

The Service has informed SIRC that it is in the process of incorporating the conflict of interest guidelines into its policy.

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 analyze 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. The data can reveal significant areas of investigative activity, as well as suggest areas where the investigative effort is disproportionate to the threat under investigation.

Section 2(d) Investigations

The Minister must approve any investigation by CSIS under section 2(d) of the *CSIS Act*, often referred to the "subversion" clause.

The Minister authorized no such investigations in 1997-98.

Investigation Categories

Last year, the Committee noted that in the counter intelligence area, CSIS was using a system that effectively detracted from our ability to compile and analyze the necessary statistics. The system employed vague categories such as "political espionage" that did not describe the particular threat being investigated. While the Service continues to use these definitions, it has provided the Committee with detailed information aggregated by nation. Useful analysis is still very difficult, nevertheless, our researchers have managed to compile estimates and aggregate data which adequately describe the threats to Canada in the counter intelligence area.

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.

We compile statistics based on a quarterly review of all warrant affidavits and warrants granted by the Federal Court. Several kinds of information are tracked annually, such as the number of persons and number of locations subject to warrant powers. This format continues a practice established prior to the

The kinds of warrants granted and the nature of the targets listed provide insight into the entire breadth of CSIS investigative activities

The Service has informed SIRC that it is in the process of incorporating the conflict of interest guidelines into its policy.

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 analyze 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. The data can reveal significant areas of investigative activity, as well as suggest areas where the investigative effort is disproportionate to the threat under investigation.

Section 2(d) Investigations

The Minister must approve any investigation by CSIS under section 2(d) of the *CSIS Act*, often referred to the "subversion" clause.

The Minister authorized no such investigations in 1997-98.

Investigation Categories

Last year, the Committee noted that in the counter intelligence area, CSIS was using a system that effectively detracted from our ability to compile and analyze the necessary statistics. The system employed vague categories such as "political espionage" that did not describe the particular threat being investigated. While the Service continues to use these definitions, it has provided the Committee with detailed information aggregated by nation. Useful analysis is still very difficult, nevertheless, our researchers have managed to compile estimates and aggregate data which adequately describe the threats to Canada in the counter intelligence area.

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.

We compile statistics based on a quarterly review of all warrant affidavits and warrants granted by the Federal Court. Several kinds of information are tracked annually, such as the number of persons and number of locations subject to warrant powers. This format continues a practice established prior to the

The kinds of warrants granted and the nature of the targets listed provide insight into the entire breadth of CSIS investigative activities

Table 1
New and Renewed Warrants

	1995-96	1996-97	1997-98
New Warrants Granted	32	125	72
Warrants Renewed/Replaced	180	163	153
Total	212	288	225

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

Committee Findings

While the data provides the Committee with an excellent profile of the Service's use of warrant powers in a given year, comparisons year-to-year are less enlightening because the very nature of the affidavits alters over time as a result of legal decisions by Courts and new developments in technology. In addition, raw warrant numbers can be misleading since one warrant can authorize the use of a power against one or many persons, the Federal Court can require changes to affidavits, and decisions as to what constitutes a new warrant or a renewal/replacement of the warrant can vary according to the Service officer making the decision.

Despite these variables, however, the Committee concluded that measured overall, CSIS' exercise of warrant powers in 1997-98 was consistent with previous years: the number of persons affected by CSIS warrant powers decreased slightly and

foreign nationals continue to be the majority of persons subject to warrant powers.

Regulations

Under section 28 of the *CSIS Act*, the Governor in Council may issue regulations governing how CSIS applies for warrants. In 1997-98, no such regulations were issued.

Federal Court Warrant Conditions and Other Developments

All warrants authorized by the Federal Court contain conditions which limit the use of warrant powers and which the Service must follow in their execution. In 1997-98, the Federal Court instructed CSIS to change several conditions:

- significantly broadened were some conditions that define the types of information CSIS can retain from mail intercepts;
- the definition of who is covered by the condition concerning solicitor-client communications was broadened;
- the Court articulated specific rules governing the Service's destruction of

electronic and paper-based records it collects; and,

- a ruling on a specific warrant would appear to have the effect of eliminating future use of the “reasonable grounds to believe” statement by senior service officials in certain kinds of warrant affidavits.

In 1997-98, the Federal Court denied a small number of warrant applications. The Committee is looking into the possible ramifications of these decisions on the operational activities of CSIS and we will comment in our next annual report.

The McGillis Decision

In August 1997, CSIS applied for a warrant from the Federal Court to enable it to investigate a threat to the security of Canada. The application included a request for the inclusion of various clauses. On 19 September 1997, Madame Justice Donna McGillis of the Federal Court declared that a proposed clause in the CSIS warrant application was illegal and dismissed the Service’s application to include it in the warrant before her. Her Reasons for Order were made public on 3 October 1997.¹²

The clause at issue is known as the “visitor’s clause,” which permitted CSIS to use, at any place, the full range of powers granted in the warrant against foreign nationals not named in the warrant, if those persons met three criteria:

- they had entered Canada as visitors;
- they were identified in CSIS records, as of the date of the warrant, as intelligence

officers of a country or known members of a terrorist group; and,

- they were persons a CSIS officer at the Director General level had reasonable grounds to believe would engage in threat-related activity while in Canada.

In her Reasons for Order, Madame Justice McGillis stated that the range of the “visitor’s clause” extended significantly beyond that of either the “resort to”¹³ and “basket”¹⁴ clauses, also included in the warrant. She concluded that the “visitor’s clause” constituted an unlawful delegation to a Service employee, who acts in an investigative capacity, of the functions accorded to a judge under paragraph 21(2)(a) and subsection 21(3) of the *CSIS Act*, thus offending the minimum constitutional requirement in *Hunter et al. v. Southam Inc.*¹⁵

Following Justice McGillis’ ruling, CSIS informed the Committee that it had immediately ceased implementing the “visitor’s clause” in all warrants where it appeared. The clause would also be removed in outstanding warrants as they came up for renewal. SIRC was aware of the presence of the “visitor’s clause” in past CSIS warrants. In instances where the clause had been invoked, the Committee ensured that CSIS had respected the conditions of the clause, and that it had not been applied to Canadians.

The Committee regards the approval of warrants as the sole prerogative of the Federal Court. However, we consider it to be our responsibility to ensure that affidavits before the Court — presented by the Service in accordance with paragraph 21(2)

Our review also serves to ensure that CSIS rigorously observes the conditions that are imposed by the Court on the Service’s use of the warrant powers granted

of the *CSIS Act* — fully reflect the facts of the case. Our review also serves to ensure that CSIS rigorously observes the conditions¹⁴ that are imposed by the Court on the Service's use of the warrant powers granted.

CSIS Operational Branches

The Service has four operational branches: Counter Terrorism, Counter Intelligence, Analysis and Production, and Security Screening.

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. Various domestic extremist groups are also regarded as potential threats to the security of Canada because of their capacity to foment violence.

For fiscal year 1997-98, CT Branch made a number of structural changes that resulted in the redeployment of additional resources to deal with emerging terrorist threats.

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 1997-98, CT branch produced 557 threat assessments, an increase of 17 from last year's total of 540. 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.

Counter Intelligence (CI) Branch

The Counter Intelligence Branch monitors threats to national security stemming from the espionage activities of other national governments' intelligence operations. At CSIS headquarters, the CI Branch must adapt its program to changes in the threat environment, and to the intelligence requirements of its clients. The regional offices must also demonstrate flexibility at the operational level by focusing on high priority targets, and those targets that offer the greatest opportunity for meeting national security objectives.

By the middle of this decade, 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. The Service has signed arrangements with some former and sometimes current adversaries with the aim of encouraging such agencies to act with more "transparency", and in order to seek out common ground for cooperation and information sharing.

The changing international environment has required the CI Branch to focus on several new threats. One new priority is the potential vulnerability of Canada's electronic infrastructure. With high and growing reliance on electronic information, Canada, like other industrialized nations, is open to attacks of a sufficient gravity as to constitute a serious threat to security. Physical or electronic assaults against computer-based information systems can destroy, alter or result in the theft of information. In cooperation with other elements of Canada's security intelligence system, CI Branch has programs for assessing and countering such threats.

Another area of increased attention is transnational crime, which the Branch addressed by establishing the transnational criminal activities section in 1996.¹⁷ In 1997-98, a new geographical area became a focus of this section's attention and resources.

Analysis and Production (RAP) Branch

RAP is the Service's research arm, and as we noted last year, the Branch has recently undergone significant structural change. In 1997-98, the organizational changes continued with the aim of better reflecting the main operational branches of the Service. Toward this end, RAP realigned its Public Safety Section to work closely with the Counter Terrorism Branch, and the National Security Section was partnered with the Counter Intelligence Branch. RAP also augmented its production through the use of new technologies.

In the course of the reorganization, RAP evolved from a geographical to a functional

orientation so that RAP analysts could focus more effectively on one threat-related field. In the past, analysts who worked in a geographical unit would be responsible for producing assessments on all elements (terrorism and espionage) of threat-related activity occurring within that region. Analysts will now focus their efforts in order to develop greater depth of knowledge and expertise in a single field. Another major development was the integration of the operational and strategic analysis groups, this according to the Service, in order to ensure that those with complementary skills worked more closely together.

