set out in our special report to the Solicitor General — *The Heritage Front Affair*.

CSIS Management of Human Sources and the Heritage Front Affair

In *The Heritage Front Affair*, the Committee wrote that a CSIS source was involved in a harassment campaign⁷ by white supremacists. The senior Service managers said that they had not been apprised of this activity, nor did they sanction it. The Committee concluded that CSIS policy and direction in the source management area was “seriously deficient.”⁸ SIRC accepted that sources could not merely be passive. The Committee said, however, that CSIS officials “should regularly stand back from day-to-day transactions to assess the operation in its totality;” that is, they should draw up a “balance sheet” of the benefits and dangers of a particular operation. While the Committee did not “advocate detailed rules that would unduly limit CSIS,” we did conclude the following:

We recommend, rather, Ministerial guidelines that require CSIS management to carefully weigh the benefits and the dangers of each human source operation on a regular basis; taking due account of the special circumstances of each case.⁹

On 1 August 1995, the Solicitor General issued a new Ministerial Direction to the Director of CSIS on human source use in response to the issues raised by the Committee in *The Heritage Front Affair*. The Ministerial Direction, and the subsequent policy changes expanded the controls on sources in three areas: *agent provocateur* activities, discreditable conduct activities, and activities touching upon sensitive institutions such as campuses, religious institutions or trade unions.

7. SIRC Report. *The Heritage Front Affair*, Report to the Solicitor General of Canada, Section 5, 9 December 1994, pp. 9-10.

8. *The Heritage Front Affair*, Section 13, p. 12.

9. *The Heritage Front Affair*, Section 13, p. 14.

We sought to examine all source operations that could influence targeted or non-targeted organizations or groups. We also sought out cases that involved *agent provocateurs* or disreputable conduct, and here we found no new ones. But we identified a number of cases where sources were involved with sensitive institutions; of these we audited several.

We concluded that the majority of the cases reviewed were in compliance with the revised Ministerial Direction and written policy. We believe that the operations were reasonable in terms of the intelligence they yielded: in a number of cases the potential for serious violence was very likely averted because of the information gained. Several operations involved considerable danger to the country had they not succeeded since the acquisition of weapons and explosives was at issue. In sum, SIRC believes the operations were justified and concludes that CSIS officials demonstrated adequate control over the actions of the sources.

We found problems in three cases:

The first operation involved a source who reported on a meeting that occurred in the course of collecting information about a target. CSIS managers told the source that they had no interest in the milieu where the meeting occurred, a context which involved legitimate dissent and protest. The Service's records, however, contain a detailed account of a meeting attended by the CSIS targets. Much of the reporting involved statements that stopped short of suggesting violence by persons who were not targets. In addition, the Service obtained informa-

tion about an imminent, non-violent demonstration, and subsequently disseminated the information to the police.

The second case involved a CSIS operation that, in the view of the Committee, posed a potential risk to a sensitive institution – namely, the free flow of ideas on a university campus. Intelligence suggested that there was a potential threat, and CSIS was of the opinion that the threat warranted the risk. The Service terminated the investigation.

The third case gave rise to questions concerning the origin of certain information CSIS collected. The source was a government official who in the normal course of work had access to sensitive personal information. The Service was interested in the source's knowledge about a particular community, not in information the source might have gained through work. CSIS managers did not, in our opinion, adequately document their instructions that the source was not to provide information acquired in this manner. When SIRC researchers came across information that appeared to come from the source's occupation, inquiries of the Service were made. We subsequently ascertained that the information was not improperly acquired.

SIRC will continue to monitor the Service's management of human sources.

Economic Espionage

At the time we last commented on CSIS' economic security effort in 1993, the program was new, and the state of knowledge about economic

We sought to examine all source operations that could influence targeted or non-targeted organizations or groups

espionage was limited. The program is now six years old and the Committee's review indicates that the main difficulty confronting the Service in this area is its own overly broad definition of what constitutes an economic threat.

The Service faces considerable obstacles to reasonably defining its role in dealing with economic threats to Canada. Economic espionage can target many sectors of Canada's economy, and the threats can emanate from foreign governments, agencies or individuals working on their behalf. It is often

very difficult to differentiate between the activities of private sector companies and those of governments.¹⁰ Nonetheless, a reassessment of the Service's definition of what constitutes an economic threat and how that definition is applied in its operations, is warranted.

What is an "economic threat"?

When we examined the Service's economic security investigations it was evident that CSIS' definition of economic security — which includes "information of economic significance" — transcends those

Background to CSIS Economic Security Program

The changing international threat environment of the post-Cold War world has pushed economics to the top of the national intelligence agendas of many countries, Canada not excluded. The Government of Canada has broadened its definition of national security to include the concept of "economic security" which CSIS defines as "the [set of] conditions necessary to sustain a competitive international position, provide productive employment, and contain inflation."

Reflecting these changes in the nature of the challenges to Canadian security, the Service initiated in June 1991 a comprehensive approach to two issues: "Economic Security" and the "Proliferation of Weapons of Mass Destruction." In order to coordinate the existing organizational sections within CSIS investigating these areas, the Service formed the Requirements Technology Transfer (RTT) Unit.

Economic Security and Proliferation Issues (ESPI) Unit

In October 1995, the Service restructured the RTT unit into what is now the Economic Security and Proliferation Issues (ESPI) Unit. ESPI's economic security mandate is to investigate "the clandestine acquisition or transfer, by foreign governments, of proprietary/classified technology and information valuable to Canada's economic interests."

Liaison/Awareness Program

One of ESPI's primary means of carrying out its responsibilities is through the Liaison/Awareness Program. Under this program, ESPI meets with members of the business, government, academic, and scientific sectors in order to raise their awareness about economic security. The Liaison/Awareness Program and the ESPI investigations relating to economic security are carried out under a targeting authority from the CSIS Target Approval and Review Committee (TARC).

Targeting Authority

The targeting authority sets out the criteria as to what can be investigated as an "incident of economic espionage" under the Service's mandate. An incident must involve: the participation of a foreign government, activities of a clandestine or deceptive nature, the potential acquisition of proprietary/classified information or technology, and be detrimental to Canada's economic security.

¹⁰ The Service notes that foreign states are not inclined to advertise their involvement in the clandestine procurement of economic intelligence. CSIS investigates to ascertain whether incidents are economic or industrial espionage, the latter being the responsibility of the private sector.

technological developments many people would regard as vital to Canada's economic security. Under the service's definition, such information can range from economic policy to supplier lists. In the cases we reviewed, we were hard put to see a strong link between a foreign government and the loss of certain types of economic information, such as client/supplier lists. The Service states that such a loss is considered economic espionage if a foreign state sponsored or facilitated the loss.

An analysis of the information gathered by the Service leads us to conclude that the Service collects and retains information not specifically linked to threats to the security of Canada. While the Service has developed adequate criteria to target particular incidents of economic espionage, we found that the Economic Security and Proliferation Issues (ESPI) unit investigated some incidents which did not appear to meet those criteria.

For example, ESPI investigated several incidents that, we believe, did not have a demonstrable link to a foreign government, including activities that were primarily of a criminal nature.¹¹

We also observed that CSIS sometimes collected information from briefings and presentations under the Liaison/Awareness program that was often administrative, and not specifically linked to threats to the security of Canada.

We recommend that administrative information collected from the Liaison/Awareness Program be retained in a non-section 12 data base.

We wish once again to reiterate the view we expressed in our 1993 review, that CSIS has a role to protect those areas of Canadian technology which bear directly upon national security, and about which it is necessary to advise the government. The Service should investigate only those activities that constitute "threats to the security of Canada" as set out in its mandate.

Intra-government cooperation

Since our most recent review of the economic espionage investigations revealed relatively little cooperation and coordination between CSIS and other government departments, a forthcoming SIRC study will look specifically at these issues. The investigation of economic espionage requires that the Service have access to, and make efforts to employ, both technical and business-related expertise.

A Homeland Conflict

The Committee reviewed the CSIS investigation of some persons in Canada who were associated with an internal armed conflict in an overseas country. The review covered the period from April 1994 through March 1996, and was a follow-up to a previous Committee review of similar activities in the period 1990 to 1992.¹² The CSIS investigation concentrated on the activities of a small number of people who supported the conflict

The Service faces considerable obstacles to reasonably defining its role in dealing with economic threats to Canada

11. The Service maintains that under section 2(b), it can conduct preliminary inquiries to corroborate a foreign intelligence lead on the possibility of criminality, before advising the police. We will judge these matters on a case by case basis.

12. SIRC *Annual Report 1992-1993*, page 22.

through a variety of activities on behalf of organizations that were parties to it.

The 1996 CSIS *Public Report* refers to activities that have been used to support terrorist actions, including fundraising, advocacy and information dissemination. These types of activities could, consequently, be of legitimate interest to the Service under section 2(c) of the *CSIS Act*.

Accordingly, our audit set out to determine whether the activities that CSIS investigated indeed represented a threat to the security of Canada, and whether the investigation complied with legislation, Ministerial Direction, and CSIS policy and procedures. We were also interested in whether the Service had followed up appropriately on concerns that we had expressed in the earlier review. To this end, we examined the Service's documents and, where appropriate, we sought clarification of questions arising from the document review.

Targeting decisions

After measuring requests from CSIS officers to senior management for targeting approval against the Service's established policies, and seeing whether the documents we examined substantiated the requests, we have determined that CSIS had sufficient grounds to conduct the investigation and employ the investigative methods authorized by senior management.

To receive targeting approval, CSIS policy calls for a complete and balanced description of the activities of the targets. SIRC researchers found that one of the requests could have been more complete and better balanced. For example, a request submission expressed concern about the possibility of violence occurring in Canada, but did not include information in the Service's files to the effect that a party to the insurrection at issue was unlikely to change its practice of confining terrorist activity to the homeland. The Service asserts that the inclusion of this information would not have altered the decision to approve the investigation.

CSIS' Role in Preventing Politically Motivated Violence

CSIS plays a pivotal role in Canada's defence against the possible threats posed by groups associated with politically motivated violence. The "threats to the security of Canada" which it is specifically charged to investigate include "activities within or relating to Canada directed toward or in support of the threat or use acts of serious violence against persons or property for the purpose of achieving a political objective within Canada or a foreign state..." [section 2(c), *CSIS Act*]

In addition to informing the Government in general about the nature of security threats to Canada, CSIS' intelligence and advice is specifically directed at several government departments or agencies. The information can form the basis for immigration screening profiles used in processing immigrants. In specific cases, CSIS advice can play an instrumental role in determining the admissibility of an applicant, or in the denial of citizenship. Security intelligence may also serve as a basis for determining an individual's suitability to have access to classified information, as well as assisting the police in crime prevention and in criminal prosecutions.

Conduct of the investigation

Our review focused on a small number of persons who were targeted, human sources who reported on the targets under investigation, and other investigations conducted under the targeting authorizations. The individuals investigated were leading members of their respective organizations, and had been included in the earlier SIRC audit report. We agreed both with CSIS' decision to continue investigating the activities of these persons and with the means of investigation the Service employed.

Our researchers examined CSIS documentation to determine if the investigation was consistent with the authorization and see if the Service had reasonable grounds to suspect a threat to the security of Canada.

The targeting authority for the investigation was directed at groups in Canada which operated in support of the principal organization conducting the armed insurgency in the homeland. Since there are smaller, less significant groups involved in the struggle who may also have adherents or supporters in Canada, CSIS found it necessary to investigate the possible supporters of one such group and did so under the investigative authority assigned to the principal organization.

While the Committee is in accord with the Service's decision to investigate the smaller group, we believe it should have been carried out under an authority separately obtained.

The Committee found one instance where we believe the Service had insufficient grounds to carry out

certain investigative measures against a person rumoured to be providing funds to an insurgent group in the homeland.

In a previous SIRC audit report, we expressed our concern about a CSIS investigator who appeared to use a community interview in order to inappropriately obtain personal information from the subject being interviewed. In the course of the current review, we found that the Service conducted interviews in several cities across Canada to learn more about the ethnic communities and to assess the extent and nature of a possible threat. These interviews were conducted appropriately.

We randomly selected a small number of human sources for review. We were interested in the relevance and reliability of the information provided by these sources with respect to the activities under investigation, whether the management of the sources was consistent with law and policy, and whether there were any unusual problems.

While we found that, in general, CSIS' investigation was in accordance with its operational policy, and the information it collected was necessary for the investigation, we identified one inappropriate action. A source reported on the activities of targets by attending a meeting on a campus without obtaining the prior approval of the Solicitor General as is set out in Ministerial Direction. CSIS has acknowledged this to be a compliance issue and is investigating.

CSIS had sufficient grounds to conduct the investigation and employ the investigative methods authorized by senior management

We found the exchanges with foreign agencies were consistent with the agreements in force

Liaison and exchanges of information with foreign agencies

In its 1993 report, the Committee drew attention to a case where CSIS inappropriately provided information to a foreign agency about the travel plans of a Canadian resident to a country with a poor human rights record. The most recent review shows no incidents that would raise similar concerns.

In all of the cases we reviewed, we found the exchanges with foreign agencies were consistent with the agreements in force.¹³

Quality of advice to government under section 12¹⁴

CSIS discloses the information it has collected to government clients in formal written reports and briefings. An issue for our review was whether these reports accurately reflected the information in the Service's files. We concluded that CSIS reports to Government on this investigation — while tending to be general in nature — were useful and timely.

Section 15 immigration security assessments¹⁵

The aim of this review was to assess the appropriateness of CSIS actions with respect to the powers it exercises under section 15 of the *CSIS Act* in connection with individuals from the same country whose conflict was the subject of the broader CSIS investigation.

SIRC wanted to ascertain whether the information in the briefs CSIS prepared on prospective immigrants was consistent with the information

in the Service's operational and screening files, whether the Service's recommendations were consistent with this information, and whether the assessments were prepared in accordance with the Service's operational policy. Five randomly selected security assessments prepared by CSIS were examined in depth.

The Committee was in accordance with the advice provided by CSIS in all of the assessments, and found a minor omission in one. It is evident that some information from a prospective immigrant/refugee's immigration screening interview was in fact entered into the section 12 data base. CSIS policy implies that the interviews of prospective immigrants are not to be used for other investigations. We believe that CSIS policy does not adequately address the collection of section 12 information during section 15 interviews. We have brought this issue to the Service's attention.

The Committee's general finding

The Committee has found that the Service's investigation in this matter was appropriate and that it was carried out in accordance with legislation, Ministerial Direction, and policy. We note also that following concerns expressed in SIRC's 1993 report, the Service adjusted its conduct of the investigation in a satisfactory manner.

¹³. For additional information on the CSIS Liaison Program with Foreign Agencies see page 3 of this report.

¹⁴. Section 12 of the *CSIS Act* mandates the Service to collect, analyse and retain information on threats to Canada and "report to and advise" the Government about what it has learned.

¹⁵. Under section 15 of the *CSIS Act*, the Service has the sole responsibility for security screening applicants for landed immigrant and refugee status.

