SECURITY INTELLIGENCE REVIEW COMMITTEE

ANNUAL REPORT 1997 - 1998

An Operational Audit of CSIS Activities

Canada

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

Tel: (613) 990-8441
Fax: (613) 990-5230
Web Site: http://www.sirc-csars.gc.ca
Collect calls are accepted, and the switchboard is open
from 7:30 a.m. to 5:00 p.m. Eastern Standard Time.

Cat. No. JS71-1/1998
ISBN 0-662-63833-6

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

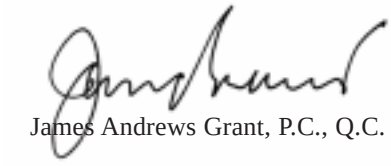
30 September 1998

Dear Mr. Scott:

As required by section 53 of the *Canadian Security Intelligence Service Act*, we transmit to you the Annual Report of the Security Intelligence Review Committee for the fiscal year 1997-98, for your submission to Parliament.

Yours sincerely,

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



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

Robert Keith Rae, P.C., Q.C.

Introduction

With the presentation of this report, the Security Intelligence Review Committee (SIRC) enters its fifteenth year of work on behalf of the Parliament and people of Canada. In carrying out our functions, Members engage a broad range of Canadians — journalists, specialists of all kinds, Parliamentarians, government officials, and citizens with queries or complaints. Judging from the tenor of these contacts, we believe that the security intelligence regime approved by Parliament in 1984 has proved its worth. There has been significant progress, and we are pleased that past and current Members of the Committee, as well as our staff, have been able to make a contribution.

The Members of the Security Intelligence Review Committee believe that the current accountability structure for the Canadian Security Intelligence Service (CSIS) works reasonably well. However, we are increasingly aware that SIRC's role in that structure is not as well understood as it should be. A large factor with which the Committee must contend in communicating with the people of Canada stems directly from the tensions inherent in security intelligence operations in a democratic society. The Committee's mandate places it at the very centre of the dilemmas that result.

Out of regard for safety and security, certain kinds of information must be withheld from general knowledge, yet democratic society rests on maximum possible transparency in government. The inevitable absence of facts and information invites speculation and even fantasy, yet there are well-grounded constraints on what can be done to correct misperceptions. There are multiple administrative and legal mechanisms to help ensure that the country's security intelligence apparatus functions responsibly, but the great majority of citizens are compelled to trust others to carry out the monitoring for them.

Members of the Committee and our staff grapple daily with these dilemmas, and annual audit reports represent our best efforts at finding the correct balance between the competing demands of transparency and accountability on one side, and the safety of Canadians and security of Canada's national interests on the other.

It is the Committee that decides what is in the report and no other body

This balancing act engenders some peculiarities in the Committee's communications with the public. Statements in annual audit reports such as "the Committee reviewed a CSIS investigation of some persons in Canada who were associated with an armed conflict in an overseas country" cannot help but appear unnecessarily oblique or even devious. However, both the law of the land and prudence when it comes to individual safety and national security leave the Committee no responsible alternative.

There are two other essential points readers should keep in mind when examining any of the Committee's reports.

The first is that they can be assured that it is the Committee that decides what is in the report and no other body. No arm of Government or the Service or the bureaucracy dictates its content — we do. As a matter of routine – and as is common practice

in the relationship between auditor and the body being audited – the Service reviews drafts of our reports in order to eliminate factual errors. But the final call is ours and ours alone. The report is then sent to the Solicitor General for delivery to Parliament, and as the *CSIS Act* directs, the Minister is obliged to present the report unaltered to Parliament (and the public) within a fixed period of time.

Our annual audit report is not a bureaucratic afterthought or a public relations handout. It is instead, the culmination of an entire year's detailed review of all facets of the Service's activities

Secondly, our annual audit report is not a bureaucratic afterthought or a public relations handout. It is instead, the culmination of an entire year's detailed review of all facets of the Service's activities. Every study conducted, query pursued, and complaint received, forms a part — in one way or another — of the report which the *CSIS Act* mandates us to present to Parliament.

Members of the Committee are acutely aware that citizens' trust in our work must be earned and nurtured, and then earned again. We hope that efforts such as this year's audit report go some way towards meeting those goals.

How SIRC's Annual Audit Report is Organized

This year's audit report maintains the organization and format instituted in 1996-97. Comments and feedback Committee Members and staff received during the year seemed to bear out our hope that the revised format would be both more functional and more informative.

In general, the report is organized to reflect the Committee's primary functions: first, to review CSIS intelligence activities, second, to investigate complaints about CSIS and associated matters, and third, to act in concert with other parts of the governance system to protect Canadians from threats to their security.

- Section 1 presents the Committee's review and audit of what the Service does and how it does it. The sub-sections represent the different methods the Committee employs to make these assessments.

- Section 2 deals with the Committee's role as a quasi-judicial tribunal with the power to investigate complaints of various kinds.

- Section 3 brings together under one heading — CSIS Accountability Structure — the Committee's review of the multiple administrative and legal mechanisms that hold the Service accountable to Government, Parliament and the people of Canada.

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

Subjects the Committee believes will be of historical, background or technical interest to readers are set apart from the main text in shaded insets. Unlike the main body of the report, they do not reflect Committee opinion or conclusions as such and are intended to be factual in nature.

A minor but, we believe, important innovation for this year's report is that where appropriate, each section of the audit report is labelled with the SIRC study from which it is abstracted. The full references are found in Appendix B.

Section 1: A Review of CSIS Intelligence Activities

A. Areas of Special Interest for 1997-98

This part of the audit report presents the results of major research and analysis carried out by the Committee in the course of the year. The special inquiries are in addition to, and are intended to complement and reinforce, the other forms of audit research the Committee undertakes.

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

This year, the subjects of the Committee's special interest are the following: CSIS investigations into urban political violence; the Meshal incident in Amman, Jordan; the Service's role in immigration screening; matters surrounding a foreign conflict and several domestic threats; intra-governmental cooperation in matters of economic security; policies and procedures for exchanging information with law enforcement agencies and other government departments; the Service's liaison program with foreign intelligence agencies; and, the first phase of our review of CSIS cooperation with the Royal Canadian Mounted Police.

In addition, the Committee reports on four other studies that were smaller in scope — the first concerns the Service's policies regarding "sensitive" institutions, the second looks into the handling of a particular human source operation, the third reviews the remedial measures arising from a breach of security which occurred within the Service, and the fourth looks at a counter intelligence case of historical interest.

Urban Political Violence

Report #94

In 1997 we examined four CSIS investigations of Canadian persons and organizations conducted under section 12 and paragraph 2(c) of the *CSIS Act* — that part of the Service's mandate which directs it to investigate threats of "serious violence" for the purpose of achieving a political objective, more commonly known as the "counter terrorism" clause. What drew the Committee's attention to this particular set of cases was in part a need to reassure ourselves that CSIS was not conducting counter subversion investigations under its counter terrorism mandate. Investigations and their accompanying targeting authorities conducted under section 2(d) of the *Act* — the "counter subversion" clause — require the personal authorization of the Minister,[1] a step not normally required for other kinds of investigation.

As with most of the Committee's reviews, our evaluation also considered whether the Service had reasonable grounds to suspect a threat, whether the level of the investigation was proportionate to the seriousness and imminence of the threat, and whether the information collected was strictly necessary. In the course of our review, SIRC researchers had access to all CSIS reports and files generated during the investigations.

The Committee's Findings

The first two cases dealt with a series of violent incidents which occurred in the mid-1990's. We concluded that the Service did have reasonable grounds to suspect a threat to national security and that only information strictly necessary to provide advice to the government was collected.

However, the Committee also observed difficulties in the relationship between the Service and the police agency leading the criminal investigation that was simultaneously underway against the same targets. The friction between the two agencies centered on the disclosure requirements imposed by the Courts since the R. v Stinchcombe decision. [See inset page 31]

Under the police force's interpretation of the decision, any information it possessed — verbal or written, formal or informal, and regardless of source — was subject to disclosure to the Courts. The Service, in order to protect the integrity and security of its investigations and methods responded to this position by carefully filtering its exchanges with the police force in question. While the Committee is satisfied that the impact of the disagreement was local and temporary, the Committee will continue to monitor the repercussions, if any, of the Stinchcombe decision for CSIS operations and inter-agency relations, especially in the counter terrorism area.

The third case we examined was an issue-based investigation that spanned the country, but focused primarily on Toronto and Vancouver. Of the over 200 field reports the investigation generated, two were not strictly necessary in our view. In the first, the information collected did not deal with violent activity of any sort. The Service agreed with our observation and subsequently deleted the report from its data base. The second report we questioned dealt with the visit to Canada of a representative of a political party of a foreign country. While the Committee did not originally accept the rationale for CSIS involvement in this matter, information we have since received from the Service leads us to conclude that a potential threat to national security was indeed present.

In the fourth investigation reviewed, we identified no problems.

Counter Terrorism or Counter Subversion?

With respect to whether the investigations were conducted under the appropriate section of the *Act*, the Committee is satisfied that the four investigations were properly authorized. The selection of targets, as well as all investigative activities and reporting, were based on the potential for violence to achieve a political objective, and not the nature of the political opinions themselves.

The Committee will continue to monitor the repercussions, if any, of the Stinchcombe decision for CSIS operations and inter-agency relations

In addition, the investigative techniques used were proportionate to the threat.

Operational Cooperation and the Meshal Incident

The Committee found no evidence that CSIS was involved in any manner with the Meshal-Amman incident

The media reported that on 25 September 1997, two agents of the Israeli intelligence service Mossad carrying Canadian passports attempted to assassinate Khaled Meshal, an official of the Palestinian organization Hamas,[2] in Amman, Jordan. The attempt failed, and Jordanian authorities seized the agents and the passports. The incident, and the use of Canadian passports by Israel's intelligence service, raised a number of questions, some of which were prominent in various media at the time, about CSIS cooperation with foreign agencies.

The Review Committee devoted considerable effort to examining the events surrounding this incident not least because of the serious nature of the allegations — that CSIS may have been a party to an assassination attempt in a foreign country.