The RAP Government Liaison Unit, created in 1992, is the mechanism by which CSIS identifies government requirements. As RAP is the only multi-disciplinary operational branch in the Service, it has been tasked by the CSIS Executive with responsibility for the production of Memoranda to Cabinet, the Director's Annual Report to the Minister, and the CSIS Annual Public Report.

We will conduct a study of the Analysis and Production Branch in fiscal year 1998-99 and comment in our next annual report.

Security Screening Branch

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 and provincial governments (section 13 of the *Act*);

One new priority is the potential vulnerability of Canada's electronic infrastructure

- 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*).

[SIRC gathers and compiles statistics about CSIS security screening activities. For details, please see Appendix E.]

Security Assessments and the Department of National Defence

While 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, until recently, two institutions of government conducted their own security screening: the Royal Canadian Mounted Police (RCMP) and the Department of National Defence (DND). As of 1 July 1998, CSIS assumed the responsibility for security clearances for DND as well.¹⁸

The Service estimates that some 12,000 requests will be forwarded by DND to CSIS, and the Service has recruited and trained new staff to conduct investigations out of regional offices related to DND employees. CSIS has not been approached to conduct the security clearances for the RCMP, nor is the Committee aware of any such initiative.

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. CSIS does not provide foreign agencies with recommendations concerning the suitability of a person to obtain a foreign security clearance.

In 1997-98, the Service received a total of 1,756 foreign screening requests, and, among these, CSIS conducted 171 field investigations. The Service provided 20 briefs to foreign clients.

Information and Advice to the Minister of Citizenship and Immigration¹⁹

Immigration and refugee applications from within Canada for permanent residence
CSIS has the sole responsibility for screening immigrants and refugees²⁰ who apply for permanent residence from within Canada. CIC forwards the vast majority of these applications directly to CSIS for screening via an electronic data link from the CIC's Case Processing Centre (CPC) in Vegreville, Alberta.

Immigration and refugee applications from outside Canada for permanent residence
Immigration and refugee applications for permanent residence that originate outside of Canada are managed by the Overseas Immigrant Screening Program. Under this Program, CSIS shares the responsibility for the security screening process with CIC officials abroad, usually the Immigration Program Managers.

CSIS only becomes involved in the immigration screening process if requested to do

so by an Immigration Program Manager or upon receipt of adverse information about a case from established sources. This approach allows the Service to concentrate on the higher risk cases. The number of referrals to CSIS represents approximately 20 percent of the national volume; in 1996-97, some 215,000 applications.

Enforcement action under the Immigration Act²¹

The Service provides information and advice generally to CIC for the purpose of preventing the entry into Canada of persons who pose a security threat. There are two programs that deal specifically with individuals who can be subject of enforcement action under the *Immigration Act*: the Enforcement Information Index (EII) and the Point of Entry Alert system.²²

The Service's assistance is further subdivided by the form it takes: (a) information-sharing through the CIC data banks, the Enforcement Information Index, and the Point of Entry Alert System; and (b) information, advice, and assistance in the conduct of interviews with people who are detained under the *Immigration Act* or "interdicted" at a point of entry.

Enforcement Information Index²³

The EII program is designed to warn immigration officials abroad and alert officials at Canada's points of entry about persons who may pose a security threat. Under this program, CSIS provides basic identifying data about individuals who could be the subject of enforcement action.

Individuals detained under the Immigration Act

Under the *Immigration Act*,²⁴ a person seeking entry into Canada may be detained by CIC up to seven days at the point of entry. This may occur where the Deputy Minister of Immigration has reason to believe that the person is inadmissible on security grounds under the *Immigration Act*.

The purpose of the Service's assistance is to provide information and advice to CIC in support of the detention of a person on security grounds. The goal is to contain a potential threat or detain the individual pending further investigation by the Service. The Service is often expected to react quickly²⁵ since the objective is to obtain a voluntary departure, issue an exclusion order, or prepare a security certificate.²⁶

The Point of Entry Alert (interdiction program)

Linked to the Enforcement Information Index program, CSIS (through CIC and Revenue Canada) can issue a point-of-entry alert for any person of security concern whose arrival in Canada is thought to be imminent. The purpose is to allow CIC and Customs officials to determine that person's admissibility.

The CSIS Refugee Watch List

Quite apart from assistance to CIC, the Committee notes that during the fiscal year 1995-96 CSIS created a new internal process to signal the arrival as refugees or immigrants of those persons who are of concern to CSIS. Should the individual require a security clearance or immigration status, the individual is identified and reviewed by CSIS. In 1995-96, seventy-nine

The EII program is designed to warn immigration officials abroad and alert officials at Canada's points of entry about persons who may pose a security threat

The purpose of the Service's assistance is to provide information and advice to CIC in support of the detention of a person on security grounds

individuals of concern to CSIS were entered onto the list.

*CSIS, citizenship applications and the Alert List*²⁷

On 1 January 1997, CIC instituted a mail-in system whereby all applications for citizenship are processed by the Case Processing Centre (CPC) in Sydney, Nova Scotia. As part of the tracing procedures, the names of all applicants are sent to CSIS through electronic data transfers for cross-checking against names in the Security Screening Information System data base, more specifically, the Service's Alert List. As of July 1998, the Alert List held the names of 259 individuals who had come to the attention of CSIS through TARC-approved investigations, and while not yet citizens, had received landed immigrant status.

The vast majority of citizenship applications are processed in an expeditious manner with the rest requiring additional analysis by the Service before it sends a recommendation to Citizenship authorities. In fiscal year 1997-98, CSIS received a total of 91,873 names from CIC. Out of these, 23 cases (at the time of publication of this report) were still in the initial data review stage, 24 were under active investigation, and three cases were in the briefing stage. The Solicitor General had approved the deferral of two cases, while a third was in the process of being examined for a deferral.²⁸ In addition, CSIS provided seventeen briefs to CIC on individuals who have been or continue to be of concern to CSIS but whose activities do not meet the threshold for denial of citizenship based on security grounds.

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. 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 24 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 to or cooperate on an operational level with domestic agencies. 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 1997-98

The Service signed no new agreements with domestic agencies in fiscal year 1997-98. For this audit report, the Review Committee carried out two studies pertaining to on-going domestic arrangements, the first dealing with information exchanges between the Service and law enforcement agencies (see page 18) and the second addressing specific issues in the relationship between the RCMP and CSIS (see page 27).

International Arrangements

Pursuant to section 17(1)(b) of the *CSIS Act*, the Service must obtain the approval of the Solicitor General — after he has consulted with the Minister of Foreign Affairs — in order to enter into an arrangement with the government of a foreign state or an international organization. During the exploratory and negotiating phase leading to an agreement, the Service cannot pass classified information to the foreign agency. It may, however, accept unsolicited information.

Arrangements for 1997-98

In fiscal 1997-98, CSIS concluded nine new liaison agreements with foreign agencies. During the same period, 11 existing liaison agreements were expanded to broaden the types of information that can be shared. The Service also entered into talks on potential liaison agreements with several other foreign government agencies.

Our most recent audit identified no problems of consequence in the implementation of these agreements, however, some of the new arrangements will bear closer monitoring as they are activated and as events transpire.

Collection of Foreign Intelligence

Foreign intelligence refers to the collection and analysis of information about 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, and with the approval

of the Solicitor General, collect foreign intelligence. The collection must take place in Canada, and cannot be directed against Canadians, permanent residents or Canadian companies.

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;
- we assess whether CSIS has met the test to collect information from section 16 operations; and,
- in general terms, we assess whether the Service’s cooperation with the Communications Security Establishment (CSE) complies with the *CSIS Act*.²⁹

Findings of the Committee

Ministerial Requests

As part of our review, the Committee examines all Ministers’ requests for section 16 operations. For the period 1997-98, we identified a number of requests that did not fully comply with the requirements of a Government Memorandum of Understanding signed in 1987 to the effect that all such requests must contain an explicit prohibition against targeting Canadians, permanent residents and Canadian companies; and further, that the request should indicate whether the proposed activity is likely to involve Canadians.

The Service is not required to enter into a formal arrangement in order to pass information to or cooperate on an operational level with domestic agencies

We saw some requests which we believe had little relevance to section 12

Section 16 Information Collection

The Committee reviewed the working files of the Service's section 16 collection activities and among those randomly selected we identified two errors: CSIS had mistakenly intercepted the communications of a person for three days, though no information was collected or retained; in a second instance, a Canadian national had been intercepted — in response to which the Service stated that the interception was purely incidental.

Retention of Foreign Intelligence

The Committee examined the foreign intelligence that CSIS retained from section 16 collection activities. We believe that in a number of instances the information collected was not relevant to the Service's mandate under section 12, including a report of a public speech and another on an intimate personal discussion.

Section 16 Information and the Communications Security Establishment

The information that CSE routinely gives the Service is "minimized" in order to comply with the prohibition on the collection of information on Canadian nationals and Canadian companies. Thus, for example, the actual identity of a Canadian would be shielded by employing the phrase "a Canadian businessman."

The Service, under special circumstances, may request these identities from the CSE if it believes the information is relevant to an ongoing section 12 ("threats to security") investigation. For its part, the Committee routinely scrutinizes these Service requests

to CSE for information to ensure that they are appropriate and comply with existing law and policy.