B. Annual Audit of CSIS Activities in a Region of Canada

Every year the Committee audits the entire range of CSIS investigative activities — targeting, special operations, surveillance, warrants, and the use of community interviews — in a particular region of Canada. A comprehensive examination such as this provides insight into the various types of investigative tools the Service has at its disposal, and permits the Committee to assess how new Ministerial Direction and changes in CSIS policy are implemented by the operational sections of the Service.¹⁶

The Targeting of Investigations

The targeting section of the regional audit focuses on the Service's

principal duty — security intelligence investigations authorized under sections 2 and 12 of the *CSIS Act*.¹⁷ When examining any instance in which CSIS has embarked on an investigation, the Committee has three central concerns:

- did the Service have reasonable grounds to suspect a threat to the security of Canada?
- was the level of the investigation proportionate to the seriousness and imminence of the threat?
- did the Service collect only the information that was strictly necessary to advise the government on the threat?

Committee researchers also keep watch generally on the manner of the Service's adherence to its own internal policies, rules and directives.

Management of Targeting

Target Approval and Review Committee (TARC)

CSIS' capacity to target (or launch an investigation into) the activities of a person, group or organization is governed by policies that rigorously control the procedures and techniques to be employed. The Target Approval and Review Committee (TARC) is the senior operational committee within CSIS charged with considering and approving applications by Service officers to launch investigations. TARC is chaired by the Director of CSIS and includes senior CSIS officers and representatives of the Department of Justice and the Ministry of the Solicitor General.

Levels of Investigation

There are three levels of investigation, with Level 3 being the most intrusive and accompanied by the most stringent legal controls and management challenges. Level 2 investigations may include personal interviews and limited physical surveillance. Level 1 investigations are for short durations and allow CSIS to collect information from open sources and from records held by foreign police, security or intelligence organizations.

Issue-Related Targeting

An issue-related targeting authority allows CSIS to investigate the activities of a person, group or organization that may on reasonable grounds be suspected of constituting a threat to the security of Canada, and are related to or emanate from that specific issue.

¹⁶ Since the 1995-96 audit of warrants was not completed in time for inclusion in the 1995-96 SIRC *Annual Report*, this audit report also presents the Committee's conclusions from last year's audit of CSIS warrant activities in a different region.

¹⁷ Section 2, paragraphs (a) to (d) define the threats to the security of Canada. Section 12 provides CSIS with the mandate for the collection, retention, analysis, and distribution of security intelligence.

Was the level of the investigation proportionate to the seriousness and imminence of the threat?

Methodology of the audit

In the region at issue, the Committee randomly selected ten investigations conducted by CSIS in the course of the 1995-96 fiscal year for study — five counter terrorism cases and five that were counter intelligence in nature. SIRC researchers reviewed all files and operational messages in the Service's electronic data base, and interviewed the CSIS officers who carried out the investigations as well as the managers who oversaw them.

Ten cases — the Committee's findings

Inappropriate targeting authority

The first case pertained to the clandestine activities of a foreign government in Canada. In the prescribed manner, Counter Intelligence Branch submitted a request to the Target Approval and Review Committee (TARC), to investigate the activities conducted or supported by a foreign state directed against Canada's economic interests. The Targeting Committee approved the Request for Targeting Authority (RTA) and the investigation began. It is the Committee's view, however, that the Service's RTA did not demonstrate a strong connection between the activities of the foreign government and potential acts of espionage against Canadian economic interests.

The Committee's analysis indicates that the RTA failed both to articulate the specifics of the economic interests it asserted were at risk or to connect the alleged activities with the particular foreign country. Appearing prominently in the request to TARC was the term "Canadian economic interests," yet the phrase was employed in a vague manner. While the targeting authorization provided the CSIS regional office with the mandate to investigate "foreign influenced activities," the examples of the activities that CSIS cited to support the request were not accompanied by evidence that these were clandestine or deceptive activities of the foreign government at issue. Nor was there an indication of a threat to any person.

The Committee has drawn the attention of CSIS officials to our conclusions on this case. CSIS asserts that sufficient and reasonable grounds existed to suspect that espionage activity had taken place in Canada.

"Issue-related" investigations

The second case pertained to an ongoing counter terrorism investigation. In January 1996, TARC renewed an earlier authorization and agreed to

Counter Intelligence and Counter Terrorism

The terms "counter terrorism" and "counter intelligence" reflect the Service's organizational structure wherein the main national security investigative functions are divided in two: the Counter Terrorism Branch addresses threats to the public safety of Canadians and national security caused by war, instability and civil strife abroad, as well as international terrorism. The Counter Intelligence Branch monitors threats to national security stemming directly from the espionage activities of other national governments' intelligence operations.

increase the intrusiveness of this particular issue-related investigation to Level 3. All CSIS regions were authorized to investigate the suspected threat of serious political violence associated with the issue.

While the Committee observed no problems with the conduct of the investigation *per se* — regional investigators collected only the information that was “strictly necessary,” and there was no evidence of extensive reporting on individuals who were not the subject of a specific targeting authority — we have serious reservations about the Targeting Committee’s decision to increase the investigation’s level of intrusiveness. Several CSIS regional assessments indicated that the threat was either low or non-existent, not in our view, sufficient justification to move from Level 2 to Level 3.

The Committee has also been made aware of reservations about issue-related investigations generally as expressed by the Inspector General of CSIS. In the studies supporting his 1995 Certificate, he wrote that he was concerned that issue-related investigations potentially involve entire communities and allow CSIS to collect and retain, as a part of the investigative record, a wide assortment of personal and other information on individuals

and groups that are not themselves CSIS investigative targets.

The Service responded to the Inspector General stating that these “investigations were only begun when the ‘reasonable grounds to suspect’ standard” had been satisfied. The Inspector General was not convinced that it was possible for the grounds to be clearly documented and specific enough to justify an investigation in such cases.

The Committee shares the Inspector General’s concerns that issue-related investigations can cover persons and groups who are not targets. For the case at issue, however, we found that the Service used its investigative powers with parsimony; regional investigators did not collect personal information on persons who were not subject to a specific targeting authority.

Ministerial approval for intra-government cooperation

Four of the ten audit investigations involved current or past Federal Government employees. In each case, the Committee concurs with the original decision to investigate, however, for three of the four we have concerns about the manner in which the investigation was conducted.

The Service used its investigative powers with parsimony

The Service’s RTA did not demonstrate a strong connection between the activities of the foreign government and potential acts of espionage

The Role of the Inspector General of CSIS

The Inspector General of CSIS is responsible to the Solicitor General and functions effectively as the Minister’s internal auditor for CSIS, reviewing the operational activities of the Service and monitoring compliance with its policies. Every year the Inspector General must submit to the Minister a “Certificate” stating “the extent to which [he or she] is satisfied,” with the activities of the Service as outlined in CSIS annual report to the Minister. The Security Intelligence Review Committee also receives a copy of the Inspector General’s Certificate.

CSIS has standard agreements with a number of Federal Government departments that define whether and how protected information can be released to the Service. These arrangements are authorized under section 17 of the *CSIS Act* and are approved by the Minister. In the first case at issue, the Service made several inquiries of the target's employer, a Federal Government agency with which CSIS has no such formal cooperation agreement.

CSIS investigators asked a senior official in the department to consult the person's security file and they interviewed the person's supervisor. We saw no evidence of Ministerial approval for contacts of this sort.

It is the Committee's view, however, that exchanges of information of the kind that occurred in this case constitute "cooperation" and so fall under the provisions of section 17. Furthermore, the Committee's interpretation of section 17 is that in the absence of a formal agreement, the Service still requires the Solicitor General's approval to "enter into an arrangement with or otherwise cooperate with" government agencies.

We believe that CSIS should obtain the Solicitor General's approval to exchange information with or otherwise cooperate with government departments and agencies with which it does not have formal arrangements.

Non-compliance with a formal cooperation arrangement

In another case involving Federal employees, CSIS investigators made

inquiries and conducted several interviews with the target's colleagues and supervisors at his place of work. Although the Service had signed an agreement with that Federal department to share information and intelligence, the CSIS investigators sought information from employees who were not designated in the agreement. One employee did not believe that he should provide the information to CSIS. Instead, he referred the Service to another, authorized employee. The meeting that ensued was not properly documented in the Service's files.

The Service maintains that a section 17 agreement does not preclude contact with other members of a government institution, in order to collect information pursuant to the conduct of a section 12 investigation.

Reasonable expectation of privacy and the Charter of Rights and Freedoms

In the third case, CSIS acquired a certain type of information from a government agency which regarded the information as the property of the agency. The agency in question believed, therefore, that it had the authority to give the information to the Service, and CSIS officers believed no additional procedures were required to fulfill the Service's obligations under the *CSIS Act*.

Given the nature of the information and the form in which it was kept, the case raises some serious issues for the Committee. These involve, *inter alia*, the reasonable expectation of privacy on the part of the target, whether CSIS should have filed a request for the information under the

The Service still requires the Solicitor General's approval to "enter into an arrangement with or otherwise cooperate with" government agencies

Privacy Act, and whether the manner of acquisition of the information could constitute an “unreasonable search” under section 8 of the *Canadian Charter of Rights and Freedoms*.

There is little precedent in law or in operational practice to assist the Committee to a swift finding on the matter. Following additional analysis of the information exchanged, the Committee is conducting further research into the case and its implications for CSIS policy in the future.

Allaying suspicions created by CSIS investigations

In respect of all the audited investigations of government employees, the Committee is concerned that the Service’s inquiries may have left the employers concerned with a negative impression about their employees.

As a necessary part of the investigation, CSIS alerts the employers to its security concerns, but does not as a matter of course notify them about its conclusions when the investigation is complete. It is highly likely, therefore, that employers are left with the impression that employees represent continuing threats to Canada’s security.

Consequently, the Committee recommends that unless there are specific operational considerations that preclude it, the Service should in future inform Federal departments concerned about the conclusions it has drawn about Federal employees investigated.

Four cases highlighted no additional problems

In the remaining four cases, we found that the Service had reasonable grounds to suspect threats to national security. The targeting levels of the investigations were proportionate to the seriousness and imminence of the threats. The Service collected only the information that was strictly necessary to advise the government about the threats.

Obtaining and Implementing Federal Court Warrants

Obtaining Warrants - Methodology of the Audit

In order to obtain a warrant, CSIS must present its case to the Court in the form of an affidavit. Every year, the Committee examines a number of affidavits with three questions in mind:¹⁸

- is the affidavit factually accurate according to the CSIS information used to substantiate the affidavit;
- is the case in the affidavit presented to the Court in its proper context; and
- are the facts and the circumstances fully, fairly and objectively expressed in the affidavit.

In order to satisfy ourselves that the affidavits are appropriate, we compare the facts presented to the information found in the Service’s files.

Committee findings, 1994-95 warrant affidavits

Incomplete affidavits

Two affidavits were examined. The first was an emergency request from

The Service’s inquiries may have left the employers concerned with a negative impression about their employees

¹⁸. Over the course of the last fiscal year, the Committee completed reviews of Federal Court warrants obtained by CSIS in two regions. The first review began late in 1995-96 for the period 1994-95 and we were unable to present our conclusions in that year’s annual report. The second warrant review took place in 1996-97, for activities in 1995-96, and covers the same region as the other audits in this chapter.

the regional office, and while we found the urgency of the warrant to have been justified, we believe the affidavit could have been prepared with greater care. For one of the persons targeted by the warrant, the affidavit overstated a fact. For another person targeted, the Service failed to include in the affidavit significant information of which it was aware which contradicted its own position on the person.

The second application sought a renewal of warrant powers against a long-standing CSIS target. The Committee noted a minor contradiction between the affidavit and the information in the Service's files. Had this contradictory information been included in the affidavit, the Court would have been more fully informed of all the relevant facts. In general, however, the affidavit was factually accurate and correctly defined the context of the investigation.

Inaccurate tracking of warrant preparation

The procedures by which CSIS tracks the preparation of warrant applications is also of interest to the Committee. Normally, warrant

applications are reviewed both within CSIS and the Ministry of the Solicitor General to ensure that the affidavits are operationally and legally correct. An independent legal counsel from the Department of Justice then serves as an objective final assessor of the affidavit and the facts supporting it, prior to submission to the Federal Court.

The preparation process is tracked in diary form, which in the case of one affidavit, seemed to indicate to the Committee that the independent legal counsel did not have sufficient time to review the extensive documentation supporting the application. The Service subsequently informed the Committee that while it was not recorded in the tracking system, the independent counsel had in fact received a time extension to allow him to conduct a proper review before the warrant was obtained.

Committee findings, 1995-96 warrant affidavits

Again the Committee examined two affidavits and supporting documents in depth. For one warrant, in the counter intelligence area, we found no errors or omissions, and no problems of balance in the presentation.

The Use of Warrants to Investigate Threats to National Security

If during a CSIS investigation a section 21 warrant is required to investigate threats to national security, the Service must seek approval from the Federal Court. CSIS Legal Counsel, with the assistance of Service analysts, prepares an affidavit in support of the warrant to present to the Court. The affidavit explains why warrant powers, such as telephone intercepts, are needed, and the document must also meet other statutory requirements. For example, under section 21(2)(b) of the *CSIS Act*, the Service must show that other investigative means have failed, or are "unlikely to succeed." The warrant granted on the basis of the affidavit lists the powers given to CSIS, who will be subject to them, and where they may be deployed. The warrants also contain any conditions imposed by the Court on the manner in which CSIS can carry out its investigation.

Discrepancies in an affidavit

However, with the second audited warrant — directed at counter terrorism targets — we found a number of discrepancies between the statements in the affidavit, and the documents in the “schedule of facts.” In several cases, the Service wrote that it had “established” certain associations or certain patterns of contact. The supporting documentation, however, was often equivocal, and in our view, the facts appeared to be weaker than the language suggested. In some cases, the schedule of facts contained documents that seemed to contradict the Service’s case.

In the view of the Committee, these discrepancies did not undermine the case for targeting the persons named in the affidavit; that is, the affidavit was fundamentally sound, and the security threat it addressed was serious. Most of the problems stemmed from documents that were omitted from the schedule of facts, and the discrepancies between the supporting documents and the affidavit.

After conducting further research, we concluded that this particular affidavit was an aberration, and not a trend. We believe, however, that CSIS should maintain a consistent high level of rigour in the process of compiling and reviewing facts and supporting documentation, employed in affidavits.

Warrant implementation – findings

The Committee reviewed the implementation of warrants against two CSIS targets and found the Service to

have complied conscientiously with the warrants’ terms and conditions.

Warrants for two new areas of inquiry

An additional focus of this year’s review of warrant implementation was an examination of the new challenges the Service faces in exercising powers granted by warrants. Federal Court warrants are now required for two new areas of inquiry, which have “reasonable expectation of privacy” implications which the Service has recognized.

The Committee has recommended that CSIS adopt clear policy about the requirement for a Federal Court warrant to collect information in these instances.

As this is a new area, the Committee intends at a later date to conduct an in-depth review of the impact on the Service’s requests for and execution of these warrants.

Audit of Sensitive Operations and Associated Ministerial Direction**Methodology of the audit**

The very nature of sensitive operations dictates that they are the subject of relatively frequent Ministerial Direction. In addition, policy for implementing sensitive operations is set out in some detail in the *CSIS Operational Policy Manual* and all requests for sensitive operations, depending on the level of sensitivity, require at a minimum, the approval of Service senior management.