Methodology of SIRC's Review

In order to understand how and whether CSIS was involved in the Meshal incident, we examined all Service files with a possible connection to the matter, as well as those that pertained to Service operational cooperation with Israeli officials. We looked into investigations of previous incidents of alleged misuse of Canadian passports, and the advice that the Service had provided to the Government. We noted that the Government of Canada had protested to Israeli officials about the misuse of Canadian passports. Review Committee staff also examined all information exchanges between CSIS and Israeli authorities between 1992 and 1997.

Personal interviews with relevant officials also formed part of our inquiries: these included CSIS officials, Canadian Consular officials, and a senior federal official with the Passport Office. In view of his public comments about the matter, including passport misuse, the Committee also interviewed Canada's former Ambassador to Israel, Mr. Norman Spector.

The Committee's Findings — Main Points

Though CSIS has provided operational assistance to the Israeli officials in the past,

- The Committee found no evidence that CSIS was involved in any manner with the Meshal-Amman incident.
- We found no evidence that Israeli authorities consulted with CSIS about the assassination attempt before the fact.
- We found no evidence (in this incident or ever) of Israeli authorities requesting from CSIS the use of Canadian passports.
- Equally, we found no evidence of CSIS providing Canadian passports to Israeli authorities or turning a blind eye to their use.

Passport Misuse

In our review of CSIS files, we sought out information that would shed light on

whether the Service knew about and then passed to the Government information about the misuse of Canadian passports generally. We found that CSIS had provided comprehensive information to the Government on this issue, had fully investigated all cases of passport misuse by foreign intelligence agencies and, with one exception, had reported to the appropriate agencies of government all instances of suspected passport misuse.

In making queries about the single exception, the Service explained to us that it did not release the information because to do so would have jeopardized third party information from a foreign intelligence service.

With respect to the advice CSIS gave to government in this area, a Director in Canada's Passport Office — the agency of Government with prime responsibility for passport matters — told the Committee that the Service's information had been very helpful and that he knew of no instance in which relevant information had been withheld.

Intelligence "Bartering"

The Committee took note of allegations in the media that CSIS might have provided the Canadian passports or "looked the other way" in return for information from Israeli officials. We found no evidence of such arrangements between Israeli authorities and CSIS in regard to passports or any other inappropriate exchanges.

This conclusion is based on a review of the Service's files, and interviews with CSIS officers and diplomatic officials. Files that predated the *CSIS Act* were examined and retired CSIS officers who would have known about intelligence "bartering" arrangements were sought out and interviewed. None of the allegations were in any way substantiated.

The Committee acknowledges the importance of the "give-get" or *quid pro quo* principle in the intelligence world. However, we can see no substance to it in this case. We came to the conclusion that the story has entered the realm of urban mythology — an oft repeated story with no foundation in fact.

We came to the conclusion that the story has entered the realm of urban mythology — an oft repeated story with no foundation in fact

The Seized Passports — Forged or "Acquired"?

Jordanian authorities gave the two seized passports to Canadian officials. After conducting a technical examination of the passports, RCMP forensic specialists concluded that they were forgeries. The Service's technical specialists then performed their own examination of the two passports and concluded that,

- the passports were counterfeit in their entirety;
- the forgeries were of excellent quality; and
- that given the effort involved, the forgers probably produced the counterfeit passports in large lots.

The Service's information was distributed to the relevant Federal agencies responsible

for passports and for monitoring entry points into the country.

The Nature and Scope of CSIS-Israel Cooperation

In the aftermath to the assassination attempt in Amman, questions were raised in the media as to whether the relationship between CSIS and Israeli officials was restricted to information exchanges, or whether they had cooperated in operational matters.

The term "joint operation" is to be found in the Service's *Operational Policy Manual* and from the Committee's perspective its meaning is ambiguous at best

For the period 1992 through 1995, the Committee identified four matters in which there was cooperation between CSIS and Israeli authorities. We reviewed each of the cases to determine whether CSIS complied with policy, Ministerial Direction and the law. We detected a problem in one case and evident policy ambiguity in another.

Failure to Obtain Independent Confirmation

The first case involved assessments generated by Israeli officials and passed to the Service. In one element of the case, it was evident that CSIS failed to seek out independent confirmation of the shared information. We informed CSIS of our concern about the matter, which involved operational assistance (see below), and recommended to it a course of action.

A Policy Gap

Among the media speculation surrounding the Meshal incident was that CSIS and the Mossad were involved in "joint operations." The term "joint operation" is to be found in the Service's *Operational Policy Manual* and from the Committee's perspective its meaning is ambiguous at best.

This is illustrated by the second case, the only one that went beyond information exchange and approached that of a "joint operation." In it, CSIS provided assistance in Canada to foreign officials that was, the Service states, of an urgent and pressing nature. As such, and according to Ministerial Direction, a CSIS senior executive approved the activity and the Minister was notified after the fact.

The *CSIS Operational Policy Manual* contains provisions for "operational assistance" and "joint operations," and permits senior CSIS personnel to give approval to either form of operational cooperation if the situation is urgent and pressing. The Ministerial Direction, in comparison, states that "operational cooperation" with foreign services must as a rule be approved in advance, and that "operational assistance" can be authorized by senior Service officials in case of urgent and pressing need. The Ministerial Direction is silent on the issue of "joint operations."

It is the Committee's view that in both policy documents a number of key terms employed lack clear definition. The result is an apparent discontinuity between the guidelines in Ministerial Direction and the Service's policy manual which governs the conduct of individual CSIS officers. We believe steps should be taken by the Ministry and the Service to address these policy lacunae.

CSIS Role in Immigration Security Screening

Report #105

Scope and Methodology of the Audit

The main objective of this study was to understand the Service's role in assisting the Government with its Immigration Program and to assess the quality of the relationship between the Service and its interlocutors at Citizenship and Immigration Canada (CIC). Although the review focuses on CSIS' role in providing advice and information to CIC, we also examined that department's priorities and strategies insofar as they impact on the Service's functions. We learned, for example, that in 1998-99, CIC will focus its efforts on enhanced screening efforts at Canada's ports of entry, including offshore and at international airports. Thus, a corresponding increase in CSIS activities in these areas can be anticipated.

To carry out the study, SIRC researchers met with officials from CIC, CSIS, members of the legal community involved in immigration and refugee law from both government and the private sector, as well as representatives of non-governmental organizations working in the field. All relevant CSIS files, interview reports and the briefs sent to CIC were examined. In addition, the Committee conducted on-site audits at three Immigration Case Processing Centers abroad (two in the Middle East and the other in Buffalo, New York). We interviewed an Ambassador and several Immigration Program Managers in order to gain additional insight into the cooperative relationship. The CIC informed us that it views its working relationship with CSIS as extremely good.

The Nature of the Cooperative Relationship

Since the establishment of CSIS, a series of cooperative processes have evolved which define the mechanisms under which the Service assists the country's Immigration monitoring effort:

- the Immigration and Refugee Application for permanent residence (inland and overseas);
- vetting of applications from foreign officials and visitors to Canada;
- enforcement actions (arrest, detention, deportation);
- vetting of individuals claiming refugee status; and
- reviewing applications for citizenship.

Within these programs, the Service's authority for immigration screening is derived from sections 14 and 15 of the *CSIS Act*. The assistance rendered by the Service takes the form of information sharing on matters concerning threats to the security of Canada as defined in section 2 of the *CSIS Act* and advice to CIC in respect to the inadmissibility classes of section 19 of the *Immigration Act*. In addition, the Service carries out immigration screening investigations, including any necessary interviews.

Committee Findings

The cooperative mechanisms for each of the programs noted above are described in some detail elsewhere in this report [see Section 2: Investigation of Complaints,

It is evident to the Committee that the screening process overall is a difficult exercise in risk management

page 62]. The Committee's focus here was to examine activities the Service undertakes to assist CIC that impact on the cooperative relationship generally.

The Increased Use of Electronic Data Processing for Immigration and Refugee Applications

The most visible involvement of the Service in the immigration process is its participation in immigration security screening interviews

With respect to the Service's role in CIC's handling of Immigration and Refugee Applications for Permanent Residence within Canada and abroad, the Committee noted that electronic data exchanges between CIC and CSIS, and the use of pre-established security profiles, considerably reduced the time required for the screening process. Applications for permanent residence initiated from outside Canada — some 80 percent of the total of 215,000 applications — fall under the Overseas Immigration Screening Program. For these, the Service shares responsibility for screening with Immigration officials.

It is evident to the Committee that the screening process overall is a difficult exercise in risk management. There is a constant need to balance security interests against the requirements to fulfill the immigration program's goals in a timely and efficient manner. That the dilemmas associated with prudent management can be especially acute was highlighted in our review of two Middle East immigration posts. Obvious external factors such as geography and the local political situations, and organizational issues such as the capacities of foreign agencies to process the Service's requests for information, all impinge upon the nature of the Service's participation in immigration matters.

The Committee noted that consideration is being given to expanding the technological means currently used to process inland applications to include the processing of applications world wide. The wider adoption of such procedures should facilitate information sharing and at the same time standardize and augment the immigration screening process. We urge CSIS — in cooperation with CIC — to continue to pursue such improvements.

Terminology in a Revised Immigration Act

In the fall of 1996, the Minister of Citizenship and Immigration Canada announced the appointment of an Advisory Group to conduct an independent review of Canada's *Immigration Act*. The Legislative Review Advisory Group working independently from CIC focused on adjustments to legislation and policies that would be required in order to meet the objectives of Canada's immigration policies. Among the recommendations advanced by the Group was a proposal aimed at standardizing terminology across relevant portions of Canadian law. Specifically, they suggested that provisions in any new immigration act referring to an applicant's inadmissibility to Canada on security grounds should be congruent with the definitions of "threats to the security of Canada" contained in the existing *CSIS Act*. The Review Committee fully supports this recommendation.

Immigration Interviews and Screening

The most visible involvement of the Service in the immigration process is its participation in immigration security screening interviews.[3] Typically, arrangements

for the interview are made by CIC and are conducted by regional Security Screening investigators. It is often the case, however, that for various reasons an investigator from one of the Service's other operational branches is also present.