This year we saw some requests which we believe had little relevance to section 12 — a person's possible involvement in criminal activity being one example. The Committee also identified an instance where the Service's request was made only verbally leaving no written record for us to examine. We have notified the Service that we believe all requests to CSE should be in writing.

The Committee recommends that all CSIS requests to CSE for identifying information be fully documented.

Follow-up to the 1995-96 Audit Report

In the 1995-96 SIRC Annual Report, the Committee discussed a case in which the CSE documentation used in support of a CSIS targeting decision was unavailable from CSIS for our review — with CSIS stating that it no longer held the information. At the time, the Committee strongly recommended that in future, CSIS retain for examination by the Committee "any supporting document or telex used as reference in a TARC 'Request for Authority' or a warrant affidavit." During the year under review in this report, the Service instructed its officers to retain copies of this information.

Management, Retention and Disposition of Files

Files are the essential currency of intelligence gathering. Every CSIS investigation

denying that an individual is a target by stating positively that the complainant in question had not been the subject of a section 12 investigation.

Not satisfied with the response, the complainant's counsel asked the Committee to investigate further. Our investigation revealed that CSIS had not been involved in the activities described.³³ In communicating our findings to the complainant we noted that while we could certainly understand the frustration our response might elicit, it was the Committee's view based on experience that CSIS would not willfully deny the existence of information in the knowledge that SIRC's powers of review and its access to all of the Service's holdings would reveal the information if it indeed existed.

The Committee found nothing unreasonable or inappropriate in CSIS activities in relation to the three other cases, and that assurance was conveyed to the complainants.

Complaints Regarding CSIS Assistance to Citizenship and Immigration

During fiscal year 1997-98, we received ten complaints dealing with the Service's assistance role in the delivery of the Immigration Program. Most dealt with the time taken by CSIS to provide security assessments or advice to the Minister of Citizenship and Immigration .

In one case where we had completed a review of the documentation, the complainant informed the Committee that he did not wish to pursue the matter further. In respect of another six cases, we confirmed to the complainants upon completion of our review

that CSIS had finished its enquiries and provided its advice to CIC. Because the Committee has no jurisdiction regarding the activities of CIC, our role typically ends at this point unless the complainant requests further inquiries. In an additional three cases, requests were made that the Committee look more closely into CSIS conduct during security screening interviews and at the nature of the Service's advice to CIC. The necessary investigations (which involve the testimony of numerous witnesses) are not yet complete, and will be reported upon in next year's annual audit report.

Misdirected Complaints and Complaints Outside SIRC's Mandate

During the year, the Committee received five complaints regarding matters that had not yet been taken up with the Service by the complainants. We informed each of the complainants of the requirement set out in the *Act*, whereby all complaints must first be submitted to the Director of CSIS. As at July 1998, the Committee has heard from only one complainant claiming to be not satisfied with the Service's response. We are currently investigating the matter.

In respect of eight additional complaints, our preliminary reviews led us to conclude that the complaints did not fall within the purview of the Committee as set out in the *CSIS Act*. In two of the eight cases, the complainants (both ex-CSIS employees) were entitled to seek redress by means of a grievance procedure.

Another complaint consisted of a request by a representative of CSIS employees for the Committee to look "again" at bilingualism

The Committee found nothing unreasonable or inappropriate in CSIS activities in relation to the three other cases

The focus of our investigation is on the decision of the deputy head to deny the government employee or contractor a security clearance

and work relations within the Service. In 1986, the Solicitor General, with the concurrence of the Director of CSIS, asked the Committee to review the linguistic situation in the Service with a view to assessing the likely impacts of Official Languages programs on the Service's operations. However, in our response to this recent complainant, the Committee expressed the view that Commissioner of Official Languages was better qualified to undertake such a review. In the absence of a specific mandate from the Solicitor General, and taking into consideration the limits of our enabling statute,³⁴ we concluded that the issue was not within the Committee's mandate.

Findings on 1997-98 Security Clearance Complaints

We received one complaint pursuant to the denial of a security clearance. As is normal in cases of this type, the focus of our investigation is on the decision of the deputy head to deny the government employee or contractor a security clearance — a decision usually based primarily on the Service's recommendation.

At the time of publication of this report, the complainant had informed us that he intended to avail himself of the opportunity to make representations to the Committee about the deputy head's decision to deny the clearance.

Findings on 1997-98 Ministerial Reports

Citizenship Refusals

In our 1995-96 annual report, the Committee reported that it had received a Ministerial report concerning the citizenship application

of Ernst Zündel. At that time, SIRC's jurisdiction to investigate the matter was successfully challenged in the Federal Court of Canada, where it was held that because of statements contained in a SIRC report, *The Heritage Front Affair*, (a study carried out under a different part of the Committee's mandate) there was a reasonable apprehension that the Committee would be biased in its investigation of the Ministerial report about Mr. Zündel.

The Government subsequently appealed the decision, and on 27 November 1997 the Federal Court of Appeal ruled: "Considering SIRC's duality of functions, which must be understood as permitting the exercise of both powers, and considering that this bi-functional structure does not in itself give rise to a reasonable appearance of bias..." the Court saw no reason why the Committee, acting within its statutory framework, should be prohibited from pursuing an investigation of Mr. Zündel under the *Citizenship Act*, notwithstanding earlier statements.

Mr. Zündel sought leave to appeal this decision to the Supreme Court of Canada — leave which was denied on 30 April 1998. Because the Member originally assigned to the investigation has since died, the Committee has had to resume its investigation *ab initio*. The matter is in the process of being heard.

Deportation Orders

The Committee received no Ministerial Reports of this type during 1997-98. However, a case involving a report received in 1996-97 has continued to evolve. In a matter

first heard by our former Chair, the Committee ruled that the subject of the complaint was of such character as to fall within the class of persons described within paragraph 19(1)(g) of the *Immigration Act*: “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.

The Committee’s decision was appealed, with the Federal Court of Canada ruling that portions of 19(1)(g) contravened the freedom of association assured by paragraph 2(d) of the *Charter of Rights and Freedoms* in a manner that was not demonstrably justified in a free and democratic society. The Court referred the matter back to the Committee for reconsideration.

Another Committee Member was subsequently asked to rule on whether the subject

of the complaint, a permanent resident of Canada, was a person described in paragraphs 19(1)(e), 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 remained in force following the Federal Court judgement.

Having found that the subject of the Ministerial Report was a person described in paragraphs 19 (1)(e) and 19 (1) (g), the Member concluded that a security certificate should be issued.

Canadian Human Rights Commission Referrals

The Committee received one referral from the Canadian Human Rights Commission based on alleged discrimination in employment on the grounds of religion — discrimination contrary to the *Canadian Human Rights Act*.³⁵

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 of the Committee

After examining all the files in the case, and receiving representations from all parties, the Committee saw no evidence to substantiate allegations of discrimination. We found further that the assertion by the Department concerned that its denial of clearance was based wholly on matters concerning the security of Canada had merit and had been adequately substantiated.

B: 1997-98 Complaints about Security Screening

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.

Committee Findings

For the year under review, CSIS forwarded eighteen briefs³⁶ to departments, twelve of which were information briefs and six were rejection briefs. Since the Service's Government Security Policy (GSP) clients are required to notify the Service of their decision only when it differs from the Service's recommendation, and given that there were no instances in which CSIS was so informed, it can be deduced that there were six denials of a security clearances by

The Evolution of the Security Clearance Complaints Procedure

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.

government departments. It should be noted that in the absence of a complaint by an affected party, the Committee is unaware of decisions that may or may not have been taken by Federal Government departments on the basis of CSIS briefs. The Committee noted with interest that although the number of security clearance denials had increased, the number of these complaints to the Committee had not risen accordingly.

Unequal Access to “Right of Review”

As noted in the description of the procedures in place for handling security clearance complaints, 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.

For government employees denied clearance, there exists a “right of review” by the Committee. However, section 42 gives this right only to those persons who contract directly with the government. For individuals and employees falling under the jurisdiction of

Aerodrome Security Regulations and the *Aeronautics Act*, their only recourse is the comparatively lengthy and expensive process of a Federal Court action.

The number of people potentially involved is significant. Before an airport restricted area pass can be issued, an individual must have an airport security clearance. Since the inception in 1987 of the Airport Restricted Area Access Clearance Program, more than 140,000 persons have had to obtain such clearance and 31 individuals have had clearance denied to them. None have access to a Committee review of their cases.

The issue of the unequal redress system has been a preoccupation of the Committee since 1987 and we believe that the situation should not be allowed to continue. The Committee understands that the Minister of Transport made representations to the Solicitor General concerning the problem in 1996. We hope the matter will be pursued so that this obvious inequity can be remedied.

The issue of the unequal redress system has been a preoccupation of the Committee since 1987

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.”

Security Screening in the Government of Canada

The Government Security Policy (GSP) 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* (the “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 (i.e., 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. 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.

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 give effect to 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 Directions govern CSIS investigations — for example, those conducted in potentially sensitive areas such as 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 behavior 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.

For 1997-98, we were advised of one new Ministerial Direction.

National Requirements for Security Intelligence 1997-98

National Requirements contain general direction from Cabinet as to where CSIS should focus its investigative efforts, as well as guidance on the Service's collection, analysis and advisory responsibilities. It appears that the Government has returned to a one-year National Requirements cycle instead of the two-year plan adopted in 1995. For 1997-98, the National Requirements set out the priorities for CSIS in five areas: counter terrorism, counter intelligence, security screening, foreign intelligence support, and reporting criminal activity. The new Ministerial Direction brings changes to a number of these areas.