We believe the affidavit could have been prepared with greater care

“Reasonable Expectation of Privacy” and Canadian Law

The phrase “reasonable expectation of privacy” encapsulates a vital principle of Canadian law with respect to when and under what conditions the State may intrude on the privacy of an individual. Managing security intelligence involves constant weighing of the balance between two imperatives — individual privacy and threats to Canada. In commenting for the Department of Justice on the Supreme Court of Canada’s *Charter of Human Rights and Freedoms* decisions in this area, Graham Garton, Q.C. wrote:

Respect for individual privacy is an essential component of what it means to be “free.” As a corollary, the infringement of this right undeniably impinges upon an individual’s “liberty” in our free and democratic society. It is apparent, however, that privacy can never be absolute. It must be balanced against legitimate societal needs. This Court has recognized that the essence of such a balancing process lies in assessing reasonable expectation of privacy and balancing that expectation against the necessity of interference from the State. Evidently, the greater the reasonable expectation of privacy and the more significant the deleterious effects flowing from its breach, the more compelling must be the State objective, and the salutary effects of that objective, in order to justify interference with this right: *R. v. O’Connor*, [1995], 4 S.C.R. 411.¹⁹

For the purposes of the audit, the Committee examined a set of randomly selected human source investigations. In addition, we reviewed all requests from the Service for Ministerial approval of and all requests to CSIS senior managers pertaining to operations involving “sensitive institutions” or any operations dealing with lawful advocacy, protest and dissent.

Committee findings

No attempt to influence sensitive institutions

In none of the operations involving sensitive institutions that we examined did CSIS attempt to influence or direct the activities of the organizations, and source management in this regard was in compliance with the most recent Ministerial Direction.²⁰ In most of the cases, the sources’ associations with the respective organizations were not at the behest of the Service.

Ambiguity in source direction

In one of the selected cases, the Committee found the Service’s officers seemed to be unnecessarily indecisive about whether to advise a source to report a crime the person had information about to the authorities. The source thus received an ambiguous message concerning the commission of criminal acts by others. The Committee believes that the Service should have clearly counselled the source to report the information to the appropriate authorities.

Senior management approvals for operations

Of note among the senior management approvals for operations the Committee examined were the following:

The Service approved a request for a source to participate in a demonstration that had the potential to

¹⁹. Department of Justice, March 1997.

²⁰. The management of human sources, their participation in an organization’s activities and the impact of new Ministerial Direction is examined by the Committee in detail at page 10 of this report.

become violent. The source had little choice but to participate and the Service appropriately counselled him on how to avoid violent incidents.

Three approvals granted dealt with operations involving academic institutions; one of these raised a substantive issue.

Under Ministerial Direction — since revised— any use of a source on campus had to be approved by the Solicitor General. Under the procedure which obtained at the time, the Minister approved the use of a source on a particular campus.

The Service subsequently directed a second source to attend the same event under the initial approval. It is the Committee's view that the Service's action in this context was a clear contravention of the spirit of the 1984 Ministerial Direction²¹ on university campus investigations.

Retention of sensitive information on non-targets

Section 12 of the *CSIS Act* stipulates that information can be

retained by CSIS in regard to threats to the security of Canada only to the extent that it is "strictly necessary." The Committee found during its examination of one of the audit cases that the Service was holding information in a computerized data base that clearly did not fall into this category. The report at issue contained personal and sensitive information about a person who had never been a CSIS target nor the subject of an investigation, but instead had been interviewed as a potential source.

The Committee recommends that source recruitment assessments involving persons who are not targets not be retained as part of the Service's section 12 data base.

The Service informed us that it has taken corrective action.

The Surveillance of Groups and Persons

The Committee reviewed a sample of targets who were the subject of

In none of the operations involving sensitive institutions that we examined did CSIS attempt to influence or direct the activities of the organizations

Lawful Advocacy, Protest, Dissent and Sensitive Institutions

Sensitive operations invariably involve the use and direction of human sources, and while human sources can be the most cost-efficient form of intelligence collection, their use also entails the greatest risk in terms of impact on societal institutions, legitimate dissent, and individual privacy. The *CSIS Act* specifically prohibits the Service from investigating "lawful advocacy, protest or dissent" unless carried on in conjunction with threats to the security of Canada as defined in the *Act*. The Service is obligated to weigh with care the requirement for an investigation against its possible impact on the civil liberties of persons and sensitive institutions in Canada, including trade unions, the media, religious institutions and university campuses.

21. See "Ministerial Direction" page 52.

... the Committee was satisfied to see that CSIS regional employees made considerable efforts to understand the homelands conflicts. . . .

surveillance coverage in fiscal year 1995-96. We examined the surveillance reports to determine whether the surveillance,

- conformed to the requirements and restrictions set out by the Target Approval and Review Committee (TARC);
- exceeded the “strictly necessary” provision of the *CSIS Act*, or otherwise unduly or unnecessarily infringed on a person’s privacy; and
- complied with Ministerial Direction and the *CSIS Operational Policy Manual*.

Committee findings

Our review of selected cases indicates that the Service complied with all policies and procedures for carrying out surveillance operations and conducted them in an appropriate manner. There were no occasions where emergency requests for surveillance were made in the Region we audited.

Quality of surveillance with reduced resources

Surveillance is a resource-intensive activity. In the region we reviewed, the Committee did not find that the

selective tasking for surveillance and the Service’s diminishing resources had a negative effect on the quality of surveillance operations.

Interviews Within Particular Communities

Since 1990, CSIS has employed community interviews regularly in order to learn more about potential threats to Canada’s security from the spillover of overseas “homelands” conflicts into Canada. The interviews also serve to sensitize ethnic communities about the aims of the Service and its role in protecting the security of Canada and Canadians. In the region the Committee audited for this report, three programs to interview leaders of communities or interest groups were underway.

As in past audits of community interviews, the Committee’s concern was to determine whether the interviews were conducted in a proper manner. Specifically, were they properly authorized; was the information collected and retained only that which was “strictly necessary”; and was the scope of the interview program appropriately defined.

CSIS and the Use of Surveillance

CSIS uses surveillance to learn about the behaviour patterns, associations, movements, and “trade-craft” of groups or persons targeted for investigation. As an investigative tool, surveillance is used to detect espionage, terrorism, or other threats to national security. Large amounts of personal information can be collected and retained in the course of surveillance operations. The Service’s surveillance units use various techniques to gather information. In an emergency, surveillance can be used before a targeting authority has been obtained.

In general, the Committee was satisfied to see that CSIS regional employees made considerable efforts to understand the homelands conflicts figuring prominently in the current interview programs. As part of the preparatory work, the investigators reviewed background reports from other Government of Canada departments.

Findings of the Committee

Interview program I

The Service considers this community interview program to have been the most successful and the Committee concurs. To date, neither CSIS nor SIRC have received a single complaint relating to the interviews conducted.

The Committee saw no evidence that the Service collected inappropriate personal information about those persons interviewed. It retained only what was “strictly necessary” to advise the government. Investigators asked questions regarding the potential for violence or foreign influence in the ethnic community and the impact of Canada’s military role in the conflict.

The Service’s Regional office noted that there had been isolated incidents of inter-ethnic community harassment by what it termed “hot heads” during the period under review, but stressed that there was no trend to widespread or serious violence. With regards to foreign embassy interference, the Service observed none of consequence.

The Committee believes that as the overseas conflict winds down, we would expect to see the end of this

particular community interview program.

Interview program II

The second community interview program revealed an apolitical community which, while concerned about the unfolding events overseas, did not manifest a potential for violence in Canada. The Regional office noted that during the period of the interviews, a foreign mission in Canada tried to apply subtle influence on the community to refrain from political involvement in the home country.

The Committee noted that CSIS interviewed relatively few people and that the investigators appeared to be respectful of those they spoke to; we saw no evidence of the collection of inappropriate information.

The interview program was terminated after six months — a decision the Committee believes was valid considering the paucity of reasonable grounds to suspect a threat to national security arising from the ethnic community in Canada.

Interview program III

The Committee identified no difficulties with the few interviews conducted in this program, but did take issue with the fact that the investigation was set in motion in the first instance.

The targeting authorization referred to information from foreign services to the effect that overseas extremists might have taken root in Canada. This prompted CSIS to develop the community interview program. The

The Committee saw no evidence that the Service collected inappropriate personal information about those persons interviewed

The Committee did take issue with the fact that the investigation was set in motion in the first instance.

The Committee remains concerned about the ambiguity evident in the definition of what constitutes a community interview program

Committee saw no evidence in the documents to sustain that premise.

The Service has acknowledged that while it was unaware of any extremists or their supporters in Canada at the time, threats of violence from extremists overseas remained a concern, as did a potential indirect threat to Canadians living overseas. The Committee noted, however, that the content of interviews focused on what was happening in Canada, not on the events taking place abroad.

In any event, the investigation failed to corroborate the original information or to identify possible affiliates of extremist organizations in Canada. The Service subsequently elected to allow the investigation to conclude upon the expiry of the targeting authority and stated that it would monitor any future developments related to the threat via its other investigations.

Development of written policies for community interviews

The Committee is pleased to note that the Service acted on a previous SIRC recommendation and elaborated a policy which would compel investigators to inform interviewees that their cooperation is voluntary.

As in previous years, the Committee remains concerned about the ambiguity evident in the definition of what constitutes a community interview program. The correspondence that CSIS sent us to explain the issue was helpful, and we believe the Service should consider adding the information to its policy.

The Committee recommends that the definition of community interview programs be clearly set out in CSIS policy.

In a related policy matter which remains unresolved, the Committee recommended in its last audit that the Service update its *Operational Policy Manual* to include an existing memorandum on procedures for community interviews. We have seen no corporate policy revisions in this area to date.

C. Inside CSIS

The third part of this section dealing directly with what CSIS does and how it does it, consists of the Committee's comments and findings on how the Service manages its own affairs and its relations with other agencies of Government and other national governments.

Statistics on Operational Activities

By law, the Committee is obliged to compile and analyse statistics on the operational activities of the Service.

Annually, the Service provides the Committee with statistics in a number of areas: warrants, sensitive operations, finances, person-year usage and the like. We compare them against the data from previous years and question CSIS about any anomalies or new trends that we identify.

New classification system undermines Committee analysis

In 1996-97 we learned that the Service modified its statistical collection categories in the counter intelligence area. Under the old system, the categories were mainly geographically based, and as such were readily linked to identifiable targets. Under the new system, the statistics are subsumed under “themes” — economic espionage, political espionage, military espionage, foreign intelligence, proliferation, and foreign interference.

CSIS stated that the modifications were due, in part, to efforts to respond better to Cabinet Direction. However, the Committee found that many of the new definitions were unhelpfully vague and effectively undermined our ability to compile and analyse the necessary statistics.

For example, under the new system, a foreign intelligence service that uses a source to obtain information from an elected official might fall under “political espionage.”

In addition, the new categories sever the statistical measures of investigations from readily identifiable targets, and because the titles are no longer standard, they make multi-year comparisons impossible.

The Committee, therefore, has asked CSIS to provide us with all of the statistical data by standard geographic, in addition to the new thematic, classifications.

Warrants and warrant statistics

Collecting and evaluating information on warrants is viewed by the Committee as an important task. Warrants are one of the most powerful and intrusive tools in the hands of any branch of the Government of Canada; for this reason alone their use bears continued scrutiny. In addition, the kinds of warrants granted and the nature of the targets listed provide insight into the entire breadth of CSIS investigative activities and are an important indicator of the Service’s view of its priorities.

Table 1 compares the number of warrants over three fiscal years.

... many of the new definitions were unhelpfully vague and effectively undermined our ability to compile and analyse

Table 1
New and Renewed Warrants

	1994-95	1995-96	1996-97
New Warrants Granted	85	32	125
Warrants Renewed/Replaced	130	180	163
Total	215	212	288

Foreign nationals continue to constitute the majority of persons subject to warrant powers

In 1996-97, the number of new warrants rose dramatically to 125, a substantial increase attributable to the restructuring of the warrants.²² The Service drew up affidavits requesting warrant powers in additional areas of investigation, resulting in the Federal Court granting a number of new warrants. In addition, Federal Court warrants are now required for new types of inquiry.

The number of persons affected by CSIS warrant powers has increased slightly because of the addition of the new areas of investigation. Foreign nationals continue to constitute the majority of persons subject to warrant powers.

Regulations

Under section 28 of the *CSIS Act*, the Governor in Council may issue regulations concerning how the Service may apply for warrants. In fiscal year 1996-97, no new regulations were issued.

Federal court warrant conditions

All warrants granted by the Federal Court contain conditions which the

Service must follow in their execution. In 1995-96, there were a number of revisions and additions to the conditions attached to CSIS warrants. The Federal Court made one amendment and added two restrictions on how the Service can execute warrants in one type of warrant, and narrowed the manner in which the Service is able to execute warrant powers in another. Finally, three new conditions were laid down by the Federal Court which served to restrict certain types of warrants.

As we noted in the section on warrant implementation, the Committee continues to monitor changes in warrants and the powers associated with them.

CSIS Finances

On an annual basis, the Service provides the Committee with basic information on CSIS funding, and over the course of the year, we also examine any funding problems that come to our attention.

Table 2 shows spending by CSIS over the last six years:

Table 2
Actual Expenditures (\$000)

	Personnel	Other Expenditures	Capital	Total
1992-93	124,926	72,591	27,833	225,350
1993-94	118,819	77,282	48,190	224,291
1994-95	115,579	71,715	18,381	205,675
1995-96	110,723	69,048	4,383	184,154
1996-97	100,153	65,287	0	165,440
1997-98 ²³	99,751	65,243	0	164,994

22. In our 1995-96 *Annual Report*, we pointed out that warrant statistics do not reflect how many persons are affected by warrant powers. One warrant can involve many people, while several warrants may not mean an increase in the number of people affected.

23. *Main Estimates, 1997-98*

“Other Expenditures” includes expenses under “Construction and Acquisition of Land, Buildings and Works”, and “Machinery and Equipment.” Significant amounts were expended to upgrade CSIS computers. In 1997-98, for the first time, CSIS will pay \$2.4 million to Public Works and Government Services Canada for grants to municipalities in lieu of the payment of property taxes. The amount was formerly paid out of the Department of Public Works budget.

CSIS has been subject to significant budgetary cutbacks. In the course of the year, the Committee asked for and received a special briefing on the effect of cutbacks on the ability of the Service to cope with rapid change.

CSIS Operational Branches

Counter Terrorism (CT) Branch

The Counter Terrorism Branch is one of the Service’s two main investigatory sections (the other being Counter Intelligence) and its role is to provide the Government of Canada with advice about emerging threats of serious violence that could affect the national security of Canada. The threat from international terrorism continues to be associated with what are termed “homeland” conflicts. As CSIS has pointed out, many of the world’s terrorist groups have a presence in Canada, where they engage in a variety of activities in support of terrorist movements.²⁴

Since our last annual report, there have been no significant changes to the Counter Terrorism program.

Although public security remains the Service’s main focus, the Branch has had to respond to government-wide fiscal restraint and budget reductions.

According to CSIS, proposals for restructuring the Branch were approved by the Service’s Executive in November 1996. The proposals were consistent with the ongoing effort to make the structure of the Branch more efficient and to ensure that the maximum number of resources are directly employed in addressing the terrorist threat to the security of Canada.

The modifications in structure and operations were implemented in May 1997; their impact on the Service will be examined by the Committee in future audits.

Threat assessments

Originating primarily within the CT branch, CSIS provides other departments and agencies in the Federal Government with information about potential threats to national security by issuing threat assessments. In 1996-97, the Service brought forth 540 threat assessments, down from 602 produced the previous year.