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.

The Committee, however, is also cognizant of the complexities which arise when the prospective immigrant is also the subject of a targeting authority, allowing CSIS to employ interview techniques which are more intensive than those routinely used in immigration interviews.

Immigration interviews in which CSIS investigators participate can only usefully serve as a means to address security-related concerns if the investigators are fully informed and the interviews skillfully conducted. In this respect, the Committee supports an initiative whereby CSIS will be provided with the notes of the relevant immigration officers whenever there is an immigration referral.

In examining the immigration screening process, the Committee reviewed written guidelines to CSIS officers. We found the Service's *Procedures Guidelines on Immigration Screening Interviews* to be inadequate in several respects. The Guidelines currently state that "the investigator should not create the impression that the applicant's cooperation with the Service could facilitate the processing of the application" — a statement we take to refer to the possibility of the applicant's recruitment as a source in the context of a pending application for immigration. In our view, the Guidelines should be less equivocal on the matter and state clearly that immigration interviews will not be used for recruitment or other unrelated purposes. The Service has informed the Committee that the Guidelines are in the process of being updated. We will review the new guidelines to see if this particular concern has been addressed.

The Guidelines should be less equivocal on the matter and state clearly that immigration interviews will not be used for recruitment or other unrelated purposes

In addition, the Committee is of the view that the screening process would benefit from an explicit reference in the Service's *Procedures Guidelines* to section 8(1) of the *Immigration Act*. Here it states that an applicant who seeks entry to Canada bears the burden of proving that he or she is entitled to enter this country, and that such entry would not contravene the *Act* or the other regulations. All applicants for entry into the country should be aware that non-cooperation with the screening process will prevent their applications from being processed.

The Committee is also aware, however, that in all but exceptional circumstances,

applicants are unable to address particular concerns until they are in possession of sufficient information about what is alleged. We believe that every effort should be made by CSIS within the obvious security constraints to release the maximum amount of information to the prospective immigrant. Our review of Service briefs to CIC identified ongoing efforts toward this end.

We believe that the Service's investigative expertise could be useful in interviewing applicants suspected of war crimes

Finally, with respect to CSIS briefs, our research found that some reports contained information derived from the CSIS computerized data base and open information. It is the Committee's view that reports on immigration interviews should contain only information collected during the interviews or, failing that, be unambiguous about what was or was not discussed at that time. In reading the reports, it was sometimes difficult to distinguish between what was said by the applicant, what was said by the interviewers to the applicant, or whether the information was from other sources altogether.

CIC's "War Crimes Strategy"

The Committee is aware that one of CIC's priorities is to strengthen Canada's ability to detect applicants suspected of war crimes or crimes against humanity. In view of the fact that the RCMP does not currently assist CIC in the conduct of screening interviews, we believe that the Service's investigative expertise could be useful in interviewing applicants suspected of war crimes. The Service maintains that as a matter of routine, it passes to CIC any war crimes-related information it obtains. The Committee believes that the Service's responsibilities in this area should be formalized and set out in policy.

Service Assistance in Enforcement and Interdiction

The Service participates in the recently established Points of Entry Interdiction Program of CIC. The role of CSIS is to provide advice in an expeditious manner to CIC on whether a particular individual wishing to gain entry poses a threat to the security of Canada. Immigration officials take this advice into account when making a determination about the eligibility of an applicant under section 19 of the *Immigration Act*. Until June 1998, the Service did not document or record these opinions. However, since then, CSIS documents all interdiction interviews it participates in. The information is held in the section 15 Security Screening Information System (SSIS), and is comprised of the subject's biodata as well as a reference to whether a report was submitted to the section 12 operational data base. Notwithstanding this procedure,

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

CSIS and Individuals Claiming Refugee Status

Of the nearly 26,000 refugee claims made in Canada in 1997-98, 60 percent were made at border points and the remainder at Immigration offices inland. When a person claims refugee status, senior immigration officers question the individual and request that a personal identification form (PIF) be completed. Officials then examine all of the available relevant documentation, such as passports, other identification, and travel

documents. The officers also photograph the claimant and take fingerprints. The fingerprints are forwarded by mail to the RCMP to ascertain whether there is another claim on file with the same fingerprints, and whether the claimant has a criminal record in Canada.

It is evident to the Committee that there are flaws in this process. In a review of refugee handling procedures, the Auditor General wrote that in most cases immigration officers rule on the eligibility of a claim without first obtaining the information required to make an informed decision.[4] Thus the evaluation of eligibility is essentially based on the claimant's statement.

The Committee's review also shows that before the refugee hearings are held, the refugee claimants' names are not, as a matter of course, screened against the data banks held by the Service. As we understand the original rationale behind the decision to proceed in this manner, immigration officials did not regard the screening of all refugee applications as a productive activity since at the time only 20 percent were approved by the Immigration and Refugee Board (IRB), and in any event, most were in Canada for a maximum of six months.

The situation with respect to refugee claimants is now substantially different. Since 1993, the overwhelming majority (99 percent) of refugee claimants have been ruled as eligible to seek refugee status, and an individual claiming refugee status can count on staying in Canada for much longer before a final decision is made. In recent years, close to 60 percent of claimants have presented themselves to Canadian officials without a passport, personal identification, or travel documents.

It is the Committee's view that in this quite different and much more demanding context, CIC needs to know as much as possible about would-be refugees as it pertains to threats to Canada's security interests. Claimants' backgrounds in Canada and abroad need to be known and understood, and we are convinced that CSIS has an appropriate role to play in this process.[5] Although CSIS is currently not involved in screening refugee applicants, there are ongoing discussions with CIC on this matter.

The Committee believes that CSIS should play a greater role in refugee matters, but that role should be carefully defined and transparent

CSIS already provides some information about refugees to CIC. We have noted, for example, several instances when individuals with refugee claims have appeared before the Immigration and Refugee Board, the CIC has opposed their claim employing information obtained from CSIS, and the IRB has subpoenaed Service officers to testify about information provided through affidavits. The Committee believes that CSIS should play a greater role in refugee matters, but that role should be carefully defined and transparent.

Complaints About Immigration Screening

The Committee is charged with the investigation of any complaints stemming from immigration screening interviews. We anticipate that they will provide the Committee with even greater insight into the Service's immigration role, and how the system functions in terms of legislation, policy and fairness. The first hearing of

such complaints is scheduled for July 1998. Others will be heard in September 1998.

A Foreign Conflict

Report #96

The Committee examined a set of CSIS investigations of groups and individuals implicated in an armed conflict in a foreign country. The purpose of our review was to determine whether the Service's investigations were appropriate in light of the threat posed by the targets chosen; and were conducted in accordance with the *Act*, Ministerial Direction and established CSIS policies and procedures.

Methodology of the Review

Our review covered the period from April 1995 through March 1997, and was focused on the Service's investigation of a well-known terrorist group and a small number of individuals. Examined by Committee researchers were all hard-copy and electronic files pertaining to the selected investigations as well as the advice provided to Government arising from them. The information compiled by the Service was both voluminous and varied. The materials we reviewed included:

- targeting submissions and authorizations;
- interviews with individuals linked to the terrorist group in question;
- evaluations of the threat posed involving international gatherings (for example the 1995 G-7 Economic Summit held in Canada), visits to Canada by foreign VIPs, and possible reprisals against certain embassies in Canada;
- reports from sources;
- information from foreign intelligence services or CSIS reports prepared from that information; and
- monthly reports on terrorism issues prepared by the Counter Terrorism Branch at Headquarters.

Background to the Service's Investigations

According to CSIS, a relatively small group of Canadians, landed immigrants, and refugees in Canada support or, at the very least, sympathize with the terrorist group in question. Some of these sympathizers have fled a checkered past to seek refuge in Canada, which serves as a staging and coordination area for terrorist operations elsewhere.

CSIS and the Use of Surveillance

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

The Service regarded the potential of the threat posed as especially serious in light of the particular combination of attributes possessed by the targets:

- certain of the extremists investigated have not sworn allegiance to any one group, but instead maintain relations at the highest levels with a number of terrorist organizations;
- some of the individuals targeted, although nationals of one country, take orders from or give direction to extremists of a number of other nationalities; and,
- certain of the extremists connected to the investigations are involved in multiple foreign conflicts at any given time.

Given the international dimensions of the investigations, CSIS concluded detailed intelligence-sharing agreements with a number of foreign intelligence services with which it maintains ongoing links. The exchange of information focused on three areas: international extremist movements; the role of certain organizations which were believed to provide documents, recruit activists, and support terrorist acts; and methods of communication between extremist groups and members.

The Committee's Findings

Based on our review, we came to the conclusion that in respect of this set of investigations, CSIS had in its possession sufficient information to warrant the targeting, and that in general, it conducted the investigation in accordance with the *Act* and its operational policies. We identified a number of facts and events which pointed clearly to direct threats to Canada's national security interests including, threats to life and limb of Canadian diplomats posted overseas and the possibility of a bomb attack in Canada.

The Committee took especially serious note of information provided to CSIS to the effect that a Canadian citizen was involved in a conspiracy to assassinate a politician in a foreign country. CSIS also learned that the individual was allegedly linked to several criminal activities inside Canada. When the Service's investigators witnessed criminal activities committed by the individual and accomplices, the police force of jurisdiction was duly informed.

This same individual attracted a great deal of interest overseas, resulting in numerous exchanges of information between CSIS and the intelligence services of other countries. The extent of these exchanges varied greatly. One country's service appeared impatient with the manner in which CSIS was supplying the requested information, and there was some friction between security services of another state and CSIS over a difference of opinion about the seriousness of the threat posed by another individual. It was evident to the Committee that these strains abated in the wake of the Service's continuation of its investigations.

While we were satisfied overall with the appropriateness of the Service's intelligence collection arising from the investigations, the Committee identified three operational reports on an individual's personal life that did not, in our view, meet the criterion of being "strictly necessary" as set out in section 12 of the *CSIS Act*. The Committee

The Service regarded the potential of the threat posed as especially serious in light of the particular combination of attributes possessed by the targets

recommended that the Service delete them from its data base and the Service has done so.