In counter terrorism, the Minister added political violence arising from states that sponsor ethnic conflict in Canada to the list of potential threats to be addressed. With respect to reporting criminal activity, the Minister directed CSIS to enlarge the list of Canadian recipients of information it receives from foreign intelligence services about transnational criminal activity; this

There are a number of independently managed systems inside and outside the Service for monitoring CSIS activities

The important change to existing policy concerned a particular category of “sensitive institution”

information will now be available to other law enforcement agencies in addition to the RCMP. With impact across the range of Service activities, the change in instructions also adds certain kinds of domestic investigations to the list of those not requiring Ministerial approval, while at the same time, broadens the Service’s requirement to report to the Minister on any investigation where there is a well-founded risk of serious violence.

The most recent National Requirements contain two elements not seen in previous versions. For the first time, the National Requirements employed the phrase “Canadian interests,” in addition to the usual “threats to the security of Canada.” We questioned the Service on whether it took this change in wording as an expansion of its mandate and an enlargement of the scope of its investigations. The Service stated in response that it regarded the phrases as synonymous, and that in any event its actions were governed by the *CSIS Act* and Service policies. The Committee intends to monitor the Service’s actions with respect to this innovation in language.

In addition, the Committee noted references to specific targets. Our interest was in knowing whether such Direction would influence the Service’s targeting decisions. In response to our queries, the Service stated that it regards the National Requirements as a general guide, but that it is the Target Approval and Review Committee (TARC) that has the responsibility to review and approve applications to conduct investigations. [for a discussion of TARC, see inset

page 39]. Once again, the Committee will monitor Service targeting decisions with the new Direction in mind.

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. Operational policies, some of which are sensitive and potentially intrusive, must comply with Ministerial Direction, the *CSIS Act*, the *Canadian Human Rights Act*, and other relevant legislation.

In the fiscal year 1997-98, the Service produced one new policy instruction and made significant amendments to an existing policy.

Countering Technical Intrusions into CSIS Operations

The new policy instruction outlines the responsibilities and mechanisms governing “counter technical intrusion inspections” in support of the Service’s operational activities. The object of the policy is to protect certain areas used for the Service’s operational activities from technical intrusion.

Investigations at Post-secondary Institutions

The important change to existing policy concerned a particular category of “sensitive institution.” In order to bring operational

policies into line with the Ministerial Direction entitled “Conduct of Security Investigations at Post-Secondary Institutions,” issued early in 1997, the Service amended its policies on campus operations. The amendments are reflected in human source operations, immigration and citizenship screening investigations, and government security screenings.

Disclosure of Information in the Public and in the National Interest

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. There were none in 1997-98.

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.” 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. CSIS policy stipulates that the Committee be informed whenever such disclosures take place. There were none in 1997-98.

Governor in Council Regulations and Appointments

Under section 8(4) of the *CSIS Act*, the Governor in Council may make regulations concerning the power of the Director of CSIS, appointments and other personnel matters. No such regulations were issued in 1997-98.

Annual Report of the Director of CSIS

The CSIS Director’s Annual Report to the Solicitor General comments on the Service’s operational activities for the preceding fiscal year. To late August 1998, we had not received the Director’s report for 1997-98. We therefore cannot comment on it here.

Certificates of the Inspector General

The Inspector General of CSIS reports to the Solicitor General and functions effectively as his internal auditor of 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 Director’s report on the operational activities of the Service and informing the Minister of any instances of CSIS having failed to comply with the *Act* or Ministerial Direction, or that involved an unreasonable or unnecessary exercise of powers. The Minister sends a copy of the Certificate to the Security Intelligence Review Committee.

The Committee received the Inspector General’s Certificate covering fiscal year 1995-96 in December 1997, and his certificate for fiscal year 1996-97 in July 1998.

Under one circumstance, explicitly referred to in the *Act*, the Minister can authorize the Service to disclose information in the “public interest”

The Inspector General expressed concerns about the factual basis for some statements in the report

During this period, the Committee also received copies of three special reports the Inspector General provided to the Minister.

1995-1996 Certificate

The Inspector General commented that he was satisfied that the Director's Annual Report for fiscal 1995-96 was a reasonable reflection of the nature and scope of CSIS operational activities for the year. While he noted that a number of statements in the report were, in his view, exaggerations and did not accurately reflect the file material that he examined, the discrepancies would not have seriously misled the Solicitor General in understanding the subjects discussed. The Inspector General repeated concerns expressed in a previous certificate, about the brevity of reporting in annual reports on activities conducted under sections 16 and 17 of the *Act*.

1996-1997 Certificate

With respect to the report of the Director of CSIS for 1996-97, the Inspector General expressed concerns about the factual basis for some statements in the report, but noted that the Director had taken greater care in providing the Solicitor General with a clear description of CSIS activities during the year. He repeated his concerns about limited reporting on activities conducted on section 16 and 17 of the *CSIS Act*. He found the report to be a reasonable reflection of the nature and scope of CSIS's activities for the year.

As required by the *CSIS Act*, these two certificates also make a number of important recommendations concerning the Service's compliance with the *Act* and Ministerial

Direction. These recommendations focused on specific investigations and CSIS practice in the following areas: targeting, the use of informants, information retention, disclosure of information and CSIS' cooperation with other agencies. In view of the complexity of these issues, we will comment on them in our next annual report.

Unlawful Conduct

Under section 20(2) of the *CSIS Act*, the Director of CSIS 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 1997-98, we received one report of possible unlawful conduct by an employee of CSIS. However, because the case is presently under criminal investigation, and no final actions have been taken, we are unable to comment on the report.

To date, the Service has made 14 reports to the Minister concerning unlawful conduct under section 20(2) of the *Act*. In addition to the new instance noted above, two others dating back to 1989 and 1990 remain unresolved. Following inquiries from the Committee, the Service has assured us that in concert with the other agencies of Government with jurisdiction in the matter, it has taken the appropriate steps to resolve both cases.

SIRC Consultations and Inquiries

As noted earlier, the Committee is a key part of the CSIS accountability structure.

In 1997-98 we undertook specific activities in this respect in the following areas:

Tracking and Timing of Formal Inquiries

In 1997, we augmented the system used to track the inquiries we make of CSIS and the length of time the Service takes to reply. Written questions to the Service include a due date giving it a reasonable amount of time to respond. For tracking purposes, the “clock” starts ticking the day after the due date, with end of fiscal year calculations being based on the average number of days that the Service exceeds the grace period. In fiscal year 1997-98, we directed 142 formal questions to the Service; the average response time was 39 days following the sending of the request.

In addition to formal questions, the Committee may make informal requests of CSIS. In all such cases for the year under review, the Service responded expeditiously to what were sometimes urgent queries.

Briefings

In the course of their regular audit functions, the Review Committee’s research staff have daily contact with CSIS personnel. As well, the Service arranges special briefings for Committee Members or staff at our request or on the recommendation of the Service with the topics ranging from new developments in technology to investigations of special interest.

At its monthly meetings, the Chair and Committee Members meet with other government officials to keep open the lines of communication and stay abreast of new developments. The Committee met with the

Director of CSIS in August 1997 and March 1998. When meetings of the Review Committee are held outside of Ottawa, Members visit CSIS Regional Offices. The Committee met with senior CSIS Regional Managers in Québec City in May 1997, in Vancouver in April 1998, and in Toronto in June 1998. The balance of the monthly meetings were held in Ottawa.

SIRC Activities Additional to CSIS Review

The Committee met with the Solicitor General and the Deputy Solicitor General in September 1997, and two senior officials from the Office of the Inspector General of CSIS in October 1997.

The Chair and the Executive Director attended a conference for Intelligence Review Agencies held in Canberra, Australia in November 1997.

During the course of 1997-98 Committee Members met a number of visiting scholars and officials, among them were:

- the Director General and two senior officials of the Australian Security Intelligence Organization (ASIO) (September 1997);
- the United Kingdom’s Intelligence and Security Committee (March 1998);
- the British Columbia Civil Liberties Association in Vancouver (April 1998);
- in May 1997, the Committee’s Director of Research met with five members of Germany’s Bundestag; and,
- a Professor from the University of London, UK, to discuss public management of the security and intelligence sector (May 1997).

We augmented the system used to track the inquiries we make of CSIS and the length of time the Service takes to reply

The Committee's Counsel and Senior Complaints Officer attended meetings in the Middle East in January 1998, as part of a Committee review of the CSIS Immigration Screening Program.

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 1997-98, 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

On 30 April 1998, the Prime Minister of Canada announced the appointment of the Honourable Bob Rae, P.C., Q.C. to SIRC.

The Honourable Edwin Goodman, P.C., O.C., Q.C., the Honourable Georges Vari, P.C., O.C., C.L.H., and the Honourable Rosemary Brown, P.C., O.C., O.B.C. marked the end of their five-year mandates with the Committee. We are grateful for the time and dedication that these members contributed during their tenure at SIRC.