CSIS stated that it could not attribute the decline to any specific cause. The volume of threat assessments is contingent on a number of factors beyond the Service’s control: the number of foreign visitors whose presence in Canada is cause for warning; the volume of requests received from other government departments and agencies; and the number of threats identified during the year.

Many of the world’s terrorist groups have a presence in Canada, where they engage in a variety of activities in support of terrorist movements

24. CSIS 1996 Public Report.

CSIS provides other departments and agencies in the Federal Government with information about potential threats to national security by issuing threat assessments

Counter Intelligence (CI) Branch

Counter Intelligence Branch monitors threats to national security stemming from the espionage activities of other national governments' intelligence operations. By fiscal year 1996-97, the CI Branch was no longer investigating many former adversaries and intelligence services in what, since the end of the Cold War, have become emerging democratic states.

Instead, the Branch was pursuing a strategy of encouraging such agencies to act with more "transparency." That is, in its pursuit of liaison relationships with former and even current adversaries, the Branch has sought to find common ground for cooperation and information sharing.²⁵

In May 1996, Canadians learned about a Counter Intelligence Branch success: the arrest of the Lambert couple (Dmitry Olshevsky and Elena Olshevskaya). The Lamberts were trained "illegals" — spies who entered Canada illegally and assumed false Canadian identities.

During 1996-97, the number of intelligence officers in the Counter Intelligence Branch rose slightly. The Service states that the Branch is focusing its resources on the areas of transnational crime, economic security, and issues surrounding the proliferation of weapons.²⁶ Where formal agreements are in place, the Service has strengthened its liaison relationships with foreign agencies to share information in these areas.

Analysis and Production (RAP) Branch

The Service's research arm, the Analysis and Production Branch, underwent a major reorganization in 1996-97. The goals of the reorganization were two: to improve the coordination of intelligence production with the Privy Council Office's Intelligence Assessment Secretariat,²⁷ and enhance the intelligence support to the main consumers of its product inside the Service — the operational desks, the Executive, Security Liaison Officers, and the like.

The Analysis and Production Branch adopted a new structure with three divisions: one responsible for counter intelligence and foreign intelligence matters, a division that deals with counter terrorism matters, and a division to prepare documents such as the public annual report and the classified annual report to the Solicitor General.

The Branch received no additional resources with which to operate. The Strategic Analysis Unit was disbanded and its analysts integrated within the other units as "experts in residence." A new unit was established to deal with foreign intelligence.

The Branch states that it is seeking to play a more proactive role by improving its dialogue with consumers of foreign intelligence products and those who set the Government of Canada's foreign intelligence requirements. The Branch now employs a standardized format for its reports, with a shorter turnaround time for production.

25. The Service's Foreign Liaison program is the subject of a special report beginning on page 3.

26. The Service's efforts in regard to threats to Canada's economic security are subject of a special report at page 11.

27. The Intelligence Assessment Secretariat of the Privy Council Office (PCO) produces foreign intelligence assessments. It coordinates the interdepartmental activities and assessments of the Intelligence Assessment Committee, chaired by the Executive Director, whose membership is composed of senior officials from the departments and agencies most concerned with intelligence matters.

The Analysis and Production Branch has become more involved in “environmental scanning” activities. Using publicly available information, the Branch analyses foreign disputes to assess the potential of these conflicts to impact on Canadian interests.

Arrangements with Other Departments and Governments

Domestic arrangements

In carrying out its mandate, CSIS cooperates with police forces, and federal and provincial departments and agencies across Canada. As outlined earlier in this year’s audit report,²⁸ the Service may conclude cooperation agreements with domestic agencies after having received the approval of the Minister. Usually, the agreements pertain to exchanges of information, and less frequently, to collaboration in the conduct of operations or investigations.

Currently, CSIS has twenty-four arrangements with Federal Government departments and agencies, and eight agreements with the provinces. CSIS also has a separate arrangement with several police forces in one province. The Service is not required to enter into a formal arrangement in order to pass information or cooperate on an operational level with domestic agencies, though Ministerial approval for such contacts is required. It is the usual practice for the Service to enter into a formal arrangement when the other party requires terms of reference or the setting out of agreed undertakings.

Arrangements for 1996-97

The Service signed no new agreements with domestic agencies in fiscal year 1996-97 and stated that all of its current agreements were working well. In the course of our review of CSIS operations the Committee identified no significant concerns with regard to domestic agreements.

An agreement which expired in 1994 has not yet been renewed and no consultations to accomplish its renewal were held during the audit period. However, cooperation between the Service and the agencies covered by the previous agreement has continued without difficulty, with the approval of the Minister.

Information exchanged with other domestic agencies

Annually, the Committee reviews the information CSIS exchanges with other bodies in Canada in order to ensure that the Service is collecting and disclosing information in conformity with the *CSIS Act*, Ministerial Direction and Service policy.²⁹ In particular, we review whether,

- the threat is balanced against the infringement on personal privacy resulting from the passage of information;
- the exchange of information is strictly necessary to meet the Service’s operational requirements pursuant to section 12 of the *CSIS Act*;

The Service may conclude cooperation agreements with domestic agencies after having received the approval of the Minister

²⁸. See Section 1, “Annual Audit of a Region” discussion of Ministerial approval for intra-government cooperation.

²⁹. Under the *CSIS Act*, the Service is to cooperate with federal and provincial departments and agencies (section 17), and disclose information [section 19(2)] “for the purpose of the performance of its duties and functions.” Operational cooperation with other government institutions includes the exchanges of information, the provision of operational assistance, and can include the execution of joint operations. Section 38(a)(iii) of the *CSIS Act* states that the Committee has a duty, “to review the arrangements entered into by the Service pursuant to subsections 13(2) and (3), and 17(1) and to monitor the provision of information and intelligence pursuant to those arrangements.”

The Committee questioned both the relevance of the reports to threats to the security of Canada and the necessity for the Service to collect them

- the information exchanged consists of unnecessarily personal and sensitive information, such as medical or welfare records;
- the information exchanged is reasonable, and factually accurate;
- all CSIS disclosures of information are in accordance with the preamble to subsection 19(2) or paragraphs 19(2)(a) to (d); and
- the information that CSIS provides is within the mandate of the agency receiving it.

Methodology of the audit

For calendar year 1995, the Committee examined approximately 5,000 exchanges of information with other government institutions, such as the police, federal and provincial departments and agencies. All disclosures made under section 19 of the *CSIS Act* were also reviewed. We conducted on-site reviews in two regional offices in order to assess the status of cooperation between CSIS and other agencies in those regions.

Findings of the Committee

We found that the majority of the CSIS exchanges of information in 1995 were within policy parameters and statutory requirements. Several issues, however, require comment.

Collection of information on advocacy

The nature of a set of reports a regional police force gave to CSIS, and the Service's subsequent handling of them, gave rise to Committee concerns. The reports commented on a series of events that involved public advocacy or protest. The Service had deposited all of the

reports into the Service's operational (section 12) data base. However, on review of the reports' contents, the Committee questioned both the relevance of the reports to threats to the security of Canada and the necessity for the Service to collect them in order to fulfill its role in advising the government.

The Committee notified the Service of its concerns, following which, CSIS agreed to delete three of the four reports. CSIS believes that the remaining report contains section 12 information. The Committee remains of the view that the outstanding report should also be removed from the operational data base, since the activities reported upon are not related to a Service investigation.

In regard to the collection and retention of information of this type generally, the Committee believes that existing Service policy does not provide comprehensive guidance to its officers.

We recommend, therefore, that the Service review and set out policy which addresses gaps in current policy pertaining to information exchanges with police agencies in relation to advocacy, protest, and dissent.

The Committee will continue to monitor the situation.

Clarification of separate mandates

In the course of its investigations, the Service interviewed managers in two government departments. On reviewing the files on this matter, the Committee was not able to

determine whether the interviews had an operational (section 12 of the *CSIS Act*) or security screening-related (section 15) purpose. In response, the Service stated that its policies did delineate between these types of investigations; the Committee's view differs and our concerns remain.

The *CSIS Act* clearly defines two kinds of investigatory powers for the Service, each with its own array of managerial and legal tests and controls. The Committee believes that any blurring of intent between these two quite separate functions wherein information collected with one stated purpose is used for another, raises concerns about the taking of administrative "shortcuts" and invasion of privacy.

We recommend, therefore, that the Service take the necessary measures to ensure that section 12 and section 15 investigations are clearly distinguishable, and, where they may of necessity overlap, ensure that all the applicable tests and controls are in place.

Our recommendation is directed at CSIS practice, rather than policy. The Committee intends to pay continued special attention to this issue.

Non-compliance with an information exchange agreement

Under a written agreement with a particular Federal Government department the Service has access to certain information acquired by the department. Under the agreement, an official of the department

is designated as the point of contact between the agencies.

In its review, the Committee became aware of a case where CSIS by-passed the designated person and communicated directly with another employee of the department, thus—in the view of the Committee—contravening the agreement. The Service is of another view generally about such agreements, in that it regards designated persons as facilitators who may be used in the liaison role, but who are not the only persons CSIS can approach for information.

The Committee regards its own interpretation as the correct one. Where the Service has reached a formal agreement covering section 12 investigations with a government department or agency — the main purpose of which is to set out terms and conditions governing the relationship — the Service is obliged to comply strictly with the terms of that arrangement.

Non-compliance with requirements for accessing personal information

In order for the Service to access personal information acquired by a Federal Government department or agency, the Service is required to file a request through section 8(2)(e) of the *Privacy Act*. The Committee has identified three cases where, in our opinion, CSIS did not comply with the *Act*.

In one case, the Service did not agree with the Committee's view that the information at issue was personal in nature. The Committee continues to hold to its original position.

We found that the majority of the CSIS exchanges of information in 1995 were within policy parameters and statutory requirements

The Director of CSIS will now report all disclosures made in the national interest (special disclosures) to the Committee.

In respect of the other two cases, the Service stated that while the information was personal in nature, it did not originate as a government record and thus was not subject to the requirements of the *Privacy Act*. The Committee's review of the information led us to conclude differently: the opinions collected by the Service were in our view based on information acquired in the government workplace, and the Service should have filed an information request in these cases as well.

Policy and direction

In 1995, there was no new Ministerial Direction related to domestic agreements and cooperation or exchanges of information

There were two changes to CSIS policy with implications for inter-agency cooperation. In the first, the Service issued written policy on operational cooperation with other Canadian government institutions. The policy formalizes current practice and thus does not call for comment from the Committee.

The second policy issued, responds to a recommendation in the Committee's 1992-93 report, which addressed the issue of "special disclosures" by the Service. As a general principle, the Service is restricted as to whom it may disclose information. CSIS may make special disclosures to persons outside of government, at the request of the Solicitor General.

At the time, the Committee recommended that special disclosures meet the same test as disclosures made under section 19(2)(d) of the *CSIS Act*; that is, the Commit-

tee should be notified when they are made. Under the new policy, the Director of CSIS will now report all disclosures made in the national interest (special disclosures) to the Committee.

International arrangements

Pursuant to section 17(b) of the *CSIS Act*, the Service must obtain the approval of the Solicitor General — after consultation with the Minister of Foreign Affairs and International Trade — before entering into an arrangement with the government of a foreign state or an international organization. During the exploratory and negotiating phase leading to an agreement, no classified information is exchanged.

Arrangements for 1996-97³⁰

As of 31 March 1997, the Service had a total of 203 arrangements with 123 countries and three international organizations. During the year, the Minister approved one new arrangement with a foreign agency in Asia and three existing arrangements were expanded. Two of the three agencies' predecessor organizations (both in countries on the same continent) had poor human rights records; the revised agreements will allow for consultation and technical assistance.

Information about transnational crime

A number of intelligence agencies abroad collect information about trans-national crime. One of the functions of CSIS Security Liaison Officers posted abroad is to develop and maintain the inter-

³⁰ The broad scope of the Service's foreign liaison and cooperation activities are subject of a special audit report in Section 1, page 3.

agency relations required to facilitate the exchange of this information.³¹ In turn, the Service passes the information on to the appropriate law enforcement authorities in Canada.

Collection of Foreign Intelligence

Foreign intelligence is information concerning the “capabilities, intentions or activities” of a foreign state. Under section 16 of the *CSIS Act*, the Service may, at the written request of the Minister of Foreign Affairs and International Trade or the Minister of National Defence, collect foreign intelligence.

Methodology of the audit

The Committee employs various methods to audit the collection of foreign intelligence:

- as required by section 16 of the *CSIS Act*, we examine Ministers’ requests for assistance;
- we review all information about Canadians retained by CSIS for national security purposes;
- pursuant to the “strictly necessary” requirement of section 12 of the *CSIS Act*, we assess whether CSIS has a valid reason to retain information from section 16 operations;
- in general terms, we assess whether the Service’s cooperation with the Communications Security Establishment (CSE)³² complies with the *CSIS Act*.

Committee findings

The Committee noted several new developments regarding both policy and operational matters with respect to section 16 (foreign intelligence) operations within the Service.

At the policy level, CSIS published in 1995-96 a new chapter in the *CSIS Operational Policy Manual* formalizing existing procedures.

In an operational matter, CSIS has established a new system for handling foreign intelligence reports. This new mechanism does not materially change the Committee’s ability to track the manner and extent to which CSIS retains foreign intelligence.

Inappropriate use and retention of identifying information

Two cases drew special attention from the Committee. In the first, the Service sought and obtained from the Communications Security Establishment information that identified a person or organization without sufficient explanation of why it required the information.

In the second case, we identified an instance where information about a prominent individual’s involvement in a morally questionable activity had been retained — improperly, in the Committee’s view. We believe that the retention of the identifying information in this case was not “strictly necessary,” given the potential detriment to the person.

The Committee employs various methods to audit the collection of foreign intelligence

31. For more on CSIS Security Liaison Officers see, page 3.

32. The Communications Security Establishment is an agency of the Department of Defence. As described by the Auditor General in his 1996 report to Parliament, *The Canadian Intelligence Community*, the CSE, “analyses and reports on intercepted foreign radio, radar and other electronic emissions... and provides this foreign intelligence to Canadian government clients.”

The Committee constantly monitors the Service's file management policies and practices

We recommend that CSIS clarify its policy in regard to the "strictly necessary" requirement when assessing whether to retain identifying information from foreign intelligence in the Service's computerized data base.

Stale-dated ministerial requests

In last year's report, the Committee noted that a number of standing requests for assistance from Ministers were three or more years old, and had not been signed by the then current Ministers. The Ministers subsequently signed the requests.

Management, Retention and Disposition of Files

Files are the essential currency of intelligence gathering. Every CSIS investigation and every approved target requires the creation of a file, and a system for making the information in it available to appropriate officers in the Service. Balanced against this information gathering apparatus is the clear restriction on the Service set out in the *CSIS Act*, that it shall collect information "to the extent that it is strictly necessary." The Committee constantly monitors the Service's file management policies and practices to help ensure that no unnecessary information is improperly retained or distributed.

File disposition

CSIS files are held according to pre-determined schedules that define how long they must be retained after Service employees cease using them. When this period expires, the National

Archives Requirements Unit (NARU) in CSIS reviews the files for disposition. The staff in NARU decide whether to keep the file, destroy it, or send it to the National Archives' holdings.