Coordination of Government Economic Security Efforts — the Service's Role

Report #92

The Committee's 1996-97 review of the CSIS economic espionage investigations revealed relatively little formal cooperation and coordination between CSIS and other government departments on economic security issues.[6] We also concluded that for CSIS to conduct meaningful investigations of threats posed by economic espionage, it would need to have access to additional technical and business-related expertise.

For this year's audit report, we sought answers to three questions: what mechanisms for coordination on matters of economic security among government departments and agencies were in place, what was the nature of the Service's participation, and what impact did these mechanisms have on CSIS investigations. Our inquiries for the audit covered Ministerial Direction given to CSIS and the Service's administrative cooperation files. The Committee also conducted interviews with staff in the Economic Security and Proliferation Issues (ESPI) Unit at CSIS Headquarters.

Current Cooperation and Coordination Mechanisms

ESPI has two specific areas of investigative responsibility: the threat of economic espionage directed against Canadian national interests, and the proliferation of weapons of mass destruction. Our most recent review showed that while ESPI has not been asked to participate in any formal coordination body in the economic security area, it does consult with and engage in joint presentations with other Federal Government departments and agencies, as well as liaise with law enforcement bodies.

We noted that ESPI refers clients to other agencies that are expert where the Service is not. In the course of Liaison/Awareness

Background to CSIS Economic Security Program

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

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

presentations, for example, the Service was sometimes asked by private sector contacts for more information on how they could ensure that their information systems were secure. In such cases, CSIS would refer the inquiries to the Communications Security Establishment.

The Service's product in the economic security area is directed to a wide range of domestic Federal Government clients, based on their needs. Among these clients is the Intelligence Assessment Committee (IAC) of the Privy Council Office (PCO). The IAC coordinates and facilitates interdepartmental cooperation in preparing analytical and assessment reports for Ministers and senior government officials.[7] CSIS participates in the process upon request by preparing reports for the IAC, though our review indicated that on issues of economic security, the requests are few and far between. CSIS contributions to the area have been on an *ad hoc* basis and mostly in the form of inter-departmental committee discussions. The Service has also provided intelligence on a bilateral basis to other departments, as well as through the production of intelligence assessments shared with domestic clients.

Committee Findings

In its 1996-97 Report, the Committee suggested that the Service could better fulfill its mandate in the area of economic security by making more use of technological and business-related expertise. One source of such information lies in other areas of Government. It is apparent to the Committee, based on this most recent review, that the dearth of coordination and cooperation between Government agencies is a reflection not of the Service's efforts, but of what appears to be the relatively low priority the Government of Canada as a whole gives to the issue. The development and maintenance of any formal cooperation process within government is a complex undertaking contingent upon the priorities and resources of the various government departments involved. The Service showed itself to be a capable and willing participant in the coordinating mechanisms that do exist, but these bodies devote relatively little effort to economic espionage matters.

The Service showed itself to be a capable and willing participant in the coordinating mechanisms that do exist, but these bodies devote relatively little effort to economic espionage matters

When our previous study found little ongoing cooperation with other government departments and agencies, we were concerned about the impact on the Service's economic security investigations. Notwithstanding the low priority apparently assigned to the subject by other agencies, the Service has said that its economic security investigations were not adversely affected by the lack of coordination in the area. Our review identified no evidence to dispute the Service's conclusion.

On the basis of both the 1997 and 1998 studies, we concluded that the Service has not devoted much in the way of resources to economic espionage investigations but that other sectors of Government appear to regard matters of economic security as having an even lower priority than does CSIS. It was also our view that the Service's definition of economic security encompassed more issues than many would agree are vital to Canada's security, that strong evidence of foreign government interference was elusive, and that some of the information the Service had collected

was not specifically linked to threats to the security of Canada.

In summary, we believe that the Service should clarify its definition of economic security in order to better focus its investigations and avoid the problems outlined above. This Committee sees CSIS as being limited by its mandate to the investigation of state-run intelligence agencies and their proxies in this area. We believe that the focus is not strictly on economic security, but rather foreign interference in Canadian society. If the Government of Canada wishes CSIS to go beyond this, it should introduce amendments to the legislation. We have been informed that the Service is comfortable with the direction it has received from the Government on this issue.

It was also our view that the Service's definition of economic security encompassed more issues than many would agree are vital to Canada's security

Exchanges of Information with Domestic Agencies

Report #95

In the course of discharging its mandate to investigate suspected threats to the security of Canada, CSIS exchanges information and intelligence with other Canadian government departments and police forces. The *CSIS Act* specifically provides for the Review Committee to examine both the exchange and cooperation agreements the Service has with other agencies, as well as the information and intelligence shared.[8] As a matter of practice, the Committee examines most CSIS exchanges of information on an annual basis, and evaluates the effectiveness of Service cooperation in two regional offices.

Methodology of the Evaluation

In sorting through literally thousands of information exchanges, the Committee looks for those that exceed the Service's mandate or are unnecessary. The goal is to assure ourselves that CSIS has the authority both to provide the information it shares with others and collect the intelligence others provide to it. We also review the content of the exchanges to determine whether personal privacy has been violated, and to ensure that the nature and scale of the information is proportional to the alleged threat posed by the individual.

An additional and equally important aim of our review is to assess the quantity and quality of inter-governmental cooperation at CSIS regional offices: has the Service adhered to the guidelines set out in its arrangements with other institutions; is it in compliance with the *CSIS Act*, with its own policies and procedures with respect to disclosure and liaison, and with Ministerial Direction.

Committee Findings

This year's domestic exchange report is unusual in that cooperation issues dominated our findings. In the two regional offices visited, we focused our review on the status of CSIS cooperation with other federal and provincial agencies.

CSIS and Law Enforcement Relations

Both CSIS regional offices we audited were experiencing difficulties in their relations with a particular law enforcement agency with respect to certain investigations. In one CSIS region, relations with a police agency were at an extremely low ebb during our audit because of a legal action underway at

that time. In view of the fact that the specific issue is the subject of a separate Committee review, we did not pursue the case in this audit. [See "A Problematic Case of Inter-agency Cooperation", page 32].

We did, however, inquire generally into the Region's problematic relationship. The CSIS Regional office stated that its operations had not been significantly affected by the legal case, and that in any event, the law enforcement agency in question was not central to Service investigations in the region. Our review of the region's information exchanges confirmed that the Service's primary law enforcement relationship was with another police agency, where relations continue to be excellent.

In the second region, the problem concerned an investigation against a target that the Service and the police had conducted in parallel. The Service was unhappy that it had not been given more access to police information and intelligence on the case, reflecting differences of opinion generally between the agencies over access to each other's information. We were assured by the regional office that the disagreements had not affected other investigations.

The Committee was unable in the time permitted to determine all of the factors contributing to the tensions between CSIS and the police. We believe that the relationship between the organizations warrants closer examination and a study focused on the issue is underway. One early conclusion we were able to draw from the current review is that conflict between the Service's requirement to protect its sources and the law enforcement need to use CSIS information in judicial proceedings is a source of tension. At the heart of this issue is the 1991 Supreme Court of Canada decision in R. v. Stinchcombe. [See the inset on the Stinchcombe ruling, page 31]

The issue of judicial disclosure weighs most heavily on CSIS counter terrorism investigations. The Review Committee will continue to monitor the impact — if any — of judicial disclosure on national security operations.

Conflict between the Service's requirement to protect its sources and the law enforcement need to use CSIS information in judicial proceedings is a source of tension

CSIS Cooperation with Citizenship and Immigration at Points of Entry

The Committee has taken note of a new initiative in which CSIS has undertaken to work with other federal agencies to improve existing procedures in regard to the interdiction at points of entry into the country of individuals known to be threats to Canada's security. Called the Point of Entry Alert Program (POEAP), an evaluation of it forms part of the Committee's review of immigration screening beginning at page 9 of this report.

CSIS Denied Access to Provincial Government's Information

The Committee's review identified a case where CSIS was refused access to information held by a ministry of a provincial government. Under the agency's interpretation of the province's privacy legislation, CSIS did not qualify as a "law enforcement body" and thus could not receive the information. CSIS suggested a number of options that would be consistent with the province's laws and still permit the sharing of appropriate information with the ministry in question. The Service also stated that it was still able

The Committee's review identified a case where CSIS was refused access to information held by a ministry of a provincial government

to access information from other agencies in the province under another provision of the same law. On the Review Committee's part, we had concerns about the inconsistent application of the law inherent in such a position and queried whether the Service could continue to have access to information held by any government body in the province. After reviewing the matter, we concluded that we did not take issue with the Service continuing to negotiate access with each ministry, as long as the latter had the statutory authority to release the information.

Exchanges Outside the Mandate

Three information exchanges between CSIS regional offices with other government agencies drew the Committee's attention. In the first, CSIS had received and retained section 12 ("threats to Canada") information in the absence of a targeting authority. We agreed with the Service's explanation that the reports were unsolicited and fell within the Service's mandate. In the second, we identified information CSIS had received from another agency that we believed was outside the Service's mandate to collect. And with respect to the third exchange, the nature of the information led us to question the Service's authority to pass on the information it had collected to a particular agency.

New Policies and Ministerial Direction for Information Exchange

CSIS has signed no new arrangements with other government agencies since 1996 and the Minister issued no Direction that would have impacted on the Service's exchanges of information and cooperation. We noted that the Service initiated new operational policy involving on-going cooperation with another federal government agency.

CSIS Liaison with Foreign Agencies

Report #98

Methodology of the Audit

Under section 38(a)(iii) of the *CSIS Act*, the Committee reviews the foreign arrangements entered into by CSIS with foreign police and intelligence agencies, and monitors the flow of information to agencies with which CSIS has arrangements.

This year, we examined two posts that are instrumental to the Service in its collection of information concerning extremism. The review encompassed the following material:

- all exchanges of information handled by the CSIS Security Liaison Officers (SLOs) at the two posts, including electronic exchanges;
- all correspondence with the foreign intelligence agencies handled by the posts; and
- all instructions and reference materials provided to and by the SLOs, including "Assessments of Foreign Agencies".