Accounting to Parliament

During 1997-98, the Review Committee Chair met with several Members of Parliament to exchange views on how SIRC could assist Members of the Standing Committee on Justice and Human Rights to fulfill their responsibilities. We appeared before the Sub-Committee on National Security on 15 April 1997 and before the full Standing Committee on 14 May 1998 to respond to questions about the Main Estimates. In her opening comments, the Committee Chair, the Honourable Paule Gauthier, P.C., O.C., Q.C. reviewed the

Table 3
SIRC Budget 1997-98

	1997-98	1996-97
Personnel	831,000	805,000
Goods and Services	575,000	598,000
Total Operating Expenses	1,406,000	1,403,000

Source: 1997-98 Estimates, Part III, Section II.

Committee's key plans and strategies for the following year, and identified the external factors that influence the Committee's operations and budget. In closing, Paule Gauthier invited suggestions or constructive criticism on ways in which the Review Committee could better perform its duties.

Staying in Touch with Canadians

Symposia

Research Staff participated in the conference and annual general meeting of the Canadian Association for Security and Intelligence Studies (CASIS), held in Ottawa in June 1998.

SIRC on the Internet

Since its debut on the Internet in October 1996, the SIRC website (www.sirc-csars.gc.ca) has received more than 279,000 visits. We plan to improve our web site so that it better reflects the Review Committee's ongoing work, while at the same time making it a more useful research tool for our clients.

All SIRC annual reports — dating back to 1984-85 when the Committee was established — are now accessible through the web site. The list of Committee studies has been updated and we have added hot links to other web sites of interest. The site also provides readers with information about procedures for filing complaints about CSIS activities and the denial of security clearances, as set out in sections 41 and 42 of the *CSIS Act*.

Impact of Budget Reductions

Government-wide budget reductions continue to have an impact on the Committee's research functions. Until last year, the

Committee allotted its research resources between two teams: one reviewed counter intelligence operations while the other was devoted to examining the counter terrorism side of CSIS work. The Committee has since integrated research resources so as to increase its effectiveness in reviewing the activities of CSIS.

In last year's report, we stated that the Review Committee would be doing more work "in house", using outside lawyers less, and employing fewer contract researchers. We are satisfied with this redeployment of resources and, with respect to the complaints function, are confident that our staff Legal Counsel has developed an expertise in most of the relevant areas beyond that which we could find elsewhere.

The investigation of complaints and ministerial reports is the most costly area of discretionary spending for the Committee. Small changes in their numbers can significantly affect the Committee's budget and operations. They consume a lot of staff time, require the purchasing of expensive legal services, and their very nature makes it difficult to predict how many there will be or their complexity. As a result of a 1993 amendment to the *Immigration Act*,³⁷ however, the Committee is anticipating an increase in the number of ministerial reports the Committee will be required to handle.

In the area of information technology, the Committee has ensured that its information systems are "year 2000" compliant, and has engaged outside specialists in this regard. As a matter of policy, the Committee will continue to stay abreast of innovations in

The Committee is anticipating an increase in the number of ministerial reports the Committee will be required to handle

information technology so as to continue the steady increase in productivity seen over the last five years.

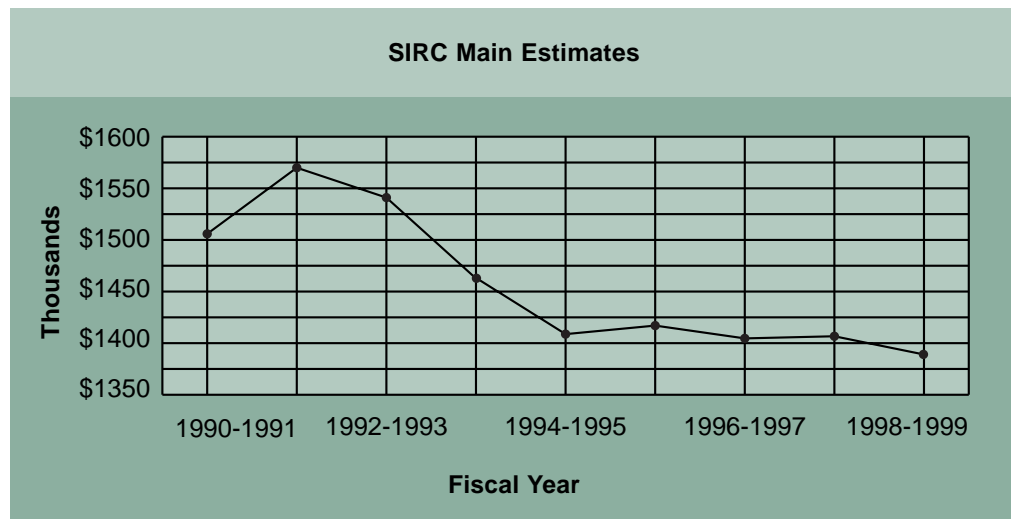
Personnel

The Committee currently has a small total staff of 14: 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 sensitive and highly-classified material using special security procedures.

The Committee has recently seen some major staff changes with the departure of six long-time employees who retired or obtained new posts in government. To all

we express our sincere gratitude for their hard work, loyalty, and dedication to SIRC. We are pleased to welcome the new employees to fill the vacancies in our research and administrative divisions.

At its monthly meetings, the members of the Committee decide formally on the research and other activities they wish to pursue, and set priorities for the staff. Management of day-to-day operations is delegated to the Executive Director with direction when necessary from the Chair in her role as the Chief Executive Officer of the organization.



Glossary

ASIO	- Australian Security Intelligence Organization
CASIS	- Canadian Association for Security and Intelligence Studies
CCM	- Correspondence Control Management
CIC	- Citizenship & Immigration Canada
CI	- Counter Intelligence
CPC	- Case Processing Centre
CSE	- Communications Security Establishment
CSIS	- Canadian Security Intelligence Service
CT	- Counter Terrorism
DFAIT	- Department of Foreign Affairs & International Trade
DIRECTOR	- the Director of CSIS
DND	- Department of National Defence
EII	- Enforcement Information Index
ESPI	- Economic Security and Proliferation Issues Unit
FOSS	- Field Operational Support System
GSP	- Government Security Policy
IAC	- Intelligence Assessment Committee
IOET	- Intelligence Officer Entry Training
IRB	- Immigration and Refugee Board

MOU	- Memorandum of Understanding
NAC	- National Archives Canada
NARU	- National Archives Requirements Unit
PCO	- Privy Council Office
POEAP	- Point of Entry Alert Program
RAP	- Analysis and Production Branch
RCMP	- Royal Canadian Mounted Police
RTA	- Request for TARC Authority
SERVICE	- Canadian Security Intelligence Service (CSIS)
SIRC	- Security Intelligence Review Committee
SLO	- Security Liaison Officer
SSIS	- Security Screening Information System
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 *)

1. *Eighteen Months After Separation: An Assessment of CSIS' Approach to Staffing Training and Related Issues*, (139 pages/SECRET) * (86/87-01)
2. *Report on a Review of Security Screening for Applicants and Employees of the Federal Public Service*, (SECRET) * (86/87-02)
3. *The Security and Intelligence Network in the Government of Canada: A Description*, (61 pages/SECRET) * (86/87-03)
4. *Ottawa Airport Security Alert*, (SECRET) * (86/87-05)
5. *Report to the Solicitor General of Canada Concerning CSIS' Performance of its Functions*, (SECRET) * (87/88-01)
6. *Closing the Gaps: Official Languages and Staff Relations in the CSIS*, (60 pages/UNCLASSIFIED) * (86/87-04)
7. *Counter-Subversion: SIRC Staff Report*, (350 pages/SECRET) (87/88-02)
8. *SIRC Report on Immigration Screening*, (32 pages/SECRET) * (87/88-03)
9. *Report to the Solicitor General of Canada on CSIS' Use of Its Investigative Powers with Respect to the Labour Movement*, (18 pages/PUBLIC VERSION) * (87/88-04)
10. *The Intelligence Assessment Branch: A SIRC Review of the Production Process*, (80 pages/SECRET) * (88/89-01)
11. *SIRC Review of the Counter-Terrorism Program in the CSIS*, (300 pages/ TOP SECRET) * (88/89-02)
12. *Report to the Solicitor General of Canada on Protecting Scientific and Technological Assets in Canada: The Role of CSIS*, (40 pages/SECRET) * (89/90-02)
13. *SIRC Report on CSIS Activities Regarding the Canadian Peace Movement*, (540 pages/SECRET) * (89/90-03)

14. *A Review of CSIS Policy and Practices Relating to Unauthorized Disclosure of Classified Information*, (SECRET) (89/90-04)
15. *Report to the Solicitor General of Canada on Citizenship/Third Party Information*, (SECRET) * (89/90-05)
16. *Amending the CSIS Act: Proposals for the Special Committee of the House of Commons*, (UNCLASSIFIED) (89/90-06)
17. *SIRC Report on the Innu Interview and the Native Extremism Investigation*, (SECRET) * (89/90-07)
18. *Supplement to the Committee's Report on Immigration Screening of January 18, 1988*, (SECRET) * (89/90-01)
19. *A Review of the Counter-Intelligence Program in the CSIS*, (700 pages/ TOP SECRET) * (89/90-08)
20. *Domestic Exchanges of Information*, (SECRET) * (90/91-03)
21. *Section 2(d) Targets — A SIRC Study of the Counter-Subversion Branch Residue*, (SECRET) (90/91-06)
22. *Regional Studies (six studies relating to one region)*, (TOP SECRET) (90/91-04)
23. *Study of CSIS' Policy Branch*, (CONFIDENTIAL) (90/91-09)
24. *Investigations, Source Tasking and Information Reporting on 2(b) Targets*, (TOP SECRET) (90/91-05)
25. *Release of Information to Foreign Agencies*, (TOP SECRET) * (90/91-02)
26. *CSIS Activities Regarding Native Canadians — A SIRC Review*, (SECRET) * (90/91-07)
27. *Security Investigations on University Campuses*, (TOP SECRET) * (90/91-01)
28. *Report on Multiple Targeting*, (SECRET) (90/91-08)
29. *Review of the Investigation of Bull, Space Research Corporation and Iraq*, (SECRET) (91/92-01)