During fiscal year 1996-97, NARU reviewed 12,495 files. Of these, 8,565 were destroyed, the Service retained 3,896 files, and 34 will be sent to National Archives once the retention dates are reached. This is far lower than last year's 115,000 files processed by the Unit, a decrease owing to the final disposal in the year previous of the remainder of approximately half a million files inherited from the Royal Canadian Mounted Police in 1984.

New File Statistics

Comparing new file statistics for 1995-96 and 1996-97 highlights two interesting trends:

- major decreases in the files on foreign nationals visiting Canada, where there was a counter intelligence concern; and
- increases in the number of files on screening, particularly in the categories of citizenship, immigration and refugees.

The Committee is cautious about drawing too much from these observations. A decrease or increase in the number of files does not, of itself, presage a change in the threats to national security. It may instead represent variations in individuals' memberships or group affiliations, or alternatively reflect the Service's focus on the most dangerous elements in some groups.

CSIS retention of internal E-mail

One continuing area of concern for the Committee has been the management of the Service's E-mail system. In the past, CSIS, like most large organizations, relied almost exclusively on hard copy, paper-based files. This was helpful to the Committee's research and audit activities in that all written communications within CSIS could be found in these files, including internal memoranda and notes pertaining to operations.

Recently, however, the Service has converted its information management system to a "paperless" electronic one which automatically retains formal communications within CSIS (thus retaining it for audit) but does not do so for "informal" correspondence.

Early in the new system's implementation period, the Committee noted a relative dearth of E-mail notes (the equivalent of the old hardcopy internal memoranda) normal to most operations. We subsequently learned that for the informal E-mail notes to be retained required a decision by each CSIS officer on whether to "save" the correspondence. Indeed, CSIS staff were alerted to the fact that anything they saved would be subject to review.

CSIS has since revised its instructions to employees; the new procedures appear to facilitate saving the E-mail that should be placed in the corporate record. The Committee has since noted a gradual increase in the volume of operational E-mail

that we encounter in the course of our reviews. We will continue to monitor the situation.

Internal Security

In the 1994-95 SIRC Annual Report, we reported on the case of Aldrich Ames, a Central Intelligence Agency employee arrested for spying for the Soviet Union. On 16 November 1996, a second Central Intelligence Agency employee, Harold James Nicholson, was arrested for spying on behalf of Russia. Like Ames, Nicholson's motivation was financial. It does not appear that he obtained or betrayed information that can be considered injurious to Canada's national security.

As a result of the Ames case, CSIS undertook a review of its own internal security practices. The Committee received the final report of that review, *Finding the Balance*, in October 1996.

The Service's report concluded that, "CSIS maintains sound and effective security practices," and underlined the view that security procedures must be balanced against the rights of CSIS employees. The report recommends a number of changes in the areas of security clearances for CSIS staff, as well as enhanced security awareness programs, and increased physical security. In addition, the report recommends that CSIS employees be required to disclose financial information on hiring, and be subject to polygraph testing on a periodic basis.

One continuing area of concern for the Committee has been the management of the Service's E-mail system

... there is little empirical evidence for concluding that there is value in the increased use of the polygraph in employment screening

The Committee believes that the employee complement of CSIS should be broadly representative of Canada's population

The implementation of new procedures for vetting security clearances for external contractors, and random searches of staff and visitors was also recommended. The Committee understands that as of the time of release of this report, most of the recommendations have been adopted.

Committee comments on matters of internal security

It is the Committee's view that employee awareness of security issues and knowledge of proper procedures is at least as important as designing new procedures. We noted that the report deferred extensive comment on the control and handling of classified documents and instead recommended that a study be conducted. CSIS informs us that the study has since been undertaken.

We also believe there is little empirical evidence for concluding that there is value in the increased use of the polygraph in employment screening. The Committee continues to hold to the opinion expressed in previous reports that a rigorous program of security checks would probably be more effective.

Personnel Recruitment and Representation Within CSIS

Recruitment of personnel

The Service held two Intelligence Officer (IO) Entry Training Courses for fiscal year 1996-97 with a total of thirty participants. All but one recruit successfully completed the course. Five of the

trainees were conversions from other positions within the Service.

The female to male recruitment ratio was seventeen females to thirteen males, a change from last year's ratio of ten to twenty-two. The representation of visible minorities was one male and three females.

All students met the bilingualism criteria.

Representation of Canadian population in the Service

The Committee believes that the employee complement of CSIS should be broadly representative of Canada's population. Over the past several years, we observed some progress in the Service's recruitment of certain groups, but much remains to be done.

The Service made the most progress in meeting its objectives for the employment of visible minorities. CSIS has also made some advances in employing Aboriginal peoples and persons with disabilities, although the Service did not meet the objectives it had set for itself. CSIS states that the under-representation of Aboriginal groups is a phenomenon of the Public Service at large and results, in part, from a high resignation rate. Although CSIS achieved its objective for employing persons with disabilities in 1994, the two subsequent years have been less successful.

CSIS exceeded its objectives for placing women in the management category positions in 1995, and in

the senior intelligence officer levels in 1996. Since then, however, representation of women has declined both because of resignations, and reductions in numbers of positions in management categories where women were fairly well represented. Similarly, the Committee has noted the fact that cutbacks in CSIS staff levels have had their greatest impact on the women employees in the Administration category.

Section 2: Investigation of Complaints

Quite distinct from its function to audit and review the Service's intelligence activities, SIRC's second primary role is to investigate complaints from the public about any CSIS action. There are three discrete areas within the Committee's purview:³³

- The Committee is constituted as a quasi-judicial tribunal to consider and report on any matter having to do with federal security clearances, including complaints about denials of clearances to government employees or contractors.
- The Committee investigates reports made by Ministers about persons in relation to citizenship and immigration, certain human

rights matters, and organized crime.

- As set out in the *CSIS Act*, any person may lodge a complaint with the Review Committee, "with respect to any act or thing done by the Service."

Section A below sets out the Committee's analysis of the numbers and types of complaints received during the 1996-97 fiscal year.

Section B reviews CSIS' role in conducting security screenings and assessments on behalf of the government.

A. 1996-97 Complaints About CSIS Activities

Statistics

During the 1996-97 fiscal year, we received thirty-three new complaints under section 41 of the *CSIS Act* ("any act or thing") and

SIRC's Role Regarding Complaints About CSIS Activities

The Review Committee, under the provisions of section 41 of the *CSIS Act*, must investigate complaints made by "any person" with respect to "any act or thing done by the Service." Before the Committee investigates, however, two conditions must be met:

- the complainant must have first complained to the Director of CSIS, and have not received a response within a period of time that the Committee considers reasonable, (approximately thirty days) or the complainant must be dissatisfied with the Director's response; and
- the Committee must be satisfied that the complaint is not trivial, frivolous, vexatious or made in bad faith.

Furthermore, under subsection 41(2), the Committee cannot investigate a complaint that can be channelled through another grievance procedure under the *CSIS Act* or the *Public Service Staff Relations Act*. These conditions do not diminish the Committee's ability to investigate cases and make findings and recommendations where individuals feel that they have not had their complaints answered satisfactorily by CSIS.

³³ The *CSIS Act* stipulates that SIRC conduct investigations pursuant to complaints made to the Committee under sections 41 and 42. The *Act* also states that SIRC can conduct investigations in regard to reports or matters referred to the Committee pursuant to section 17.1 of the *Citizenship Act*, sections 39 and 82.1 of the *Immigration Act* and Section 36.1 of the *Canadian Human Rights Act*.

Table 3
Complaints (1 April 1996 to 31 March 1997)

	New Complaints	Carried Over from 1995-96	Closed in 1996-97	Carried to 1997-98
CSIS Activities	33	4	36	1
Security Clearances	1	0	1	0
Immigration	1	0	0	1
Citizenship	1	0	0	1
Human Rights	0	0	0	0

one under section 42 (denial of security clearance). In addition, the Committee received two ministerial reports — one pertaining to the *Citizenship Act*, the other to the *Immigration Act*.

Findings on 1996-97 complaints “with respect to any act or thing”

During fiscal year 1996-97, we received five complaints from persons who asserted that the Service had subjected them to surveillance, kidnapped them, censored their mail or telephone service, or medically implanted devices in them.

In response to complaints, the Committee as a general rule neither confirms nor denies that the person complaining is a target. The Committee thoroughly investigates the complainant’s assertions in order to ensure that the Service has not used its powers unreasonably. If we find that the Service has performed its duties and functions efficiently and properly, we then convey that assurance to the complainant. The Committee

found nothing unreasonable about CSIS activities in relation to these five cases and that assurance was conveyed to the complainants.

Ten complaints were received about which the Committee took no action, apart from advising the complainants that in failing first to take the complaint to the Service directly, they had not met the requirements necessary for SIRC to investigate further. Six other complainants were informed that the Committee did not have jurisdiction to investigate their particular cases.

For the second consecutive year, we received nine complaints with respect to the Service’s activities in providing security assessments and/or advice to the Minister of Citizenship and Immigration Canada. In four cases, the Committee was able to confirm that the Service had concluded its enquiries and had forwarded, or was about to forward, its recommendations to Citizenship and Immigration Canada (CIC). In two other complaints, the Committee ruled that the complexity of the cases justified the time taken by CSIS to process the assessments.

If we find that the Service has performed its duties and functions efficiently and properly, we then convey that assurance to the complainant

The Evolution of the Security Clearance Complaints Procedure

The Committee has been constituted as a complaint tribunal to consider and report on any matter having to do with federal security clearances. Under section 42 of the *CSIS Act*, a complaint can be made to the Committee by:

- a person refused federal employment because a security clearance has been denied;
- a federal employee who is dismissed, demoted or transferred, or denied a promotion or transfer for the same reason; and
- anyone refused a contract to supply goods and services to the government for the same reason.

This quasi-judicial role as a complaint tribunal is of immediate interest to individuals who have their security clearances denied and are adversely affected in their employment with the Federal Government as a result. Of course, an individual cannot complain about the denial of a security clearance unless such a decision has been made known. In the past, there was often no requirement that the individual be so informed. The *Act* remedies this by requiring deputy heads or the Minister to inform the persons concerned.

Until the *CSIS Act* was promulgated, not only were many individuals unaware that they had been denied a security clearance, but even those who were informed were often not told why their applications had been denied. Now, the law requires the Committee to give each individual who registers a complaint as much information about the circumstances giving rise to the denial of a security clearance as is consistent with the requirements of national security. The Committee must then examine all facts pertinent to the case, make a judgement as to the validity of the decision taken by the deputy head, and then make its recommendations to the Minister and the deputy head concerned.

In another two cases, the Committee found that the delays took place in departments other than the Service, and where the Committee has no jurisdiction. In respect of the final complaint, we informed the complainant of the requirement to first submit his complaint to the Director of the Service. At the time of publication of this report, the complainant had written to the Director. He was dissatisfied with the Service's response and had again filed with the Committee.

Findings on 1996-97 security clearance complaints

The single complaint received by the Committee regarding security

clearances was directed at a department that performs its own security screening investigations. The Committee was informed by the department concerned that it had not in fact revoked or suspended the security clearance of the complainant, and we were assured that the complainant continued to hold a valid security clearance. Given the fact that the investigating agency was other than the Service, additional inquiries were beyond the Committee's jurisdiction.

Changes to Procedures in Respect of the Governor in Council

When the Committee receives a Ministerial Report, it investigates the grounds on which the report is based, then submits a full report to the Governor in Council.

In the case of an application for citizenship, the Governor in Council may issue a declaration to prevent the approval of any citizenship application for a two-year period. In regards to immigration applications, the Governor in Council may direct the Minister of Citizenship and Immigration Canada to issue a security certificate against a person and to proceed with the deportation of that individual.

During fiscal year 1996-97, the Minister of Citizenship and Immigration Canada introduced Bill C-84 in Parliament to amend the *Citizenship Act* and the *Immigration Act*. The amendments allow the Governor in Council to appoint a judge to replace the Committee, in the event that we are of the opinion that we cannot fulfill our mandate. The Bill contains an interim provision to cover court decisions that were rendered before the Bill came into effect.

Findings on 1996-97 Ministerial reports³⁴

Citizenship refusals

In our annual report last year, the Committee stated that it had received one Ministerial report pursuant to this section. At that time, SIRC's jurisdiction to investigate the matter was successfully challenged in the Federal Court, where it was held that there was a reasonable apprehension that the Committee would be biased in its investigation of the Ministerial report concerning the citizenship application of Mr. Ernst Zündel.³⁵ The Government launched an appeal to the Federal Court.

Deportation orders³⁶

The Committee received no Ministerial Reports of this type during 1996-97.

Persons appearing before the Immigration Appeal Division³⁷

During 1996-97 the Committee received one such report. In this case, the Immigration Appeal Division is unable to begin its review until the Governor in Council has made a decision on the Committee's report.

The Committee will be revisiting a case first heard by our late Chairman. He had determined that the subject of the complaint came within the class of persons described within paragraph 19(1)(g) of the *Immigration Act* as "persons who there are reasonable grounds to believe...are members of...an organization that is likely to engage in...acts of violence" that would or might endanger the lives or safety of persons in Canada, and thus are not admissible to Canada.

34. 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 the person's activity is part of a pattern of criminal activity punishable by way of indictment. See the *Citizenship Act* (section 19.1 onward).

35. *Zündel v. Minister of Citizenship and Immigration Canada*, Federal Court of Canada, Decision of Mr. Justice Heald, 1 August 1996.

36. A joint report signed by the Minister of Citizenship and Immigration Canada and the Solicitor General may be issued to the Committee when both Ministers are of the opinion, based on security or criminal intelligence reports

received and considered by them, that a permanent resident is a person described in the inadmissible classes of the *Immigration Act*. See the *Immigration Act* (section 39 onward).

37. A report signed by the Minister of Citizenship and Immigration Canada and the Solicitor General may be issued to the Committee when both Ministers are of the opinion, based on security or criminal intelligence reports received and considered by them, that a person who has lodged an appeal (against a deportation order) before the Appeal Division is a permanent resident described in the inadmissible classes of the *Immigration Act*. See *Immigration Act* [section 81(1) onward].

The most frequently requested security checks cover the person's life for a period of ten years prior to the application

The Federal Court of Canada subsequently ruled, however, that a portion of this same paragraph 19(1)(g) contravened the freedom of association assured by paragraph 2(d) of the *Charter of Rights and Freedoms* in a manner that is not demonstrably justified in a free and democratic society.

The Committee has subsequently been asked to determine whether the subject of the report, a permanent resident of Canada, is a person described in paragraphs 19(1)(e), 19(1)(g), and 27(1)(c) of the *Immigration Act* as they existed on 29 May 1992, and that portion of paragraph 19(1)(g) of the *Immigration Act* that remains in force and was not disputed by the Federal Court judgement.

A member of the Review Committee will re-examine the matter during the course of 1997-98.

Canadian Human Rights Commission referrals³⁸

The Committee received no referrals of this type for the year under review.

B. Security Screening Procedures within the Government of Canada

CSIS' role in security assessments

Pursuant to section 15 of the *CSIS Act*, the Service may conduct investigations in order to provide security assessments to:

- departments and agencies of the Federal Government (section 13 of the *Act*);
- the government of a foreign state (section 13 of the *Act*); and
- the Minister of Citizenship and Immigration Canada respecting citizenship and immigration matters (section 14 of the *Act*).