Our audit involved on-site visits to examine files and to conduct interviews with SLO personnel and others. At CSIS Headquarters, we reviewed the impact of the reorganization of the section responsible for foreign liaison, and the new logging system put in

place to track exchanges of information with foreign agencies.

Reorganization of Foreign Liaison Within the Service

As discussed in last year's audit report (page 4) CSIS recognized the increasingly important role of foreign liaison in security and intelligence operations by upgrading the Foreign Liaison and Visits Section to Branch status with a Director General-level appointment as its head.

In the course of the Committee's audit of the posts, two issues of relevance to the recent headquarters reorganization arose that we believe merit highlighting.

Need for Centralized Tasking Authority

The SLOs we interviewed underlined the need for increased coordination and monitoring of requests and tasking from CSIS Headquarters. Under current practice, each operational branch of CSIS tasks SLOs directly, creating sometimes competing and conflicting demands for SLO resources. Future reviews will focus on this issue.

Correspondence Tracking System

The second issue concerned the system (recently introduced) to track correspondence at the Service's posts abroad. In the Fall of 1997, all SLO posts' systems for logging electronic exchanges were upgraded to a system called the Correspondence Control Management (CCM) program. The Committee had noted in previous audit reports that the tracking system then in place was flawed. We are pleased that CCM appears to have alleviated the earlier audit difficulties.

Activities of Security Liaison Officers

CSIS Security Liaison Officers are stationed abroad to maintain and develop relationships with foreign agencies, to conduct security screening procedures, to report events and developments of Canadian security interest, and to assist Mission Security Officers resident in Canadian diplomatic missions abroad. They meet formally and informally with the representatives of foreign police and intelligence agencies. The Committee reviewed the SLOs' actions and activities and identified a number of problems.

Canadian Residents Traveling Abroad

In examining the requests for specific information made to SLOs from foreign agencies we identified situations where the policy guidelines governing SLO conduct were silent when it came to certain kinds of requests. For example, CSIS can ask foreign intelligence services to monitor Canadian residents who travel to other countries. We recently examined several such cases.

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

An Appearance of Offensive Intelligence Gathering

In the absence of an authorization from CSIS Headquarters, an SLO conducted inquiries of foreign intelligence officers about a terrorist who it was believed might attempt to enter Canada. Under existing policy and law, SLOs have no mandate to conduct investigations outside of Canada

We identified situations where the policy guidelines governing SLO conduct were silent when it came to certain kinds of requests

and must refrain from any activity that gives the appearance of offensive intelligence gathering. We have raised the case with the Service.

Agency Assessments

In order to assist CSIS generally to decide what types of information and intelligence can be released to foreign agencies, SLOs are charged with the responsibility of preparing "agency assessments" that comment on the reliability and human rights records of foreign police and intelligence services with whom they interact. For the two posts at issue, we found that the SLOs' assessments were accurate and appropriate, especially as they pertained to the prevailing human rights situations.

SLOs' assessments were accurate and appropriate, especially as they pertained to the prevailing human rights situations

Exchanges of Information

CSIS is able to exchange information with foreign agencies via several channels: visits of officials, through SLOs stationed abroad, and by direct electronic link. Review Committee staff examine the records of all these exchanges.

Information Exchanges Involving Individuals at Risk

One of the Committee's concerns is that information the Service shares with others does not put individuals at undue risk from foreign security services. At one post, while we observed a significant volume of exchanges concerning individuals, we also noted that CSIS reports did not identify persons in Canada, and instead focused on leaders of extremist groups rather than on rank-and-file members and supporters.

At the second overseas post, CSIS had requested trace checks from foreign agencies on a significant number of persons, and in a few cases, had made available detailed information from Canada-based investigations. The Committee found no evidence that the releases were excessive, or that the releases had resulted in harm to any person.

Inappropriate Information Sharing

The Committee identified an instance where the Service's sharing of information with a foreign intelligence service was questionable. CSIS handled a request from a Canadian law enforcement agency to ask several allied intelligence services to conduct records checks on more than 100 people suspected of being involved in transnational crime. The Committee found the grounds for some of the requests to be of doubtful validity. For example, one person about whom information was requested was said to have been "caught shoplifting."

We noted that the Solicitor General during the year under review issued a new Ministerial Direction whereby CSIS was directed to facilitate the relaying of transnational crime information from foreign intelligence and security services to the appropriate Canadian law enforcement agencies.

Foreign Liaison Arrangements

Under section 17 of the *CSIS Act* the Service, with the approval of the Solicitor General, can enter into an arrangement with a foreign agency. CSIS has some 212 such agreements with foreign police and intelligence services, many of which predate the *CSIS Act*. In 1985, following the establishment of CSIS, these arrangements were

deemed to be in effect (or "grandfathered") when the Solicitor General of the day approved them. The Committee's audit of the two overseas posts shed light on a number of policy issues having to do with CSIS liaison relationships generally.

Cooperation with a Foreign Agency for Which No Agreement Can Be Found

The Ministry of the Solicitor General produced in 1985 a compendium of CSIS arrangements with foreign governments and institutions comprising the Ministry's "understanding of all arrangements presently in place between the Canadian Security Intelligence Service and foreign governments or institutions of governments." However, in the case of one foreign intelligence service with which the Service has an on-going relationship, we could find no document to show that an arrangement for security intelligence exchanges existed prior to 1984. We have notified CSIS of this discrepancy.

Reactivating Dormant Arrangements

In the course of our review, 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. In examining the reactivation, the Committee found that while an informal, local consultation process occurred, there was no formal procedure in place to review the new circumstances. We also determined that there was no provision in CSIS policy or Ministerial Direction that would require CSIS senior management or the Minister — prior to any reactivation — to revisit the terms and conditions of an arrangement made under quite different 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.

Two Instances of Cooperation Outside the Terms of the Arrangement

The Committee identified a case wherein CSIS had discussed with a foreign intelligence agency several proposals for intelligence operations which the Committee believed were outside the mandate of the existing arrangement. The scope of the arrangement suggested to us that the planning activity undertaken in fact required Ministerial approval. The Service, on the other hand, interpreted the arrangement differently, asserting that the existing agreement did cover the discussions preceding operational activity. Although the operations were not in the end carried through and did not proceed beyond preliminary planning, we believe that CSIS policy and Ministerial Direction should re-address this issue so as to remove any ambiguity.

In another case, a foreign government required that information exchanged by all of its agencies flow through its intelligence service on the way to its eventual destination. With respect to immigration and security screening information, however, the Service's arrangements were with a separate agency in the same country. CSIS followed the foreign government's direction thus causing

The Committee's audit of the two overseas posts shed light on a number of policy issues having to do with CSIS liaison relationships generally

CSIS immigration and security information to be shared with an agency with which it had no appropriate agreement.

In light of the circumstances we observed, the Committee came to the view that the practice was inappropriate and so notified the Service. The Committee subsequently learned that CSIS had taken steps to regularize the situation by seeking the authority to alter its arrangements such that immigration and security screening information could be shared with the intelligence service concerned.

Implications for Foreign Liaison Policy

CSIS foreign arrangements are governed by a 1982 Ministerial Direction that predates the 1984 *CSIS Act* and employs terminology and describes administrative procedures that are not consistent with the *Act*. Less obviously, many of the definitions and

Background to the Service's Foreign Liaison Program

From the inception of CSIS in July 1984, until 1989, CSIS had a Foreign Liaison Branch. In 1990, the Service replaced the Branch with a new system for communicating with and coordinating the efforts of the SLOs. At the time, SIRC expressed its concern about the disbanding of the Foreign Liaison Branch. The Committee regretted the loss of what it described as "An intermediary... [that could] 'blow the whistle' on the inappropriate dissemination of information abroad."[9]

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

In a previous Annual Report,[10] we expressed concern about the number of SLO posts CSIS was closing and were of the opinion that, "the foreign liaison program would benefit from more attention from the Service, not less, as seems to be the trend in terms of representation overseas."

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

In 1994-95, the reporting relationships and responsibilities changed for both the section and the SLOs, as a result of an internal management study. Most notably, the overall management of the program was once again managed under the direction of a senior manager. In 1997, the program was raised to the status of a branch, headed by a Director General. As noted in last year's audit report, the Committee presents this year an evaluation of SLO activities under the new regime.

terms in the Direction are confusing and contradictory; this is particularly true of the definitions of scope which are ambiguous as to when the Minister must be consulted or advised. Compounding the problem is the fact that Service policies in the area are drawn from this early Direction.

For these reasons, the Committee wishes to repeat the hope expressed in last year's Annual Report that forthcoming Ministerial Direction, which is intended to replace the 1982 Ministerial Direction, will describe foreign arrangements in consistent and comparable terms, understandable by all elements of Canada's intelligence community.

A Comprehensive Review of Foreign Arrangements

Fully one-half of the Service's 212 foreign arrangements managed by Service SLOs posted abroad were entered into by the Security Service prior to the establishment of CSIS and, of these, many pre-date even the 1982 Ministerial Direction. The Committee is aware of Service procedures to report on certain arrangements annually, on a local basis. However, we have in past audits identified reports that favorably rated disreputable agencies, and we remarked on arrangements that had been left dormant for many years.

The Committee is cognizant of the need for CSIS to enter into new arrangements and build on existing ones with a view to enhancing Canada's national security interests. We believe that the imminent release of new Ministerial Direction will also provide the opportunity to ensure that all foreign arrangements, particularly those that pre-date the Service, are reassessed and annotated so as to bring them into compliance with the new Ministerial Direction and the *CSIS Act*.

> We recommend that CSIS systematically reexamine all foreign arrangements after the release of the new Ministerial Direction on foreign arrangements.

The Committee also recognizes that a reexamination of foreign arrangements in the manner we suggest has significant resource implications and will require a number of years to complete.