30. *Report on Al Mashat's Immigration to Canada*, (SECRET) * (91/92-02)
31. *East Bloc Investigations*, (TOP SECRET) (91/92-08)
32. *Review of CSIS Activities Regarding Sensitive Institutions*, (TOP SECRET) (91/92-10)
33. *CSIS and the Association for New Canadians*, (SECRET) (91/92-03)
34. *Exchange of Information and Intelligence between CSIS & CSE, Section 40* (TOP SECRET) * (91/92-04)
35. *Victor Ostrovsky*, (TOP SECRET) (91/92-05)
36. *Report on Two Iraqis — Ministerial Certificate Case*, (SECRET) (91/92-06)
37. *Threat Assessments, Section 40 Study*, (SECRET) * (91/92-07)
38. *The Attack on the Iranian Embassy in Ottawa*, (TOP SECRET) * (92/93-01)
39. *“STUDYNT” The Second CSIS Internal Security Case*, (TOP SECRET) (91/92-15)
40. *Domestic Terrorism Targets — A SIRC Review*, (TOP SECRET) * (90/91-13)
41. *CSIS Activities with Respect to Citizenship Security Screening*, (SECRET) (91/92-12)
42. *The Audit of Section 16 Investigations*, (TOP SECRET) (91/92-18)
43. *CSIS Activities during the Gulf War: Community Interviews*, (SECRET) (90/91-12)
44. *Review of CSIS Investigation of a Latin American Illegal*, (TOP SECRET) * (90/91-10)
45. *CSIS Activities in regard to the Destruction of Air India Flight 182 on June 23, 1985 — A SIRC Review*, (TOP SECRET) * (91/92-14)
46. *Prairie Region — Report on Targeting Authorizations (Chapter 1)*, (TOP SECRET) * (90/91-11)
47. *The Assault on Dr. Hassan Al-Turabi*, (SECRET) (92/93-07)
48. *Domestic Exchanges of Information (A SIRC Review — 1991/92)*, (SECRET) (91/92-16)

49. *Prairie Region Audit*, (TOP SECRET) (90/91-11)
50. *Sheik Rahman's Alleged Visit to Ottawa*, (SECRET) (CT 93-06)
51. *Regional Audit*, (TOP SECRET)
52. *A SIRC Review of CSIS' SLO Posts (London & Paris)*, (SECRET) (91/92-11)
53. *The Asian Homeland Conflict*, (SECRET) (CT 93-03)
54. *Intelligence - Source Confidentiality*, (TOP SECRET) (CI 93-03)
55. *Domestic Investigations (1)*, (SECRET)(CT 93-02)
56. *Domestic Investigations (2)*, (TOP SECRET) (CT 93-04)
57. *Middle East Movements*, (SECRET)(CT 93-01)
58. *A Review of CSIS' SLO Posts (1992-93)*, (SECRET) (CT 93-05)
59. *Review of Traditional CI Threats*, (TOP SECRET) (CI 93-01)
60. *Protecting Science, Technology and Economic Interests*, (SECRET)(CI 93-04)
61. *Domestic Exchanges of Information*, (SECRET) (CI 93-05)
62. *Foreign Intelligence Service for Canada*, (SECRET) (CI 93-06)
63. *The Audit of Section 16 Investigations and Foreign Intelligence Reports*, (TOP SECRET) (CI 93-11)
64. *Sources in Government*, (TOP SECRET) (CI 93-09)
65. *Regional Audit*, (TOP SECRET) (CI 93-02)
66. *The Proliferation Threat*, (SECRET) (CT 93-07)
67. *The Heritage Front Affair. Report to the Solicitor General of Canada*, (SECRET) (CT 94-02)*
68. *A Review of CSIS' SLO Posts (1993-94)*, (SECRET) (CT 93-09)

69. *Domestic Exchanges of Information (A SIRC Review 1993-94)*, (SECRET)(CI 93-08)
70. *The Proliferation Threat - Case Examination*, (SECRET) (CT 94-04)
71. *Community Interviews*, (SECRET) (CT 93-11)
72. *An Ongoing Counter-Intelligence Investigation*, (TOP SECRET) (CI 93-07)*
73. *Potential for Political Violence in a Region*, (SECRET) (CT 93-10)
74. *A SIRC Review of CSIS' SLO Posts (1994-95)*, (SECRET) (CT 95-01)
75. *Regional Audit*, (TOP SECRET) (CI 93-10)
76. *Terrorism and a Foreign Government*, (TOP SECRET) (CT 94-03)
77. *Visit of Boutros Boutros-Ghali to Canada*, (SECRET) (CI 94-04)
78. *Review of Certain Foreign Intelligence Services*, (TOP SECRET) (CI 94-02)
79. *The Audit of Section 16 Investigations and Foreign Intelligence Reports*, (TOP SECRET) (CI 94-01)
80. *Domestic Exchanges of Information (A SIRC Review 1994-95)*, (SECRET) (CI 94-03)
81. *Alleged Interference in a Trial*, (SECRET) (CT 95-04)
82. *CSIS and a "Walk-In"*, (TOP SECRET) (CI 95-04)
83. *A Review of a CSIS Investigation Relating to a Foreign State*, (TOP SECRET) (CI 95-02)
84. *The Audit of Section 16 Investigations and Foreign Intelligence Reports*, (TOP SECRET) (CI 95-05)
85. *Regional Audit*, (TOP SECRET) (CT 95-02)
86. *A Review of Investigations of Emerging Threats*, (TOP SECRET) (CI 95-03)
87. *Domestic Exchanges of Information*, (SECRET) (CI 95-01)
88. *Homeland Conflict*, (TOP SECRET) (CT 96-01)

89. *Regional Audit*, (TOP SECRET) (CI 96-01)
90. *The Management of Human Sources*, (TOP SECRET)(CI 96-03)
91. *Economic Espionage I*, (SECRET) (CI 96-02)
92. *Economic Espionage II*, (TOP SECRET) (CI 96-02)
93. *Audit of Section 16 Investigations and Foreign Intelligence Reports 1996-97*, (TOP SECRET) (CI 96-04)
94. *Urban Political Violence*, (SECRET)(SIRC 1997-01)
95. *Domestic Exchanges of Information*, (SECRET)(SIRC 1997-02)
96. *Foreign Conflict*, (SECRET)(SIRC 1997-03)
97. *Regional Audit*, (TOP SECRET) (SIRC 1997-04)
98. *CSIS Liaison with Foreign Agencies*, (TOP SECRET) (SIRC 1997-05)
99. *Spy Case*, (TOP SECRET) (SIRC 1998-02)
100. *Domestic Investigations (3)*, (TOP SECRET) (SIRC 1998-03)
101. *CSIS Cooperation With the RCMP*, (SECRET) (SIRC 1998-04)
102. *Source Review*, (TOP SECRET) (SIRC 1998-05)
103. *Interagency Cooperation Case*, (TOP SECRET) (SIRC 1998-06)
104. *A Case of Historical Interest*, (TOP SECRET) (SIRC 1998-08)
105. *CSIS' Role in Immigration Security Screening*, (SECRET) (CT 95-06)

List of Recommendations

CSIS' Role in Immigration Security Screening

While the Committee is aware of the advantages which accrue from having CSIS section 12 investigators from the regions involved in immigration interviews, their presence does increase the possibility that the interview can be used as an investigative tool, rather than for its intended purpose: to provide an opportunity for the prospective immigrant to explain adverse information in relation to his or her security status. The Committee wishes to underscore the need for CSIS to maintain a balance between the need to provide complete and meaningful advice, and the rights of those being interviewed.

We found the Service's *Procedures Guidelines on Immigration Screening Interviews* to be inadequate in several respects. In the Committee's view, the Guidelines should state clearly that immigration interviews will not be used for recruitment or other unrelated purposes.

The Committee believes that the Service's responsibilities in assisting CIC's ability to detect applicants suspected of war crimes or crimes against humanity should be formalized and set out in policy.

CSIS provides advice to CIC on whether a particular individual wishing to gain entry poses a threat to the security of Canada.

We recommend that in future all advice given to CIC should be recorded, along with the specific details about the individual interviewed.

It is the Committee's view that CIC needs to know as much as possible about would-be refugees as it pertains to threats to Canada's security interests. The Committee believes that CSIS should play a greater role in assisting CIC in refugee matters, and that the role should be carefully defined and transparent.

CSIS Liaison with Foreign Agencies

Existing policy guidelines governing CSIS liaison with foreign agencies are silent when it comes to certain kinds of requests. For example, CSIS can ask foreign intelligence services to monitor Canadian residents who travel to other countries.