The Service conducts security screening investigations and provides security assessments for employees of the Public Service, as well as persons in the private sector who receive government contracts that involve classified work.³⁹

The requirements of a security assessment can vary, depending on the clearance level requested (confidential, secret, top secret). The most frequently requested security checks cover the person's life for a period of ten years prior to the application (five years in the case of access to secure government premises) or back to age sixteen, whichever comes first.

While it is the departments concerned that conduct initial criminal and credit checks, the Service cross-checks its own data base and conducts field investigations required (and interviews if necessary) for Level 3 clearances or "for cause."

38. 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. See section 45 (2) of the *Canadian Human Rights Act*.

39. The two exceptions are the employees of the Department of National Defence (DND) and the Royal Canadian Mounted Police

(RCMP) which conduct their own field investigations for employees requiring security clearances.

Security Screening in the Government of Canada

The Government Security Policy (GSP)⁴⁰ stipulates two types of personnel screening: a reliability assessment and a security assessment. Reliability checks and security assessments are conditions of employment under the *Public Service Employment Act* (PSEA).

Basic Reliability Status

Every department and agency of the Federal Government has the responsibility to decide the type of personnel screening it requires. These decisions are based on the sensitivity of the information and the nature of the assets to which access is sought. Reliability screening at the “minimum” level is required for those persons who are appointed or assigned to a position for six months or more in the Public Service, or for those persons who are under contract with the Federal Government for more than six months, and who have regular access to government premises. Those persons who are granted reliability status at the basic level are permitted access to only non-sensitive information (information which is not classified or designated).

Enhanced Reliability Status

Enhanced Reliability Status is required when the duties of a Federal Government position or contract require the person to have access to classified information or government assets, regardless of the duration of the assignment. Persons granted enhanced reliability status can access the designated information and assets on a “need-to-know” basis.

The Federal departments and agencies are responsible for determining what checks are sufficient in regard to personal data, educational and professional qualifications, and employment history. Departments can also decide to conduct a criminal records name check (CRNC).

When conducting the reliability assessments, the Federal Government organizations are expected to make fair and objective evaluations that respect the rights of the individual. The GSP specifies that “individuals must be given an opportunity to explain adverse information before a decision is reached. Unless the information is exemptible under the *Privacy Act*, individuals must be given the reasons why they have been denied reliability status.”

Security Assessments

The *CSIS Act* defines a security assessment as an appraisal of a person’s loyalty to Canada and, so far as it relates thereto, the reliability of that individual. A “basic” or “enhanced” reliability status must be authorized by the government department or agency prior to requesting a security assessment.⁴¹ Even if a person has been administratively granted the reliability status, that individual must not be appointed to a position that requires access to classified information and assets, until the security clearance has been completed.

40. Treasury Board of Canada, *Security Manual, Government Security Policy*, Chapter 2-4, “Personnel Security Standard.”

41. For contracts, the requirement to grant a basic or enhanced reliability check prior to requesting a security assessment does not apply.

...one of the key innovations of the *CSIS Act* was to require that the person subject to the request be informed should the application for clearance be denied

Statistics

In fiscal year 1996-97, the Service completed 1,135 field investigations and subject interviews. The Service's average response times to process security clearances during 1996-97 were 14, 23, and 101⁴² days respectively, for Government Security Policy levels I, II, III.⁴³

While the Service does not make security assessment recommendations for DND and the RCMP, on request it can conduct checks of its indices on behalf of the two agencies in order to assist in their security clearance investigations. Also at the request of DND and RCMP, the Service can seek the assistance of foreign agencies.

Committee findings

Rising numbers of security screening requests

The Committee notes with some surprise that despite government downsizing, the number of government security screening requests has increased in each of the last three years: 51,209 in 1994-95, 56,886 in 1995-96, and 63,605 for fiscal year 1996-97. While some of these requests were to update⁴⁴ or upgrade⁴⁵ existing security clearances, 35,440 were new applications. In contrast, the number of requests to downgrade clearances was minimal (68) for the same year.

Because of the manner in which the Service retains information about

the subjects of the requests, the breakdown in new requests between "indeterminate employees" and "contract employees" is unknown. There were 28,319 requests for access to government sites.

For the majority of requests, the Service's security assessment takes the form of a simple notice of assessment to departments. In fiscal year 1996-97, CSIS issued 63,594 notices.

Right of redress and right of review

As noted earlier in the description of the procedures in place for handling security clearance complaints (see inset page 44) one of the key innovations of the *CSIS Act* was to require that the person subject to the request be informed should the application for clearance be denied. The Committee continues to monitor the redress and review procedures.

Government employees⁴⁶ who wish to challenge a negative decision may do so through current grievance procedures in accordance with sections 91 and 92 of the *Public Service Staff Relations Act*. When a department denies a security clearance to external candidates and government employees, the Committee can review the matter; that is, a "right of review" is available to those affected. The procedure is also available to those persons who contract directly with the government, and who are denied a security clearance by a deputy head.

42. In previous years, the response times for the Airport program were included in the Level I clearances; hence the reason for the apparent increase in processing days from previous years. The average processing time for the "Airport Restricted Access Program and Accreditation" is one day.

43. GSP Levels: I (Confidential), II (Secret), III (Top Secret).

44. Departments must update an individual's enhanced reliability status, Level I and Level II security clearances once every ten years. Site access security clearances also must be updated every ten years. A Level III security clearance must be updated every five years. Of course, this regular update term does not preclude the department from reviewing a person's reliability status or from

asking the Service to reassess the security clearance "for cause." For the year under review, the Service has processed 7,401 requests for updates.

45. For the year under review, the Service processed 2,946 requests for upgrades. Upgrade requests are processed when the new duties or tasks of a person require that the individual have a higher level of screening than previously.

46. Persons from outside the Public Service (applicants and contractors), can complain to the Canadian Human Rights Commission, the Public Service Commission's Investigations Directorate, or the Federal Court, depending on the particulars of each case.

Of the 63,605 government security screening requests that CSIS processed in fiscal year 1996-97, ten were “information briefs”⁴⁷ and one was a “rejection brief”— the latter recommending denial of an individual’s security clearance. As of June 1997, that person had not submitted the matter to the Committee.

A similar pattern emerges when examining statistics for the previous year. In 1995-96, CSIS received 56,886 requests for security clearances. Of those, the Service issued thirty-nine information briefs and three rejection briefs. Again, none of the individuals involved applied to the Committee for a review of the decision.

The Committee’s jurisdiction is limited to evaluating activities and recommendations of CSIS. Thus, in the absence of a complaint by the affected party, SIRC remains unaware of decisions that

may or may not have been taken by Federal Government departments on the basis of CSIS information briefs.

The Committee’s mandate does allow us to ask the Service whether the departments concerned had endorsed the Service’s recommendations. CSIS replied that in two of the three cases, the departments had indeed acted on its recommendations. In the third, the Committee was informed that the recommendation to deny the clearance was never acted upon because the department chose not to hire the individual.

The Committee is concerned by the outcome of these and other similar cases in light of the clear intent of Government Security Policy when it comes to the individual’s right to redress and review.

In instances where a security clearance is explicitly denied, the Committee notes that section 42(1)

The Committee is concerned by the outcome of these and other similar cases . . .

Security Clearance Decisions – Loyalty and Reliability

Decisions by Federal departments to grant or deny security clearances are based primarily on the Service’s recommendations. Reporting to the Federal organization making the request, CSIS renders an opinion about the subject’s “loyalty” to Canada, as well as the individual’s “reliability” as it relates to loyalty. Government Security Policy stipulates that a person can be denied a security clearance if there are reasonable grounds to believe that,

“As it relates to loyalty, the individual is engaged, or may engage, in activities that constitute a threat to the security of Canada within the meaning of the *CSIS Act*.”

“As it relates to reliability, because of personal beliefs, features of character, association with persons or groups considered a security threat, or family or other close ties to persons living in oppressive or hostile countries, the individual may act or may be induced to act in a way that constitutes a ‘threat to the security of Canada’ or they may disclose, may be induced to disclose or may cause to be disclosed in an unauthorized way, classified information.”

47. An “information brief” sets out security concerns about the subject that do not meet the criteria for outright rejection. As such, an information brief is not a recommendation for the rejection of a clearance.

CSIS may enter into an arrangement with the government of a foreign state, a foreign agency, or an international organization

of the *CSIS Act* stipulates that it is the deputy head of a Federal Government department or agency who is responsible for informing employees of the denial of a security clearance. And we are also aware that it is Government policy to inform the persons refused of their right of redress.

Nevertheless, the apparent dearth of recommendations for denial (1 out of 63,605) and information briefs issued by CSIS, as well as the lack of information about what departments do with the information from the Service where no denial was recommended, will be the subject of future inquiries by the Committee.

Extended processing periods

Another issue arising from the three 1995-96 cases concerns the amount of time the Service took to provide the concerned departments with briefs: 26, 27, and 36 months, respectively. The Committee considers such lengthy periods to be excessive, particularly in the case where the Service required three years to respond to a request from a new applicant for a government position. We are aware, however, that delays may be caused by circumstances beyond the Service's control.

Security assessments for foreign states

CSIS may enter into an arrangement with the government of a foreign state, a foreign agency, or an international organization, to provide security assessments on Canadians and foreign nationals. The Service must receive the approval of the Solicitor General who, in turn,

consults the Minister of Foreign Affairs and International Trade. CSIS does not provide foreign agencies with recommendations concerning the suitability of a person to obtain a foreign security clearance.

In 1996-97, the Service received 806 foreign screening requests, and, among these, CSIS conducted 160 field investigations. The Service gave foreign clients 25 information briefs.

Advice to the Minister of Citizenship and Immigration

The Committee learned that the "Citizenship Security Flag System" referred to in past annual reports — effectively a mechanism which allowed the Service to alert the Department of Citizenship and Immigration in advance about certain individuals — is no longer in operation. The program provided Citizenship and Immigration Canada with the names and biographical data of permanent residents about whom the Service had identified security concerns. Identification by CSIS in this manner was cause for the government to closely examine the individual's applications for citizenship.

Since 1 January 1997, Citizenship and Immigration Canada employs a mail-in reporting system whereby all applications are processed by a Case Processing Centre in Sydney, Nova Scotia. Names of prospective citizenship applicants are sent from the Centre to the Service, then checked against the Service's security screening information

system data base. Most applications are processed in an expeditious manner; the balance requiring additional analysis by the Service are retained and assessed before the Service provides a recommendation to the citizenship authorities.

In 1996-97, the Service received 142,317 applications from Citizenship and Immigration, including 7,779 requests under the Refugee Determination Program, and 91,873 applications for citizenship. Of the citizenship applications, all but 39 were processed by 30 March 1997.⁴⁸

The Service completed 50,444 immigration requests in fiscal year 1996-97. Fifty percent of these cases were processed in under 42 days. The average response time for the remaining requests was 177 days. The Service rendered its advice for over 99 percent of all cases in less than one year.

Subject of a forthcoming review

In order to better understand the “client-service” relationship between CSIS and the government bodies responsible for citizenship and immigration, the Committee will conduct an in-depth review of CSIS’ role. The cooperation of Citizenship and Immigration Canada, the RCMP and immigration legal counsel outside of government, will be essential for the completion of this study.

⁴⁸. Resolution is still pending for an additional eighteen citizenship applications held over from previous years.

Section 3: CSIS Accountability Structure

The Service is an agency of the Government of Canada and as such, is accountable to government, Parliament and the people of Canada. Because of the serious and potentially intrusive nature of CSIS activities, the mechanisms set out in law to effect that accountability are both rigorous and multi-dimensional; there are a number of independently managed systems inside and outside the Service for monitoring CSIS activities and ensuring that they accord with its mandate.

It is part of the Security Intelligence Review Committee's task (the Committee itself being part of the accountability structure) to assess and comment on the functioning of the systems that hold the Service responsible to government and Parliament.

A. Operation of CSIS Accountability Mechanisms

Ministerial Direction

The *CSIS Act* requires the Committee to review Direction provided by the Solicitor General to the Service under subsection 6(2) of the *Act*. Ministerial Direction governs certain types of CSIS investigations in potentially sensitive areas such as investigations on university campuses. One of the Committee's major concerns is to identify the adequacy of Ministerial

Direction or lack of compliance with Direction that may lead to improper behaviour or violations of the *CSIS Act*. Three areas specifically play a role in the Committee's analysis: an examination of instructions issued by the Service based on Ministerial Direction; a review of the manner in which Directions were implemented in specific cases; and the identification of significant changes in the numbers of operations that require Ministerial approval.

In 1996-97 three new Ministerial Directions were brought to our attention.

National Requirements

Cabinet periodically provides general direction to CSIS about where it should focus its investigative efforts in the form of National Requirements from the Minister. A recent Direction, *National Requirements for 1995-97*, sets out priorities in five areas: counter terrorism, counter intelligence, security screening, "foreign intelligence support" and "transnational criminal activity."

The latter category represents a significant alteration of the previous requirements Direction issued in 1994-95 in that it instructs the Service to provide government with strategic assessments of transnational criminal activity that may impact on the security of Canada. In a related issue, CSIS was also directed to continue to provide criminal intelligence to Canadian law enforcement agencies under the provisions of section 19 of the *CSIS Act*.

In past Committee audits, we have expressed concern about the tardy

There are a number of independently managed systems inside and outside the Service for monitoring CSIS activities and ensuring that they accord with its mandate

provision of Ministerial Direction on *National Requirements*. The Direction — in effect a planning document — was not being issued before the end of the relevant year. The Minister elected to issue the *National Requirements* in a Direction that covered two fiscal years — 1995-96 and 1996-97. The Committee notes that the *National Requirements* for 1997-98 have been issued.

While the Committee was unable to comment in last year's report on the *National Requirements* applicable to that period because of their late issuance, we have identified no difficulties arising from that fact.

Information management

The Ministerial Direction on "Information Management" is intended to be a cumulative document, encompassing all previous Direction regarding the Service's management, retention, and destruction of files. The Direction also takes into consideration rapidly evolving information technologies.

Previous versions of the Information Management Direction from the Solicitor General specifically stated that "open information which does not meet the statutory tests for collection or retention should in future be held by CSIS quite separately and apart from investigative files." Upon review of the most recent Direction, the Committee noted that it did not contain this requirement.

In response to our query, the Ministry of the Solicitor General informed the Committee that the Direction omitted the requirement in order to allow CSIS time to discuss the policy and formulate its position on the issue.

The Ministry informed us that a new Direction on the retention of open source information is forthcoming.

Investigations on campus

Previous Ministerial Direction for "Investigations on Campus" required the approval of the Solicitor General for all CSIS operations on campus that could impact on the free flow of ideas associated with academic institutions. New Ministerial Direction reaffirms this principle, but states that the Director of CSIS can on his own approve source activities in specified circumstances, and must report his decisions to the Minister.

In a previous audit report, the Committee recommended that the Ministerial Direction governing investigations on campus be rewritten, and we note that the new Direction addresses Committee concerns about the terminology in the previous Direction not being consistent with the *CSIS Act*.

The Committee will monitor how the Service implements the new Direction.

Activities to overthrow by violence

Pursuant to Ministerial Direction issued in 1988, the Minister must approve any investigation of threats falling under what is commonly referred to as the "subversion" section of the *CSIS Act* — section 2(d), "activities directed toward...the destruction or overthrow by violence of the constitutionally established system of government in Canada." In 1996-97, the Solicitor General authorized no investigations in this regard.

In a previous audit report, the Committee recommended that the Ministerial Direction governing investigations on campus be rewritten. . .