Fully one-half of the Service's 212 foreign arrangements managed by Service SLOs posted abroad were entered into by the Security Service prior to the establishment of CSIS

Investigations of Domestic Threats

Report #100

The Committee reviewed several investigations CSIS conducted during fiscal year 1996-97 which involved threats that were domestic in origin. One investigation was issue-based, while the others focused on groups and individuals suspected of posing a threat of serious political violence as defined in sections 12 and 2(c) of the *CSIS Act*.

Findings of the Committee

We concluded that in almost all the cases we examined, the investigations met these criteria and were conducted in accordance with Ministerial Direction and established CSIS policy. Suspicions about the targeted persons and groups were well-founded; the targeting level selected for each investigation was proportionate to the threat; and, in

almost all instances, the information the Service collected and retained met the test of being "strictly necessary" for the Service to be able to ascertain the nature of the threat posed.

The Committee did, however, identify a few Service reports containing information which, in our view, did not meet the "strictly necessary" standard. The Committee recommended that the Service remove this information — which pertained to sexual orientation and psychological distress — from its data banks. The Service has done so.

We also reviewed an affidavit for warrant powers, and the advice that CSIS provided to the Government on the investigations. We concluded that the information in these documents reflected accurately, and in a balanced manner, the data and the facts collected by CSIS, and that the assessment of the potential threat was justified.

Auditing CSIS Investigations

In the course of reviewing investigations conducted by the Service, the Committee has access to and examines any and all Ministerial Direction, hard-copy and electronic files collected, as well as the Service's advice to Government in respect of the investigations. The Committee seeks answers to four central questions:

- Were there were reasonable grounds to suspect a threat to Canada's public safety and national security as defined by sections 12 and 2(c) of the *CSIS Act*;
- Were the levels of the investigations proportionate to the alleged threat;
- Was the information CSIS collected strictly necessary; and
- Did the advice the Service gave to the Government accurately reflect the intelligence it collected.

CSIS Role in Preventing Politically Motivated Violence

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

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

CSIS Cooperation with the Royal Canadian Mounted Police - Part I

Report #101

In its investigation of suspected threats to the security of Canada, CSIS cooperates and exchanges information with Canadian government departments and police forces. The nature of the cooperation is usually set out in a formal agreement between the Service and the other agency. With regard to these arrangements, the Review Committee has a responsibility to examine all agreements and to monitor the provision of information and intelligence covered by them.

This year, we focused our attention on the Service's cooperation with the Royal Canadian Mounted Police (RCMP). The nature of the cooperative relationship between CSIS and the RCMP is of particular salience because the RCMP is a significant user of the Service's product and because the RCMP provides information and intelligence to the Service. And, of course, both organizations are essential components of the system which protects the security of Canada and Canadians.

In accordance with its responsibilities as set out in the *CSIS Act*, the Service may provide to the relevant police authority — municipal, provincial, or national (the RCMP) — information that may come into its possession concerning possible criminal activities. In embarking on a study of the CSIS-RCMP relationship, the Committee's interest was not only in this standing general responsibility, but as well, in the process by which CSIS and the RCMP exchange information about activities at the core of each of their mandates: CSIS to *collect and disseminate* information about threats to Canada and the RCMP to perform necessary *police functions* in relation to those same threats.

The responsibilities of each agency are set out in general form in the *CSIS Act*, the *RCMP Act* and the *Security Offenses Act*. Pursuant to subsection 17(1)(a) of the *CSIS Act*, the means and methods of cooperation are elaborated upon more specifically in an agreement between the two agencies. This Memorandum of Understanding (MOU), completed in 1990, is an expression of the Government's expectations in the area of RCMP-CSIS relations and provides the basis for all cooperation and liaison activities between them. In reviewing CSIS-RCMP cooperation, the Committee's goal was to identify any systemic problems in the relationship that would impact upon the ability of either agency to fulfill these expectations and execute the responsibilities each has in security-related matters.

The nature of the cooperative relationship between CSIS and the RCMP is of particular salience because the RCMP is a significant user of the Service's product

Undertaking the Review

The Committee's attention to the area was drawn by recent Committee reviews which revealed several instances of difficulty and disagreement in the CSIS-RCMP relationship. We wanted to determine the extent of the problem with a view to suggesting how cooperation could be improved in order to better protect Canada's national security interests.

In embarking on the study, the Committee believed that the contrasting organizational structures of the two agencies could become

We wanted to determine the extent of the problem with a view to suggesting how cooperation could be improved in order to better protect Canada's national security interests

a significant factor in any findings we might make about operational cooperation between the two agencies. CSIS is highly centralized, whereas the RCMP's operational structure is relatively dispersed and decentralized. It is inevitable, therefore, that some issues which arise first at the regional level are discussed and resolved between the agencies' respective headquarters.

Consequently, we structured our inquiry to proceed in two stages: the first, summarized in the current audit report, examines the state of relations between the two agencies at the headquarters level. It is to be followed at a later date by a review of relations at the regional and field office levels. As a result of this "two-stage" approach to the audit, we will draw most of our conclusions and set out recommendations, if any, at the completion of the second stage which we will report on in our next audit report.

Methodology of the Audit

The relationship between the Service and the RCMP is intensive and broadly-based. Both are heavy users of the other's information and intelligence, and the formal agreement between them provides for an extensive exchange on operational matters relevant to the other's responsibilities. Both agencies operate across Canada, and there is direct liaison and operational cooperation in the regions as well as at the respective national headquarters in Ottawa. In addition to operational matters, the agreement provides for considerable cooperation on non-opertional matters which is handled mainly at the national headquarters level.

Our review covered the first eight months of 1997, though we found that in some cases, events both before and after that period had to be taken into consideration to ensure balanced and objective conclusions. Material reviewed for the audit included CSIS hard-copy administrative files and its relevant computerized data base. Interviews were conducted with the Service's RCMP Liaison Officer, other senior CSIS officers, and their counterparts in the RCMP.

The Nature of Existing Liaison Arrangements

Consistent with the agreement between the Service and the RCMP, both have agreed upon and have established mechanisms to facilitate liaison and cooperation. These mechanisms are centrally managed at both headquarters and include the assignment of personnel to a liaison role at the regional level as well as at the national headquarters of the two agencies.

The liaison officials also act as a primary channel for the exchange of operational information and intelligence. They are given *conditional* access to material and information which their host agency regards as potentially relevant to the other's security-related responsibilities. The access is conditional in that the generating agency must decide whether to accede to the liaison officers' requests for further disclosure to, or use of the information by, the other agency. Under these procedures, it is intended that liaison personnel act to identify information of potential use to their own agency. In addition, certain other forms of information and intelligence on specific matters mentioned in the MOU

are routinely exchanged via direct agency-to-agency channels.

Results of the Review

Overall, the Committee concluded that the existing liaison mechanisms have had a significant positive impact on the relations between the RCMP and the Service, particularly in providing a better mutual understanding at all levels of respective roles and responsibilities. We observed cooperation initiatives being actively supported and promoted by the senior management at the headquarters of both agencies, and can also conclude that for the most part, the existing liaison mechanisms serve to identify developing problems at an early stage.

With respect to the non-operational areas of cooperation — much of which does not go through designated liaison officers but instead involves long-standing exchange arrangements conducted on an HQ to HQ basis — we observed no difficulties of consequence.

Problems in the Use of Operational Information Exchanged

Conflicting Responsibilities and Disclosure to the Courts

While the mechanism for the basic exchange of information appears sound, the Committee did identify areas of difficulty with respect to decisions by CSIS about which information is to be disclosed and how it is to be used by the RCMP. These problems arise when the responsibilities and interests of both parties conflict in respect of CSIS operational information to which RCMP liaison officers have been given access.

The primary role of the Service is to collect intelligence on threats to the security of Canada, using sources and investigative methods which must be protected in the interests of national security. The intelligence collected is not intended to be used in any way where its disclosure could reveal the Service's methods or sources. On the other hand, in carrying out its policing function, the RCMP has different responsibilities. In certain situations, these require it to take enforcement action the undertaking of which could oblige the Crown to disclose to the Courts information in its possession to support formal judicial proceedings. In such an event, the RCMP's information — including any obtained from the Service — is subject to legal discovery and challenge, thereby exposing the sources and the methods used in its collection to examination and public disclosure.

To prevent such an eventuality, and in properly exercising its responsibilities, CSIS places restrictions on the material and intelligence it passes to the RCMP. For example, CSIS-generated material cannot be used in formal legal proceedings without the express permission of CSIS Headquarters. This restriction has inevitably caused frustration within the RCMP, particularly among investigative personnel, who view it as a serious impediment to the efficient exercise of *their* responsibilities, and whose knowledge of the constraints on CSIS, may not be complete.

In general, we observed that at the headquarters level there were substantive efforts on all sides to understand the problems and constraints that faced both agencies. We noted a willingness on the part of CSIS

We observed cooperation initiatives being actively supported and promoted by the senior management at the headquarters of both agencies

management to accommodate the requirements of the RCMP whenever possible, particularly when the public interest in enforcement actions in a specific issue were seen to outweigh the operational and security concerns of the Service.

Some tension between the two agencies over the handling of CSIS-generated intelligence is inevitable

The Committee is aware that in certain respects, some tension between the two agencies over the handling of CSIS-generated intelligence is inevitable given the conflicting requirements. Nevertheless, incidents that came to our attention which in part gave rise to our study of the CSIS-RCMP relationship, indicate that there may be less to be sanguine about at the regional level. When we conduct our review in the regions we will be looking at the problem closely with a view to determining its seriousness and its implications for national security. The Committee will present its conclusions in the next audit report.

Potential Impact of the Supreme Court's Decision R. v. Stinchcombe

The mechanism described above by which CSIS material is protected from damaging disclosure was brought into question by the 1991 decision of the Supreme Court of Canada in the case of R v. Stinchcombe. In the view of some, the Stinchcombe decision held the potential to subject all CSIS intelligence information given to the RCMP to disclosure to the courts, regardless either of CSIS rules for its employment or whether the Crown chose to use the information in a prosecution. In such a case, any information passed by CSIS to the RCMP — oral disclosure, formal advisory letters, even meetings to discuss joint investigations — would be at risk of public exposure, thus undermining national security.