We recommend, therefore, that CSIS develop policy regarding requests for assistance to foreign agencies to investigate Canadian residents traveling abroad.

The Committee took note of a case where a foreign arrangement had been dormant for ten or more years, and then was reactivated. During the dormant period, however, the political environment of the country concerned had changed substantially. While an informal, local consultation process occurred, there was no formal procedure in place to review the new circumstances.

We recommend that CSIS policy be revised so as to ensure that the terms and conditions of foreign arrangements that have been dormant for a significant period of time are revisited before reactivation.

Additionally,

The Committee recommends that CSIS systematically reexamine all foreign arrangements after the forthcoming release of the new Ministerial Direction on foreign arrangements.

A Case of Historical Interest

In this case, the Committee concluded that the nature of the interaction CSIS had with a certain foreign intelligence service required the Solicitor General's express written consent which was not obtained.

We strongly recommend, therefore, that in all cases where the Service seeks and receives Ministerial approval, that the written record reflect that fact.

Audit of Sensitive Operations in a Region of Canada

In the cases the Committee reviewed, no unwarranted collection of information involving sensitive institutions was identified. All operations were appropriately authorized by senior management.

One unusual case concerned payments to a source for a humanitarian purpose that were made in a way that did not strictly conform to current Service policies.

The Committee recommends that in future, any significant source payments that the Service makes outside established administrative procedures be authorized at CSIS Headquarters.

CSIS senior management issued instructions in January 1996 on how to deal with sources whose efforts on behalf of CSIS might conflict with their employment responsibilities. The

Committee's audit showed, however, that this instruction had not been incorporated into more formal CSIS policy guidelines.

The Committee recommends that CSIS make the senior management instructions referred to above, part of operational policy on the management of human sources.

Collection of Foreign Intelligence

The Committee routinely scrutinizes the Service's requests to the Communications Security Establishment for information to ensure that they are appropriate and comply with existing law and policy. This year the Committee identified an instance where the Service's request was made only verbally, leaving no written record for us to examine.

The Committee recommends that all CSIS requests to CSE for identifying information be fully documented.

Investigation of Complaints about Security Screening

Since the inception in 1987 of the Airport Restricted Area Access Clearance Program, more than 140,000 persons have had to obtain such clearance and 31 individuals have had clearance denied to them. None have access to a Committee review of their cases. The issue of the unequal redress system has been a preoccupation of the Committee since 1987 and we believe that the situation should not be allowed to continue. The Committee understands that the Minister of Transport made representations to the Solicitor General concerning the problem in 1996. We hope the matter will be pursued so that this obvious inequity can be remedied.

Complaint Case Histories

This section describes complaint cases submitted during the past year to the Review Committee concerning which a decision was reached. Not addressed here are complaints that were the subject of administrative reviews, were misdirected, were outside the Committee's mandate, or arose from Service assistance to Citizenship and Immigration Canada. Complaints received, but which have either not been heard or for which investigations are not yet complete, will be reported on at a later date.

A Complaint About CSIS Activities

An individual submitted a letter of complaint to the Director of CSIS in which he expressed his resentment at being "questioned and interrogated" by a CSIS investigator. He said he was "disgusted with the fact that a person from CSIS was questioning an innocent and honest Canadian about a subject that had been public information for donkeys years." He questioned the funds that the Federal Government had allocated to CSIS and stated that he believed insufficient background work had been done by the Service before he was interviewed.

In responding to the complainant, the Director of the Service stated that he was satisfied with the request from CSIS staff to interview the subject and that the procedures employed to carry it out were consistent with CSIS policy. The Director added that the interview request originated from a remark made by the subject to a CSIS employee at a Service conference. The Director explained that the comments led the CSIS employee to believe that the subject might have information which could be of operational interest to CSIS, and that the interview was sought in an attempt to clarify this point.

Committee Findings

The Committee's review of the matter determined that the individual had made a comment at a conference attended by CSIS senior management. While the nature of the comment remains unclear, CSIS staff believed on the basis of the comment that the subject had said something worth pursuing from an operational point of view. The Service sought the individual's cooperation to clarify the comments and to determine the relevancy of the information to Service operations.

The Committee is satisfied that the Service had the necessary authority to request the interview. Furthermore, we concluded that seeking the individual's cooperation in order to determine whether he did have information which could be of operational interest was a reasonable exercise of its powers. It is the Service's responsibility to report to Government on activities that may, on reasonable grounds, be suspected of constituting "threats to the security of Canada" as defined in section 2 of the *CSIS Act*. In fulfilling this part of its mandate, the

Service depends on the cooperation of members of the public who may have knowledge of, or opinions on, activities relating to threats to the security of Canada.

While the complainant had emphasized that the information alluded to at the CSIS conference was in the public domain, the Committee's view was that this fact could not have been confirmed without the Service being able to conduct its interview. We also noted that, having recently lost a close relative, the interview was conducted at a difficult and emotional time in the individual's life. The timing of the interview and the investigating officer's reference to the late relative was unfortunate, however, the CSIS investigator was not aware of this situation.

After taking into consideration all the circumstances of this case, the Committee concluded that the Service had not acted in an illegal, inappropriate, or unreasonable manner.

Investigation of a Ministerial Report Received Pursuant to the *Immigration Act*³⁸

Pursuant to subsection 39(2) of the *Immigration Act*, we were directed to investigate the grounds underlying a report requesting deportation made by the Minister of Citizenship and Immigration and the Solicitor General concerning an individual.

In the report, the Ministers concluded that the individual, a permanent resident of Canada, was a person described in paragraphs 19(1)(e),(g) and 27(1)(c) of the *Immigration Act*.

Paragraphs 19(1)(e) and (g) state:

no person shall be granted admission who is a member of any of the following classes:

(...)

Paragraph (e) persons who have engaged in or who there are reasonable grounds to believe will engage in acts of espionage or subversion against democratic government, institutions or processes, as they are understood in Canada, except persons who, having engaged in such acts, have satisfied the Minister that their admission would not be detrimental to the national interest;

(...)

Paragraph (g) persons who there are reasonable grounds to believe will engage in acts of violence that would or might endanger the lives or safety of persons in Canada or are members of or are likely to participate in the unlawful activities of an organization that is likely to engage in such acts of violence.

Subsection 27(1) lists the grounds for the removal of a permanent resident. The relevant part reads:

When an Immigration officer or a peace officer is in possession of information indicating that a permanent resident is a person who ...

Paragraph (c) is engaged in or instigating subversion, by force of any government.

On 7 November 1995, the Honourable Mr. Justice MacKay ruled that a specific portion of paragraph 19(1)(g) of the *Immigration Act* — “a member of an organization likely to engage in acts of violence that would or might endanger the lives or safety of persons in Canada” — was unconstitutional since it violated section 2(d) of the *Charter of Rights and Freedoms* in a manner not demonstrably justified in a free and democratic society.

It was Justice MacKay’s further opinion that the conclusions reached by the Review Committee in its report of 3 August 1993 were valid, with the exception of the part concerning the individual being a person described in that section of the *Immigration Act* he had ruled unconstitutional. The Court left to the discretion of the Committee whether Mr. Courtois, the member (and at the time of the ruling, the Committee’s Chair) who had conducted the initial investigation and issued the August 1993 report, would complete the review process, or whether another Committee member would be designated. This latter issue was subsequently rendered moot by the death of Mr. Courtois.

While both parties in the case expressed their preference to rely on the testimony and evidence given in the earlier SIRC procedure, the Committee Member assigned to take up the investigation invited them to present additional evidence through witnesses, if they so wished. Following a complete examination of all documentary evidence and transcripts elicited during the previous investigation, the Member heading the investigation issued instructions to both parties with a view to obtaining *viva voce* evidence on the terrorist organization with which the individual was alleged to have had a relationship, and the precise nature of that relationship, including the possible transfer of funds, assistance in recruitment, facilitation of travel, and participation in a particular terrorist incident overseas.

The parties to the case presented witnesses of their choice to address those points.

Committee Findings

The Committee’s investigation was limited to the sections in the *Immigration Act* referred to in the Ministerial report,³⁹ notwithstanding the subsequent changes to the legislation. In addition, Counsel for the complainant also raised the constitutional applicability and validity of certain sections of the *Immigration Act*.

After carefully considering all of the documentary evidence and the testimony given before the Committee, we concluded that the individual in question was in fact a person described in paragraphs 19(1)(e) and 19(1)(g) and that a certificate should be issued in accordance with subsection 40(1) of the *Immigration Act*.

With respect to the constitutional issues raised by the complainant, after carefully reviewing the composition of SIRC and its functions, the Committee concluded that SIRC was not a court of competent jurisdiction within the meaning of section 24 of the *Charter of Rights and Freedoms* and thus did not have authority to rule in the area.

Referral from the Canadian Human Rights Commission

An individual worked for a company that had a contract with a government department. At the start of the person's employment, the individual was issued an "escort pass" which allowed access to restricted areas of an airport only in the company of someone who held a "restricted area" pass. In the process of obtaining the "Airport Restricted Access and Accreditation Program" clearance, the individual was interviewed by CSIS officials. Ultimately, the individual received a letter stating that the requested clearance for the full "restricted area" pass was denied. No explanation was provided to the individual.