... we believe that important policy instruments such as these should be placed in the official policy manual more quickly

Changes in Service operational policies and instructions to officers

Derived in part from the Service's interpretation of Ministerial Direction, the *CSIS Operational Policy Manual* is intended as a guide and operational framework for CSIS officers and employees. The Committee examines changes to the *Operational Policy Manual* as if they were changes to Ministerial Direction, and regards the manual as a useful tool in assisting our reviews of CSIS investigations.

In fiscal year 1996-97, the Service produced three new policies and several revisions:

- standardizing the format of threat assessments;
- cooperating with the Department of Citizenship and Immigration Canada; and
- obtaining premises for CSIS operations.

In the course of the Committee's assessment of the new Ministerial Direction on Information Management, the Service referred to an internal policy document we had not seen. Upon our request, CSIS provided the Committee with a copy of a "service wide" policy which had been in force since 1993. While the Committee found nothing in the policy with which to take issue, we believe that important policy instruments such as these should be placed in the official policy manual more quickly.

Disclosures of information in the public and in the national interest

Disclosures in the public interest

Section 19 of the *CSIS Act* prohibits the Service from disclosing information, except in specific circumstances. Under one circumstance, explicitly referred to in the *Act*, the Minister can authorize the Service to disclose information in the "public interest." The *Act* compels the Director of CSIS to submit a report to the Committee regarding all "public interest" disclosures; in 1996-97 there were none.

Disclosures in the national interest

Under the Service's interpretation of its mandate, it holds that acting as the Minister's agent, CSIS can also make special disclosures of information in the "national interest."⁴⁹ In such circumstances, the Solicitor General would determine whether the disclosure of operational information was in fact in the national interest, whereupon he would direct CSIS to release the information to persons or agencies outside government.

While the Committee was initially concerned about the implications of such special disclosures, a new CSIS policy stipulates that we will be informed whenever they take place. The Committee will examine future special disclosures on a case by case basis. There were none during the fiscal year 1996-97.

Governor in Council regulations and appointments

Under section 8(4) of the *CSIS Act*, the Governor in Council may make regulations concerning appointments

49. On occasion, in the course of its investigations, CSIS obtains information that does not fall within the Service's mandate, but which should be provided to the proper authorities as it is in the public interest. The Solicitor General must decide if the disclosure is essential to the public interest, and whether this interest clearly outweighs any invasion of privacy that could result. With the Minister's approval, CSIS may disclose this information to any Minister of the Crown or to a person in the Public Service of Canada. See section 19(2)(d) of the *CSIS Act*.

and other personnel matters. No such regulations were issued in 1996-97.

Annual report of the Director of CSIS

The CSIS Director's Annual Report to the Solicitor General (a top secret document) comments in some detail on the Service's operational activities for the preceding fiscal year. The Committee has among its key functions, the task of reviewing this report.

This year, we comment on two annual reports. In our audit report of 1995-96, the Committee was unable to comment on the Director's report of that same fiscal year since we received his report past the point for publication in our Annual Report for that year. As a result, we describe both the 1995-96 and the 1996-97 reports from the Director in this section.

Director's report for 1995-96

In the view of the Committee, the salient points of the Director's Annual Report of 1995-96, were the following:

- The Director stated that public safety remained the Service's principal concern, and noted that the main source of politically motivated violence is the "spillover of foreign conflicts into Canada" — a factor reflected in the fact that almost two-thirds of all CSIS investigations in 1995-96 were conducted by the Counter Terrorism Branch of the Service, rather than by Counter Intelligence.
- In 1995-96, Counter Intelligence Branch reported that some thirty

countries operate "against Canadian interests, within Canada or abroad." The Service was attempting to use the establishment of liaison relations as an incentive to encourage foreign intelligence services to cease their intelligence activities in Canada.

- CSIS is becoming increasingly involved in investigating transnational crime.
- To the end of March 1996, CSIS had decreased the average time required to process a "top secret" clearance for a government employee or contractor from 113 days to 84 days as a result of the implementation of a new automated system.
- Fiscal year 1995-96 marked the establishment of a new program called the Refugee Watch List. This internal program identifies persons who are considered to be security threats and who may seek refugee status or permanent residence in Canada, or attempt to obtain a sensitive position in the Federal Government.

The Committee has three comments about the Director's report:

First, we believe that where the Minister is not otherwise informed by the Service, the Director's Report should explain the significant and substantial departures from past CSIS practices and methods. If the reasons for the trends or changes are not apparent to us, we will seek explanations from the Service and, if not satisfied, the Committee will investigate further.

In 1995-96, Counter Intelligence Branch reported that some thirty countries operate "against Canadian interests, within Canada or abroad"

The Director could have provided more information about certain domestic extremism investigations

Second, absent from the report are discussions of important issues concerning the Service's operations. For example, the report does not address issues surrounding the impact of technology on Service activities.

Third, we found that the Annual Report was silent on the activities of the Analysis and Production Branch (RAP). RAP is an important operational branch and a major conduit for advice CSIS provides to the Federal Government. It would be helpful if in future, the Director would report on such Analysis and Production Branch activities as the quantity and types of intelligence reports it produces, requirements of the consumers of RAP information, and the feedback that RAP receives from them. CSIS says that when required, information of this type can be conveyed to the Minister by other means.

Director's report for 1996-97

In his 1996-97 Annual Report, the Director emphasized that Canada faces profound, and not entirely positive changes in the global security environment; an environment that has become more unstable and unpredictable in view of the fact that the activities arising from traditional threats have not gone away, and new types have emerged.

We found that the Director's 1996-97 Annual Report provides a satisfactory overview of CSIS' most important investigative activities. We also concluded, however, that the Service did not report, or did not report in sufficient detail, on two important areas.

First, the Director could have provided more information about certain

domestic extremism investigations. And second, the Director's report did not provide an assessment of the relationship between a certain state's hostile activities in Canada, and the impact on existing arrangements for cooperation with that country.

Certificate of the Inspector General⁵⁰

The *CSIS Act* [section 38(a)(i)] directs the Committee to review the Certificates issued by the Inspector General of CSIS. In his Certificate, the Inspector General assesses the Director's Annual Report and he also conveys the findings from his audits of the Service's operational activities. The Certificate is based in large part on the Inspector General's studies and consultation reports.

The Committee received the Inspector General's Certificate covering fiscal year 1994-95 in October 1996. We did not receive his Certificate for 1996 in time for review and publication in this Annual Report.

The Inspector General commented that he was satisfied that the Director's Annual Report (1994-95) "made a useful contribution to the Solicitor General's appreciation of CSIS operations and provided him with information of value in carrying out his oversight role." But the Inspector General's audit also found a number of inaccuracies and unsubstantiated statements in the Director's report.

Inspector General's observations

In his review of CSIS activities for 1994-95, the Inspector General made a number of observations and recommendations to the Solicitor General.

⁵⁰. See inset on page 19 for a description of the role of the Inspector General of CSIS.

The Inspector General concluded that the Minister received insufficient information from CSIS in the areas of section 16 operations, section 17 arrangements, and human source operations.

He recommended that for issue-based targeting, the Service should take special care to document the grounds on which it bases requests for authorization to investigate.⁵¹

The Inspector General also suggested that CSIS clearly specify how proposed joint operations with allied intelligence agencies fulfill the statutory duties and functions of the Service. CSIS, with the Minister's approval, sometimes runs intelligence operations in Canada with the assistance of allied intelligence services. He added that the Solicitor General may wish to give CSIS guidance on when and how he should be informed of the outcome of approved operations.

The Inspector General recommended that CSIS clarify the nature and limits of Security Liaison Officers (SLO) duties abroad, and that the Solicitor General should be informed beforehand if any extraordinary measures by the SLOs are to be taken. (See page 3 for a description and assessment of the foreign liaison program, and the role of SLOs).

The Inspector General commented on a number of other matters including, the provision of warnings or advice to the private sector, the Service's transmittal of information to the Department of Foreign Affairs and International Trade, and CSIS compliance with warrant conditions regarding solicitor-client communications. He

recommended that when the Service brings cases to the Solicitor General for a decision, it should be more explicit in linking the circumstances of each case to the governing authorities and relevant controls that apply.

Finally, the Inspector General objected to a CSIS decision not to provide him with certain documents on the grounds that they were administrative in nature.

Special reports of the Inspector General

While the Inspector General's Certificate is his principal method of reporting his findings, he may issue special studies from time to time. We were made aware of no special studies in 1996-97. Under section 40 of the *CSIS Act*, the Committee can itself request the Inspector General to conduct a special study or a review on our behalf. In 1996-97 we made no such requests.

Unlawful conduct

Under section 20(2) of the *CSIS Act*, the Director is to submit a report to the Minister when, in his opinion, a CSIS employee has acted unlawfully in the performance of his or her duties and functions. The Minister, in turn, must send the report with his comments to the Attorney General of Canada and to the Committee.

In 1996-97, there were no cases of unlawful conduct reported to the Attorney General or the Committee. Of the 13 previous referrals to the Attorney General, all but two have been resolved. The two outstanding cases date back to 1989 and 1990, respectively.

The Inspector General's audit also found a number of inaccuracies and unsubstantiated statements in the Director's report

⁵¹ As the Committee noted earlier, (page 17) issue-based targeting takes place when CSIS investigates a particular sector, such as economic espionage, rather than groups or persons.

The Committee Members met with officials from CSIS' Regional Headquarters in order to keep abreast of their operations and problems

SIRC consultations and inquiries

As noted earlier, the Committee is a key part of the CSIS accountability structure. In 1996-97 we undertook specific activities in this respect in the following areas:

Formal inquiries

During the fiscal year (1 April 1996 - 31 March 1997), we directed 141 formal inquiries to the Service. This number does not include inquiries arising out of complaints. The average time CSIS took to answer a formal inquiry was 44 days, a decrease from last year's average of 53 days.

Briefings

The newly-appointed Chair, Paule Gauthier, P.C., O.C., Q.C., met with the Director of CSIS in November 1996, and the Commissioner for the Communications Security Establishment (CSE) in December 1996. The Chair and Committee Members met with the Director of CSIS in May 1996, and in December 1996. These meetings are over and above the daily contact that our Research Staff has with the Service.

The Committee Members met with officials from CSIS' Regional Headquarters in Vancouver, Halifax, Ottawa, Montreal, and Toronto in order to keep abreast of their operations and problems.

SIRC activities additional to CSIS review

The Committee met with the Inspector General of CSIS in January 1997, and the Coordinator of Security and Intelligence in the Privy Council Office in February 1997.

Visiting dignitaries from other countries often ask to meet with Members of the Review Committee. In 1996-97, the Committee met with:

- Australia's Inspector-General of Intelligence and Security, and Australia's High Commissioner to Canada (August 1996);
- staff from South Africa's Joint Standing Committee on Intelligence (JSCI) and a security agency in that country (February 1997); and
- Poland's Minister Responsible for Security, who was accompanied by two security chiefs (March 1997).

The Deputy Executive Director addressed a conference of security officials from the North Atlantic Cooperation Council/Partners for Peace (NACC/PfP). Sponsored by the NATO Special Committee, the conference was held in Brussels in November 1996 and provided SIRC with a unique opportunity to share Canada's experience in reviewing the operations of a domestic security intelligence agency with the Western powers and the emerging democracies.

The Committee's Counsel/Senior Complaints Officer attended a series of conferences sponsored by the Canadian Bar Association and the Council of Canadian Administrative Tribunals in Toronto, Hull, and Vancouver. The conferences dealt with administrative law and immigration issues.

Special reports

Under section 54 of the *CSIS Act*, the Committee can issue special reports to the Solicitor General on any matter relating to the performance and functions of the Service. In 1996-97, we submitted no studies of this kind to the Minister. (A list of all SIRC studies to date can be found in Appendix B of this report.)

B. Inside the Security Intelligence Review Committee

In October 1996, the Honourable Paule Gauthier, P.C., O.C., Q.C. was appointed as Chair of the Committee,⁵² and the Honourable James Andrews Grant, P.C., Q.C. was appointed to replace her as a Member of the Committee.

Accounting to Parliament

The Committee appeared before the Sub-Committee on National Security on 15 May 1996 to respond to questions about the *Main Estimates* for fiscal year 1996-97.

On 24 October 1996, the Solicitor General tabled the Committee's 1995-96 Annual Report in Parlia-

ment. Although it is the Minister who tables the Committee's report in the House of Commons, he has no authority to edit or otherwise alter the Committee's document.

The Committee was invited to appear before the Sub-Committee on National Security on 3 December 1996 to answer questions concerning its 1995-96 Annual Report. During this appearance, the Chair stated that she hoped that in future, "the relationship between the Sub-Committee and SIRC becomes one of mutual trust."

The Committee again appeared before the Sub-Committee on National Security on 15 April 1997, to answer questions about the 1997-98 *Main Estimates*.

Staying in touch with Canadians

Research Staff attended the Intelligence Studies Section at the annual conference of the International Studies Association (ISA), held in Toronto in March 1997. They also participated in the conference and annual general meeting of the Canadian Association for Security and Intelligence Studies (CASIS) held at the same time.

Although it is the Minister who tables the Committee's report in the House of Commons, he has no authority to edit or otherwise alter the Committee's document

Table 4
SIRC budget 1996-97

	1996-97	1995-96
Personnel	805,000	799,000
Good and Services	598,000	616,000
Total Operating Expenses	1,403,000	1,415,000

Source: 1996-97 Estimates, Part III, Section II.

52. Mme Gauthier had been a Member of the Committee since 8 June 1995, and had previously served from 1984 to 1991.

SIRC opened its official site on the Internet in late October 1996 — www.sirc-csars.gc.ca.

SIRC on the internet

To provide information about the Committee and its work to a wider audience, SIRC opened its official site on the Internet in late October 1996 — www.sirc-csars.gc.ca. To date, the Web site has been visited over eighty-five thousand times.

Our Web site explains the mandate of the Committee and provides information on SIRC's activities, biographies of the Committee Members, full versions of recent annual reports, lists of SIRC studies, recent changes to legislation that impact on the Committee, and a search procedure to allow visitors to find information on specific subjects.

The site also informs the visitor about how to file complaints to the Committee under sections 41 and 42 of the *CSIS Act*, and has links to other Internet sites we believe will be of interest to visitors; among these are Parliament, the Privacy Commissioner, and the Access to Information Commissioner.

Impact of budget changes

SIRC has reduced its spending levels since 1991-92, and will continue to do so over the next two fiscal years. Although the reductions have not been large in absolute terms, they are significant for a small organization with little budget flexibility.

Figure 1 understates the degree to which the Committee's budget has been reduced because commencing in 1995-96, translation services (\$50,000) are now included in SIRC's reference levels. Prior to 1995-96, these services were provided gratis through the Translation Bureau, Secretary of State.