As a practical matter, however, the Committee has determined, as a result of its audit of the headquarters relationship between CSIS and the RCMP, that to date, the impact on the flow of information between the two agencies has been minimal. Nevertheless, both agencies are concerned that the current Memorandum of Understanding between them fails to reflect the realities of the situation and should be revised. The RCMP is planning to conduct an internal audit of the MOU in order to determine what changes need to be made.

The Committee is aware that a number of initiatives are being examined by various parts of Government in order to address the issues raised by R v. Stinchcombe, including possible revisions to existing legislation. The Committee intends to closely monitor this difficult issue.

Asymmetrical and Incomplete Access to Information

Another problem in the area of operational information exchange came to the Committee's attention through an earlier review conducted in the regions. CSIS places limits on access that the RCMP's liaison personnel initially have to the Service's information and intelligence. An RCMP liaison officer looking for potentially relevant information to request is only able to see material that originates in the CSIS region to which the particular RCMP liaison official is accredited; he or she does not have access to material arriving at the regional office generated elsewhere in the Service even though it may relate to matters the officer has already seen.

R. v. Stinchcombe 1991 3 S.C.R. 326.
The Stinchcombe case involved a criminal proceeding where the Crown had interviewed a witness who had given evidence earlier in the proceeding that was favorable to the accused. The Crown concluded that the evidence of this witness was undependable and decided not to call the witness in the trial. The defence sought disclosure of the interview in the belief that it might contain information favorable to its case. The Crown refused. The case went to the Supreme Court, which ruled in favour of a general duty of disclosure (other than for irrelevant information or information which was privileged) on the Crown (but not on the defence). Essentially the reasons for this ruling were:

1. Disclosure eliminates surprise at trial and thus better ensures that justice is done in a proceeding.

2. The duty of the Crown in a criminal proceeding is to lay before a trier of fact all available legal evidence: it is there to secure justice, not simply a conviction. Thus, the fruits of the Crown's investigation are the property of the public to be used to ensure that justice is done. (Defence Counsel, on the other hand, is there to defend the client's interests to the extent permitted by law.)

Stinchcombe, as such, did not deal with administrative law. The Court was careful to specify that in reaching its conclusions it was not to be taken as laying down principles for disclosure in circumstances other than criminal proceedings by indictment. For this reason, the Court did not look beyond the criminal law setting in its analysis. Notwithstanding the Court's express attempt to limit the impact of its ruling and notwithstanding the criminal nature of the proceedings, the decision has been extended to administrative proceedings. Numerous cases have emerged inspired by the principles enunciated in Stinchcombe.

In short, RCMP liaison personnel may have to make a determination about the relevance of certain intelligence material in circumstances of less than full knowledge of the existing information.

While the problem was not considered by the senior RCMP headquarters officials we interviewed as particularly serious, our earlier findings in the regions lead us to believe that there exists at least the potential for CSIS information vital to the RCMP's role and responsibilities being overlooked. The Committee believes that this issue should be examined by the headquarters of both agencies to ensure that procedural and structural factors such as these are not the cause of an intelligence failure. We intend to revisit the matter during the second segment of our study.

RCMP liaison personnel may have to make a determination about the relevance of certain intelligence material in circumstances of less than full knowledge of the existing information

Avoidable Overlap in Agency Responsibilities

The Service and the RCMP have responsibilities that sometimes involve overlapping areas of operational activity. For the most part, however, these do not present serious difficulties since the agencies have clearly defined and complementary roles set out in legislation. However, the Service has begun to devote increasing resources to an area of growing concern for all countries — the rise in transnational crime. While such an initiative may be appropriate, if not handled well and defined with precision, it has the potential of generating disagreement with the RCMP and reducing the overall efficiency of the cooperative relationship.

Cooperation between the two agencies in this area is quite recent, yet the Committee has seen early signs of disagreement. We observed that the Service's role was not fully understood by some RCMP operational personnel, who had expectations about the level of CSIS input that CSIS was not prepared to meet. In addition, we found that the terms used by CSIS to describe or circumscribe its own role and that of the RCMP in the area — words such as "strategic" and "tactical" — lacked sufficient clarity in order to be very helpful in defining areas of responsibility. For its part, the Service asserted that intelligence and law enforcement personnel do understand these concepts.

While we believe the Service may have an important role in addressing the problems of transnational crime, it is essential for a continued, productive inter-agency relationship that the role be clarified and formalized in cooperation with the RCMP. The Inspector General of CSIS has looked into the matter and the Committee intends to conduct its own study.

A Problematic Case of Inter-agency Cooperation

Report #103

In 1997, SIRC reviewed a CSIS investigation of persons in Canada who were associated with an internal armed conflict in an overseas country. During the course of the review, we identified a number of potential problems arising with respect to information the Service had provided to a Canadian law enforcement agency and a government department about a person who was the subject of CSIS investigation.

Following on allegations that the person had been involved in a foreign armed conflict, the Service commenced its investigation. While the investigation was still on-going, the law enforcement agency concerned engaged the subject to perform duties involving classified information. The person was subsequently investigated by the law enforcement agency and prosecuted for certain criminal offences.

Although the law enforcement agency had access to information CSIS had collected about the person, at first it took no action in light of the situation prevailing at the time. Later on, when the law enforcement agency learned from another source that the person was alleged to have been a party to

a foreign armed conflict, it did undertake its own investigation.

Information Disclosure Procedures

The Committee concluded that the lack of early action on the part of the law enforcement agency probably occurred for two reasons. Because of the way the system operates, the law enforcement officers located at CSIS had access to only part of the information held by the Service. The regional liaison officer did not consider the information he saw to be sufficiently noteworthy to inform his colleagues in the law enforcement agency, though, in retrospect, it was thought to be relevant to the criminal investigation. Second, the CSIS investigator concluded that the individual under investigation was not a security threat and, therefore, saw no need to pursue the matter further.

Tensions in the Inter-agency Relationship

The Committee's review of events shows that attempts to prosecute the subject caused additional difficulties between the two agencies. The police needed information from the Service to pursue the case, however, instead of following the established liaison procedures for obtaining the assistance of the Service, it employed subpoena powers to compel the attendance of CSIS officers as witnesses at the trial.

While the CSIS witnesses in the end did not testify because the charges relating to their information were dropped for other reasons, the Service believed it had cause to be concerned about the manner in which its assistance was being compelled and its information used. The recent Supreme Court ruling regarding discovery and disclosure underscores the need for proper inter-agency consultation and cooperation in the area of prosecutions involving information collected by the Service.

The second problem arose when the law enforcement agency attempted to use judicial proceedings to have the person deported from Canada. Information about the subject provided by the Service to another federal government agency with which the police was in contact appeared to have the effect of undermining the law enforcement agency's efforts. However, instead of employing any of the inter-agency consultation procedures in place, the law enforcement agency obtained a search warrant to obtain a CSIS document from a third federal government agency. To obtain the search warrant, the law enforcement agency alleged criminal wrong-doing on the part of CSIS employees. The Service states that it would have provided any information or document upon request.

The Committee believes that the Service should have provided more information about the subject to the Federal Government department concerned

The Committee's Findings

In the Committee's view, several factors led to the above events, possibly including the strong perceptions of one of the key individuals involved in the case within the law enforcement agency, as well guidance to the agency provided by the Crown Counsel involved.

First, it is evident to the Committee that when the law enforcement agency hired the person concerned, it did not subject him to the stringent Federal Government security checks required of individuals privy to sensitive information. The law enforcement

agency did not seek security screening information from CSIS and so was unaware of the allegations against the subject. While the Committee has no mandate to review the actions of the law enforcement agency, we believe there is a reasonable likelihood that none of what transpired as described above would have occurred had the Service been asked to screen the employee.

Second, the Committee believes that the Service should have provided more information about the subject to the Federal Government department concerned. A more complete assessment would have resulted in the Department being better able to address the law enforcement agency's case for deportation. The Service asserted that it would have violated the "third party rule" if it had provided more information, and that, in any event, the only important part of the letter was the Service's conclusion that the individual in question did not pose a security threat to Canada.

Third, and most important, these events underline the vital importance of sound consultative procedures between the Service and law enforcement agencies. Because of their very different mandates, the potential for misunderstanding and misperception is inherent to the work each carries out. The test of a good inter-agency relationship which serves the security needs of the country is one in which the inevitable tensions and difficulties can be dealt with quickly and constructively, on a case-by-case basis.

Areas of Special Interest — Brief Reports

When Is a Source a Source? When Is an Institution Sensitive?

Report #99

Subsequent to learning of allegations that the Service had sent a source to report on activities that could be construed as having taken place in the context of a sensitive social institution,[11] the Committee conducted a review of the matter. Our aim was to ascertain the relationship of the source to the Service, the source's activities, and whether the actions of those persons associated with CSIS complied with the laws of Canada, Ministerial Direction, and the Service's policy.

Based on our review, we concluded that no laws were broken, and that CSIS collected information on persons about whom there were reasonable grounds to suspect may have represented threats to the security of Canada. However, we did identify a potential weakness in existing policy. The relative brevity of time during which the person acted on behalf of the Service meant that a standard senior management source approval procedure was not triggered. The Committee saw this as a policy problem that ought to be addressed, and we communicated our concerns to CSIS. The Service did not agree with our assessment. Since the events described, Service policy has been changed. The time condition for management approval no longer applies.

Lawful Advocacy, Protest, Dissent and Sensitive Institutions

Sensitive operations invariably involve the use and direction of human sources, and while human sources can be the most cost-efficient form of intelligence collection, their use also entails the greatest risk in terms of impact on societal institutions, legitimate dissent, and individual privacy.

The CSIS Act specifically prohibits the Service from investigating "lawful advocacy, protest or dissent" unless carried on in conjunction with threats to the security of Canada as defined in the *Act.* The Service is obligated to weigh with care the requirement for an investigation against its possible impact on the civil liberties of persons and sensitive institutions in Canada, including trade unions, the media, religious institutions and university campuses.