The individual, believing that the denial had been based on the ground of religion and thus contrary to the *Canadian Human Rights Act*, lodged a complaint with the Canadian Human Rights Commission. When the Commission received a written notice from the Minister of the Crown that the complaint related to the security of Canada, the Commission referred the matter to us.

Committee Findings

Our investigation determined that the department concerned had consulted CSIS and the RCMP – both organizations are part of the Airport Restricted Area Access and Accreditation Program. Following its interview, CSIS made a recommendation to the government department. A Review Board had been convened within the government department to consider the application in light of the information received through the consultation process. The Board was unanimous in its decision to recommend the denial of the clearance.

The Committee's role in this type of case is quite limited. We examined all of the files pertaining to the matter and received representations from all concerned parties. The documents we reviewed contained no evidence to substantiate the allegations of discrimination on the grounds of religion, and we concluded that the Minister of the Crown's assertion that the denial was based upon matters concerning the security of Canada was substantiated by all of the information available.

Security Screening Statistics

In fiscal year 1997-98, the Service issued 70,465 security assessments and completed 1,250 field investigations and subject interviews. In the vast majority of cases, the Service's security assessment takes the form of a simple notice to departments.

Table 1
Number of Completed Assessments Issued by Level of Clearance

Classification	*New or Upgraded Requests for Security Clearances	**Update of Security Clearances
Level I (Confidential)	576	318
Level II (Secret)	10,506	4,726
Level III (Top Secret)	2,179	4,325
Accreditation	1,241	7
Airport	26,703	174
Special events	19,534	176

* 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.

** Departments must update an individual's enhanced reliability status security clearance (Levels I and II) once every 10 years. Site access security clearances also must be updated every 10 years. A Level III security clearance must be updated every 5 years. These update terms do not preclude a department from reviewing a person's reliability status or from asking CSIS to reassess the clearance "for cause".

The Service's average response times to process security clearances for Government Security Policy (GSP) Levels I, II, III during 1997-98 were 1, 20, and 118 days respectively,

Screening Assessments for Foreign States and International Organizations

During fiscal 1997-98, the volume of requests that the Service received for screening assessment recommendations were,

Inland	28,687
United States	4,352
Overseas Posts	20,195
SLO Information Tracking	3,578 ⁴⁰
Total:	56,812

Advice to Citizenship and Immigration Canada

The number of briefs issued by CSIS to CIC is provided in Table 2:

Type	1995-96	1996-97	1997-98
Information Briefs	47	144	94
Inadmissibility Briefs - No Threat	51	90	108
Inadmissibility Briefs - Threat	5	5	9
Total	103	239	211

CIC coordinates the review of all cases that present security concerns, and such review can involve interdepartmental consultations. However, in all instances, CIC makes the final determination.

Notes

- 1 According to a Ministerial Direction issued in November 1988, the Minister has to personally authorize all investigations carried out under paragraph 2(d) of the *Act*.
- 2 Hamas (Islamic Resistance Movement) is defined by the US Department of State as an organization that uses “both political and violent means” to achieve its goal of an Islamic Palestinian state.
- 3 In 1996-97, CSIS conducted 1,484 interviews. In 1997-98, approximately 1,380 interviews will have been completed. It should be noted that a prospective immigrant can be subject to more than one interview.
- 4 *Report of the Auditor General of Canada*, December 1997. The Auditor General noted that in most cases, Immigration officers render their decisions well before receiving the results of the RCMP checks for duplicate claims and criminal records in Canada. The CIC responded that in all cases where there is information that a claimant does not meet the eligibility criteria, the person is found ineligible, and the claim is not referred to the Immigration and Refugee Board. Once fingerprint results are received, the legislation allows the eligibility decision to be reconsidered where necessary.
- 5 The Committee is fully cognizant of the sensitivity involved in consulting with a refugee claimant’s country of origin since, by definition, a refugee is at odds with his or her country of origin.
- 6 *An Operational Audit of CSIS Activities*, SIRC Annual Report 1996-1997, Ministry of Supply and Services Canada, 1997, pp. 12-13.
- 7 *Report of the Auditor General of Canada to the House of Commons*, Chapter 27, “The Canadian Intelligence Community — Control and Accountability”, November 1996, p. 23-19.
- 8 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 subsection 13(2) and (3), and 17(1) and to monitor the provision of information and intelligence pursuant to those arrangements.”
- 9 A SIRC Review of CSIS’ SLO Posts (London & Paris), 12 January 1993.
- 10 SIRC 1993-94 Annual Report, p. 26.

- 11 A sensitive social institution can be defined as academic, political, religious, media or trade union.
- 12 *CSIS 36-97*, Federal Court of Canada, 3 October 1997, McGillis J.
- 13 The “resort to” clause permits the Service to use the powers granted in a warrant against a target at a place not named in the warrant, which it believes the target has resorted to or will resort. The legality of this clause has been confirmed by the Supreme Court of Canada in *Thompson et al. v. The Queen*, [1990] 2 S.C.R. 1111.
- 14 The “basket clause” permits the interception of communications of persons not named in the warrant, at places specified in the warrant. The legality of the clause was confirmed by the Supreme Court of Canada in *R v. Chesson*, [1988] 2 S.C.R. 148.
- 15 [1984] 2 S.C.R. 145.
- 16 “Conditions” are the limits that the Federal Court places on the Service’s warrant powers, such as limits on certain types of searches and interceptions, and on the retention or destruction of information.
- 17 The Committee will examine the CSIS - RCMP relationship in the transnational crime area.
- 18 In January 1998 CSIS and DND reached agreement and the transfer of the responsibility became effective in July 1998.
- 19 In fiscal 1997-98, through our immigration screening research, we conducted an in-depth review of CSIS’ role in this area. [see page 9]
- 20 CSIS investigators assume the primary responsibility for security concerns, listing the names directly with foreign countries, and the application of the security profiles.
- 21 Enforcement actions: arrest, detention, removal under the *Immigration Act*.
- 22 The Point of Entry Alert Program is also referred to as the Joint Interview Program or the Interdiction Program.

- 23 EII is one of many data banks within the Field Operational Support System (FOSS) used by Immigration officers for information, identification, and processing purposes. EII holds information on all persons who have entered any part of the Immigration stream (either for admission purposes or for removal), and identifies the types of documents issued to the applicants and any action taken by CIC.
- 24 Paragraph 103.1 (1) (b) of the *Immigration Act*.
- 25 Requests from CIC must be processed as quickly as possible, given that the subject of the detention will otherwise be released by CIC, within 48 hours in most circumstances.
- 26 Pursuant to section 40.1 of the *Immigration Act*.
- 27 Formerly known as the Citizenship Flag System. Under the old system, CSIS provided CIC with a monthly hard copy list of persons identified as permanent residents who could apply for citizenship and who were of concern. The applicants had to be screened by CIC officials against the list, and when a “hit” occurred, CSIS would be asked to provide a security assessment of the individual.
- 28 When the Service believes that it is not in a position to render a recommendation to CIC concerning a citizenship application, it must seek approval from the Solicitor General to continue investigating the case and “defer” providing the assessment.
- 29 The Communications Security Establishment is an agency of the Department of National Defence. As described by the Auditor General in his 1996 report to Parliament, *The Canadian Intelligence Community*, the CSE “analyses and reports on foreign radio, radar and other electronic emissions...and provides this foreign intelligence to Canadian Government clients.”
- 30 Supreme Court of Canada, Order rendered on 30 April 1998.
- 31 *Ernst Zündel v. The Minister of Citizenship and Immigration (F.C.A.) (Ont.) (26417)*, Judgment rendered at Ottawa, Ontario, 27 November 1998.
- 32 This position was also maintained by the Federal Court in upholding exempt banks for people subject to Service investigations.
- 33 The first step of our investigation consists in asking for access to all relevant information the Service might have with respect to the subject or the subject matter. The Committee’s investigation stopped at this stage because the CSIS response was that it had no information.

- 34 Specifically, sections 8 and 41(2) of the *CSIS Act*.
- 35 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*. It should be noted that in cases such as these, the Review Committee's role is quite circumscribed, and its review must be completed within the 45-day period prescribed in the *Human Rights Act*.
- 36 CSIS provides three types of briefs to CIC:
- Inadmissible Brief - represents a threat: this brief is used when an applicant falls within one or more of the inadmissible classes in paragraphs 19 (1) (e), (f), (g) and (k) of the *Immigration Act*, and CSIS assessed the applicant as a threat to the security of Canada as defined in section 2 of the *CSIS Act*.
 - Inadmissible Brief - no threat/information: this brief is used when an applicant is deemed "inadmissible" pursuant to one or more of paragraphs 19 (1) (e), (f) (g) and (k) of the *Immigration Act* but does not, in the Service's view, pose a threat under section 2 of the *CSIS Act*.
 - Information Brief: addresses security concerns that do not meet the applicable rejection criteria as defined in section 19(1) of the *Immigration Act*, but which might assist CIC in processing an application.
- 37 This amendment broadened the category of individuals who can be denied immigrant status because of previous connections with terrorist activities.
- 38 This case was received by the Committee in 1996-97.
- 39 For example, section 19(1)(e) as it was then, section 19 (1)(g) as it was then, but with full recognition of the fact that a certain portion of that section was declared of no force and effect by Mr. Justice MacKay; and section 27(1)(c) as it was then, although it no longer exists.
- 40 Number of cases listed via the Security Liaison Officer tracking system. The number is an estimate.