Adapting to budget restraint

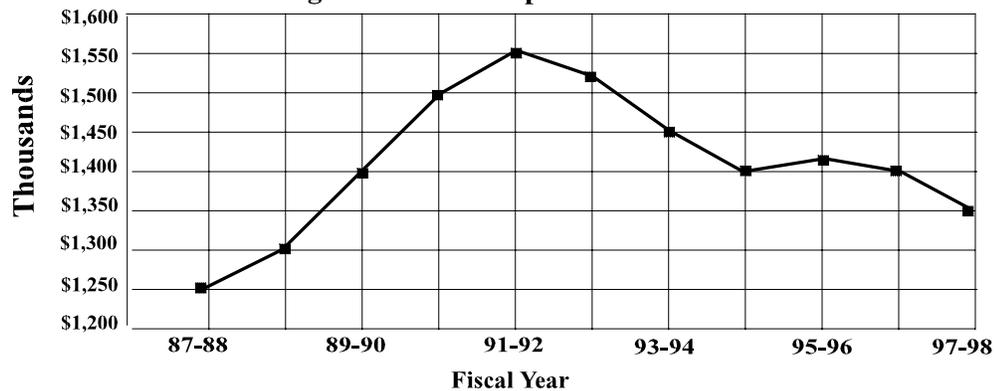
Government-wide budget reductions at SIRC have had an impact on the Committee's activities. The investigation of complaints is the most expensive area of discretionary spending for the Committee, and must, therefore, bear the brunt of the budget cuts. To deal with the reductions, the Committee is doing more work in house, and using outside lawyers less. While undertaking this and other measures, the Committee is determined to avoid increasing the time required to handle complaints, and to maintain the quality of its reports.

The review area is also being affected by budget reductions. As with complaints, more work is being done internally, and the Committee is employing fewer contract research consultants. In addition, SIRC has reduced the funding for seminars. Instead, we rely more on one-to-one meetings with academics and other experts.

In 1997-98, the Committee will increase its productivity by reassigning two positions from the General Administrative or support category to the Research section. This should increase the Research section's output by one third at minimal extra cost.

The Committee believes that all of these steps combined, 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.

Figure 1: SIRC Expenditures 1987-1998



Personnel

The Committee has a small total staff of fourteen: an executive director, a counsel/senior complaints officer to handle complaints and ministerial reports, a deputy executive director, a director of research, a project leader, and five research officers, one of whom is responsible for liaison with the media, an administrative officer who is also the Committee registrar for hearings, and an administrative support staff of three to handle the sensitive and highly classified material using special security procedures.

Reorganization and increased productivity

Effective 1 April 1997, the Committee restructured its research function to use its resources more efficiently. The Committee has integrated all research resources under a deputy executive director to more closely mirror the current deployment of resources within CSIS, and to effectively manage the intensive research program.

To recognize the contributions of the Senior Complaints Officer and the Committee's increased reliance on in-house legal resources for handling complaints cases, Sylvia MacKenzie was appointed as the Counsel and Senior Complaints Officer, effective 1 April 1997.

The Committee decides formally at its monthly meetings the research and other activities it wishes to pursue, and sets priorities for the staff. Day-to-day operations are delegated to the Executive Director with direction when necessary from the Chair in her role as the Chief Executive Officer of the organization.

... all of these steps combined, will allow SIRC to maintain or improve the performance of its responsibilities to Parliament and the public at lower cost

GLOSSARY

ARAACP	—	Airport Restricted Area Access Clearance Program
CIC	—	Citizenship & Immigration Canada
CI	—	Counter Intelligence
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
RTA	—	Request for Targeting Authority
SERVICE	—	Canadian Security Intelligence Service (CSIS)
SIGINT	—	Signals Intelligence
SIRC	—	Security Intelligence Review Committee
SLO	—	Security Liaison Officer
TARC	—	Target Approval and Review Committee

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)

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)

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

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)

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)

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)

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

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

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

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

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

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

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

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

- CSIS Activities Regarding Native Canadians — A SIRC Review*, January 1991 (SECRET) * (90/91-07)
- Security Investigations on University Campuses*, February 1991 (TOP SECRET) * (90/91-01)
- Report on Multiple Targeting*, February 1991 (SECRET) (90/91-08)
- 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)
- East Bloc Investigations*, August 1991 (TOP SECRET) (91/92-08)
- Review of CSIS Activities Regarding Sensitive Institutions*, August 1991 (TOP SECRET) (91/92-10)
- CSIS and the Association for New Canadians*, October 1991 (SECRET) (91/92-03)
- Exchange of Information and Intelligence between the Canadian Security Intelligence Service & Canadian Security Establishment*, 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)
- The Attack on the Iranian Embassy in Ottawa*, May 1992 (TOP SECRET) * (92/93-01)
- “STUDYNT” The Second CSIS Internal Security Case*, May 92 (TOP SECRET) (91/92-15)
- Domestic Terrorism Targets — A SIRC Review*, July 92 (TOP SECRET) * (90/91-13)
- CSIS Activities with respect to Citizenship Security Screening*, July 92 (SECRET) (91/92-12)
- The Audit of Section 16 Investigations*, September 92 (TOP SECRET) (91/92-18)
- CSIS Activities during the Gulf War: Community Interviews*, September 92 (SECRET) (90/91-12)
- Review of CSIS Investigation of a Latin American Illegal; a SIRC Review*, 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)
- The Assault on Dr. Hassan Al-Turabi: A SIRC Review of CSIS Activities*, 25 May 93 (SECRET) (92/93-07)
- Domestic Exchanges of Information (A SIRC Review — 1991/92)*, November 92 (SECRET) (91/92-16)
- Prairie Region Audit*, January 93 (TOP SECRET) (90/91-11)
- Sheik Rahman's Alleged Visit to Ottawa*, May 1993 (SECRET) (CT 93-06)
- Regional Audit, September 1993* (TOP SECRET)
- A SIRC Review of CSIS' SLO Posts (London & Paris)*, September 1993 (SECRET) (91/92-11)
- The Asian Homeland Conflict*, September 1993 (SECRET) (CT 93-03)
- Intelligence - Source Confidentiality*, November 1993 (TOP SECRET) (CI 93-03)
- Domestic Investigations (1)*, December 1993 (SECRET)(CT 93-02)
- Domestic Investigations (2)*, December 1993 (TOP SECRET) (CT 93-04)
- Middle East Movements*, December 1993 (SECRET)(CT 93-01)
- A Review of CSIS' SLO Posts (1992-93)*, December 1993 (SECRET) (CT 93-05)
- Review of Traditional CI Threats*, December 1993 (TOP SECRET) (CI 93-01)

- 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)
- The Audit of Section 16 Investigations and Foreign Intelligence Reports*, May 1994 (TOP SECRET) (CI 93-11)
- Sources in Government*, June 1994 (TOP SECRET) (CI 93-09)
- Regional Audit*, July 1994 (TOP SECRET) (CI 93-02)
- The Proliferation Threat*, December 1994 (SECRET) (CT 93-07)
- The Heritage Front Affair. Report to the Solicitor General of Canada*, December 1994 (SECRET) (CT 94-02)*
- A Review of CSIS' SLO Posts (1993-94)*, January 1995 (SECRET) (CT 93-09)
- Domestic Exchanges of Information (A SIRC Review 1993-94)*, January 1995 (SECRET)(CI 93-08)
- The Proliferation Threat - Case Examination*, January 1995 (SECRET) (CT 94-04)
- Community Interviews*, March 1995 (SECRET) (CT 93-11)
- An Ongoing Counter-Intelligence Investigation*, May 1995 (TOP SECRET) (CI 93-07)*
- Potential for Political Violence in a Region*, June 1995 (SECRET) (CT 93-10)
- A SIRC Review of CSIS' SLO Posts (1994-95)*, September 1995 (SECRET) (CT 95-01)
- Regional Audit*, October 1995 (TOP SECRET) (CI 93-10)
- Terrorism and a Foreign Government*, October 1995 (TOP SECRET) (CT 94-03)
- Visit of Boutros Boutros-Ghali to Canada*, November 1995 (SECRET) (CI 94-04)
- Review of Certain Foreign Intelligence Services*, January 1996 (TOP SECRET) (CI 94-02)
- The Audit of Section 16 Investigations and Foreign Intelligence Reports*, February 1996 (TOP SECRET)(CI 94-01)
- Domestic Exchanges of Information (A SIRC Review 1994-95)*, February 1996 (SECRET)(CI 94-03)
- Alleged Interference in a Trial*, 27 February 1996 (SECRET) (CT 95-04)
- CSIS and a "Walk-In"*, March 1996 (TOP SECRET) (CI 95-04)
- Investigation of a Foreign State's Intelligence Services*, 28 October 1996 (TOP SECRET) (CI 95-02)
- The Audit of Section 16 Investigations and Foreign Intelligence Reports*, 7 February 1997 (TOP SECRET) (CI 95-05)
- Regional Audit*, 16 May 1997, (TOP SECRET) (CT 95-02)
- A Review of Investigations of Emerging Threats*, 20 June 1997 (TOP SECRET) (CI 95-03)
- Domestic Exchanges of Information*, 23 July 1997 (SECRET) (CI 95-01)
- Homeland Conflict*, 13 August 1997 (TOP SECRET) (CT 96-01)

LIST OF RECOMMENDATIONS

SECTION 1: A REVIEW OF CSIS INTELLIGENCE ACTIVITIES

A. AREAS OF SPECIAL INTEREST FOR 1996-97

CSIS Liaison Program with Foreign Agencies

We recommend, therefore, that the Procedures Manual be brought up to date, and that it cover important post issues that are not addressed elsewhere.

We recommend, however, that when an SLO decides to disclose adverse open information about Canadians to a foreign agency, the SLO be required to first consult with management at CSIS Headquarters.

We recommend that the Service revise, or at least better define, its system of evaluating the reliability of foreign agencies.

Economic Espionage

We recommend that administrative information collected from the Liaison/Awareness Program be retained in a non-section 12 data base.

B. ANNUAL AUDIT OF CSIS ACTIVITIES IN A REGION OF CANADA

We believe that CSIS should obtain the Solicitor General's approval to exchange information with or otherwise cooperate with government departments and agencies with which it does not have formal arrangements.

Consequently, the Committee recommends that unless there are specific operational considerations that preclude it, the Service should in future inform Federal departments concerned about the conclusions it has drawn about Federal employees investigated.

The Committee recommends that source recruitment assessments involving persons who are not targets not be retained as part of the Service's section 12 data base.

The Committee recommends that the definition of community interview programs be clearly set out in CSIS policy.

C. INSIDE CSIS

We recommend, therefore, that the Service review and set out policy which addresses gaps in current policy pertaining to information exchanges with police agencies in relation to advocacy, protest, and dissent.

We recommend, therefore, that the Service take the necessary measures to ensure that section 12 and section 15 investigations are clearly distinguishable, and, where they may of necessity overlap, ensure that all the applicable tests and controls are in place.

We recommend that CSIS clarify its policy in regard to the "strictly necessary" requirement when assessing whether to retain identifying information from foreign intelligence in the Service's computerized data base.

COMPLAINT CASE HISTORIES

This section describes complaint cases submitted during the past year to the Committee under Section 41 of the *CSIS Act*, and concerning which the Committee had reached decisions. Not reviewed here are complaints that were the subject of administrative reviews and the nine complaints about the length of time taken by the Service to provide advice to the Department of Citizenship and Immigration Canada (CIC).

Complaints about security screening interviews

Interviews are one of the procedures employed by CSIS to assess immigration and other applicants, and it is the view of the Committee that interviews conducted by CSIS investigators can identify security related concerns only if the interviews are conducted skillfully and all possible security issues are discussed.

Conducted appropriately, interviews can also provide applicants with the opportunity to address security issues.

Investigators who conduct the interviews do not make decisions about the status of applicants. A different section in CSIS analyses the interviews, as well as information from other sources, and the results are presented in the form of briefs to Citizenship and Immigration Canada (CIC). The ultimate decision to grant or refuse an application is made by CIC.

The Committee received two complaints about alleged impropriety in regard to interviews conducted by CSIS investigators. While the Committee was cognizant of the length of time that had lapsed before CIC requested the Service's advice, we made the complainants aware of the fact that the Committee's jurisdiction when assessing whether any undue delay has occurred is limited to the actions of CSIS alone.

We concluded that neither complaint was valid. In one case worthy of note, the complainant had alleged that an investigator demonstrated "personal bias" against him during an interview. We found that this allegation was not supported by the evidence. Instead, we observed that the investigator had adopted a professional and objective approach to the assignment.

A complaint in respect to an airport interview

As a result of our investigation, we were satisfied that the Service had not used its powers in an illegal or inappropriate fashion when it had conducted an interview. We concluded that the interviewee participated voluntarily in the interview.

A complaint about sharing information with an employer

In 1995, a person was transferred to another unit within the organization that employed him — an organization that shares information with CSIS. The complainant asserted that he was told that he was being transferred as a result of information that had come to the attention of his supervisor from the Service. CSIS personnel had attempted in previous years to interview the complainant and his refusal to be interviewed had left the Service with a negative perception of the complainant.

The Service maintained that it had never told the employer that it would cease to share information if the complainant remained in the unit, and, that in 1995, it had told the employer that it knew nothing to suggest that the complainant was a security risk or that he was anything other than a loyal Canadian. The Service noted to the Committee that in its view, the matter of the job transfer within the other organization was beyond its purview.

After examining the information provided by the Service to the employer, the Committee concluded that the complaint was justified and that CSIS personnel failed to disseminate the information in its possession in an objective, responsible, and professional manner. The Service has the obligation not only to accurately observe and record the facts that it collects, it must also be fair and objective when it reports such information to others.

Except to the extent that CSIS may have influenced the actions of the organization concerned, the Committee's jurisdiction does not encompass the activities of the body for which the complainant

worked. We have, however, recommended to the Service that it share in a clear and unreserved manner with senior management in the complainant's organization, its conclusion that the complainant did not attempt to conceal intelligence activities and does not constitute a threat to the security of Canada.

A delicate balance

The Committee reviewed a complaint about CSIS from a person whose status in Canada was undetermined.

This case drew the Committee's attention to the possibility that the Service could take unfair advantage of persons who would prefer not to provide assistance to CSIS, but who are concerned that failure to cooperate would adversely affect their chances of obtaining residence in Canada. Of equal concern is the possibility that persons approached by CSIS at an early stage in the immigration process could come to believe that their chances of securing status in Canada would be improved by cooperating.

In this particular case, the Committee found the complaint justified.

Complaints about a CSIS interview

To fulfill its duty to report to government on activities that may, on reasonable grounds, be suspected of constituting threats to the security of Canada, the Service depends on the information of members of the public who may have knowledge of, or opinions on, activities relating to threats to the security of Canada, including politically motivated violence – information often obtained through personal interviews.

The Committee investigated complaints concerning an interview conducted by the Service and recorded by the interviewee. While we were satisfied that the interview fell within the legislative mandate of the Service, two statements made by the investigators during the course of the interview caused some concern.

At one point in the interview, an investigator referred to CSIS as "the political police." The investigator told the Committee that it was the first time he had ever used the phrase and assured us that he would never use it again. He explained that he was attempting to draw

an analogy with a foreign agency whose mandate resembled the Service's in that it investigated politically motivated violence.

While the Committee regards the investigator's particular choice of words as unfortunate, we also are convinced, based on a reading of the entire exchange, that he well understood the overall mandate and purpose of the Service, and furthermore, that he attempted to convey this information to the interviewee.

With respect to a statement made by the other investigator involved, the Committee believes that it is reasonable to expect more restraint and professionalism from CSIS officers than was illustrated in this instance. We acknowledge the fact that interviews are often an effective means of collecting information and intelligence, and that a sometimes useful interview technique involves the employment of leading statements.

The Committee believes, however, that such techniques should never include statements that are not placed in the proper context, or adverse allegations about groups or individuals that are not supported by the facts.