In addition, the Committee attempted to determine whether the venue for the CSIS operation did in fact meet the criteria for a "sensitive institution" — a situation for which there exists specific policy direction requiring that CSIS exercise special care. While we concluded that there was insufficient information to reach such a conclusion, we also noted that the Service's definition of a sensitive social institution may be unduly restrictive. The Committee intends to pay close attention to this issue in future reviews.

A Human Source Operation

Report #102

Periodically, the Committee conducts special reviews of human source operations where there is a high risk or where a routine audit identifies an operation that we believe warrants a more in-depth examination. The case described below meets both criteria.

The two objectives of our review were to assess whether CSIS complied with the *CSIS Act*, Ministerial Direction, and its own operational policies, and to evaluate whether the risks inherent in this human source operation were justified by the information provided by this particular source.

The source was a controversial figure prior to his recruitment by CSIS. Operational policy gives senior officials the authority to approve this kind of recruitment, and the proper approvals were obtained. For the operation generally, we found that the Service adhered to the letter of Ministerial Direction and its own operational policies. For instance, when the source's activities jeopardized the integrity of the operation, CSIS suspended the relationship.

There were, however, two areas where the Committee did take issue with the handling of the source. The first concerned management practices internal to the Service. Given the potential problems that could

have arisen upon the source's suspension, we believe the Director of the Service should have been informed at the time of the decision to do so.

The second concern bore on the Service's decision to resume a relationship with the source after the initial suspension. Based on our assessment both of the source's controversial actions and the intelligence generated, the Committee was troubled by the Service's decision. The Service's comment to us in this regard was that its decision to resume contact was based primarily on his potential to provide important information in the future.

We examined the issues surrounding a serious security breach that took place within the Service several years before

Internal Security Measures

During the course of our 1997 audit, we examined the issues surrounding a serious security breach that took place within the Service several years before. When the problem first came to light, the Solicitor General directed the Inspector General of CSIS to review the matter. In the report prepared subsequently, the Inspector General stated that certain elements of the existing internal security policy were inadequate with respect to what should have been the Service's initial response to security breaches of the kind that occurred. The report also noted that policies and procedures regarding document control and site management had not been followed, and that other security practices were in need of remedial corrective efforts.

For its part, the Committee reviewed the measures subsequently taken by the Service to resolve the security weaknesses. We also examined the Inspector General's recommendations in the matter. In our view, CSIS has been fully responsive to the requirements of the situation. Document control procedures, site management, and employee internal security awareness have all been improved.

CSIS, like all federal government agencies, is obligated to comply with the Government Security Policy as set by Treasury Board. There are policies mandated by other agencies as well — for example, encryption standards are set by the Communications Security Establishment. The CSIS security policy manual elaborates on and, in some case, enhances these standards. In addition, employees of the Service are expected to know and comply with security policies; managers are responsible for their unit's performance; and CSIS human resource policies set out penalties for non-compliance with established policies, including the failure to report potential security problems.

Consequently, the Committee believes that in addition to the corrective measures already undertaken, CSIS should broadly reexamine the security policies and practices which impact on both Service responses to warnings of imminent security problems and the investigative tools available to it once they have occurred. CSIS should also consider conducting more frequent audits of employee access to its internal electronic data bases.

A Case of Historical Interest

Report #104

In the course of a previous review, the Committee located documents showing that CSIS had been in receipt of information from a foreign source about a Canadian who had allegedly spied for a hostile intelligence service in the distant past. The files also indicated that the Service had provided assistance to the RCMP in a criminal investigation of the person in question.

The Committee's interest in the matter was three-fold: to learn under what authority a CSIS employee assisted the police in what seemed clearly to be a criminal matter; to determine what the Service was seeking to gain from a case of mainly historical interest; and to review the authorizations under which Service contact with the foreign service was made.

Our review led us to understand that the foreign source was an intelligence service with which the Service had no arrangement at the time it received unsolicited information about the alleged espionage. Prior to the transfer of information, the Solicitor General had authorized the Service to establish contacts with the foreign agency concerned with a view to setting up a formal agreement. However, there is no record of Ministerial approval having been given for the Service to request a transfer of substantive information from the foreign source.

The foreign agency offered the initial information about the agent as a gesture of good faith and subsequently provided access to all of the documentation after a request from CSIS. The Service regarded the case as a means to assess the openness of the foreign agency.

The Committee's Findings

Notwithstanding the fact that CSIS obtained a targeting authorization on the alleged agent, it is the Committee's view that Ministerial permission was required prior to receiving the bulk of the "unofficial" information from foreign officials. The Service attested to the fact that the Minister was informed on several occasions about the activity and did approve of this form of liaison with the foreign agency, though the written record was silent. It is clear that the information received was vital to the unmasking of past espionage against Canada.

CSIS had been in receipt of information from a foreign source about a Canadian who had allegedly spied for a hostile intelligence service in the distant past

The Service affirmed that the information it received was unsolicited and thus did not require Ministerial approval, though it was given. We concluded that the nature of the interaction required the Solicitor General's consent.

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

In the matter of the Service's cooperation with the RCMP's criminal investigation, our review indicates that it fully complied with the Memorandum of Understanding between CSIS and the RCMP which provides for foreign liaison assistance and support with foreign agencies on security-related matters. The files show that CSIS performed a liaison function — facilitating the RCMP's

meeting with foreign officials — and did not participate in police interviews. The Committee was satisfied that the Service cooperated with the RCMP within the parameters of operational policy, procedure, and the *CSIS Act*.

The Committee audits the entire range of CSIS investigative activities — targeting, special operations, surveillance, warrants, community interviews and sensitive operations — in a particular region of Canada

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

Report #97

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

The Targeting of Investigations

The targeting section of the regional audit focuses on the Service's principal duty — security intelligence investigations authorized under sections 2 and 12 of the *CSIS Act*. When examining any instance in which CSIS has embarked on an investigation, the Committee has three central concerns:

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

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

Methodology of the Audit

In the region at issue, the Committee randomly selected ten investigations conducted by CSIS during the 1996-97 fiscal year. However, because of changes to the Research Staff complement in the course of the review, the Committee limited the audit to seven investigations — five counter terrorism cases and two counter intelligence cases. SIRC researchers reviewed all files and operational messages in the Service's electronic data base. Researchers also interviewed the CSIS officers who carried out the investigations as well as the managers who oversaw them.

The Committee's Findings

In all cases, the Committee found that CSIS had reasonable grounds to suspect a threat to the security of Canada. The targeting levels were proportionate to the seriousness and imminence of the threats, and no actions were taken against non-targets. The Committee concluded that the Service, in most of the cases we reviewed, collected only the information that was strictly necessary to advise the government about the threats. Several cases, and the

Management of Targeting

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

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

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

issues they raised for the Committee, are summarized below.

An International Movement

With respect to the first case, the Service's Counter Terrorism Branch submitted a Request for Targeting Approval (RTA) to the Target Approval and Review Committee (TARC), to allow the Service to investigate a terrorist threat emanating from several persons and groups who were associated with an international movement. The Targeting Committee approved the request and operating under the approval, the CSIS Regional office conducted the investigations.

In its audit, the Committee focused on the Region's investigations of the threat posed by two terrorist groups from another country which CSIS viewed as having the potential to conduct acts of politically-motivated violence in Canada. While the Service based its assessment of the threat in part on the groups actions in other countries, the Committee noted that openly available analyses of the international movement were not unanimous on whether the movement possessed the ability to control events in different parts of the globe. We found that the Service's own studies reflected a similar ambiguity.

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

The Committee focused on the Region's investigations of the threat posed by two terrorist groups from another country

The Region conducted three investigations under the targeting authority. The first stemmed from allegations that three persons were linked to the two terrorist groups. The Service's inquiries revealed that the allegations were unfounded.

A second investigation resulted in the Service learning about sometimes violent factional clashes in a community. The Service acknowledged that although it believed initially that there were reasonable grounds to link these persons to a terrorist organization, the investigation found no such evidence. Instead, the Service concluded that the suspect activities were criminal in nature and not politically motivated. Conforming to standing rules in such situations, the Service turned the information over to law enforcement organizations and did not pursue the matter further.

The third investigation dealt with the activities and movements of a foreign national suspected of having contact with extremist groups. As with the factional clash investigation noted above, at the outset of the review the Committee had some misgivings about the Service's investigation since the person involved was not clearly linked to the terrorist group. CSIS' investigative efforts failed to clearly establish that the groups were active in politically-motivated violence in the Region.

Notwithstanding the Committee's view that the targeting document did not establish a strong case against the targets, it is our view that international events at the time gave the Service reasonable grounds to pursue possible threats to the security of Canada, and that the resulting investigations were reasonable and proper.

A Foreign Program

The second case involved a counter intelligence investigation where evidence of a threat proved from the Committee's perspective, at least initially, to be somewhat elusive. The Target Approval and Review Committee had authorized a low-level investigation of a person who came to Canada as a participant in an international employment program that the Service believed was sometimes used by a foreign state to carry out acts of economic espionage. The Service subsequently sought and was

given increased investigative authority to permit it to collect more information.

The Committee learned that the stimulus for the investigation of this person — and others participating in the same program — could be found in two parallel investigations: the Service's inquiries into the clandestine activities of the foreign intelligence service of a particular country, and CSIS' authority to investigate generally activities of any foreign state directed against Canada's economic interests.

The Service's interest seemed to focus on the target's employment prior to that connected with the work program in an area the Service considered may have been vulnerable to foreign espionage. Ultimately, the Service found that the target had only limited access to confidential documents and had brought more expertise to Canada than the target could have obtained here. The Service terminated the investigation. The information collected did not suggest that the subject of the investigation was in contact with foreign intelligence officials.

The key issue raised by the case for the Committee lies in the nature of the information that prompted CSIS to target the subject in the first instance. The Service had received information from foreign sources that led it to launch its investigation. CSIS commented that the investigations of others in this program were inconclusive. The Committee was not comfortable with the Service obtaining information on other participants in the subject's program in the absence of strong information that they posed a threat or that their expertise pertained to vulnerable economic sectors in Canada.

A Sensitive Investigation

A third case which drew our attention concerned the threat of politically-motivated violence in Canada. The Service investigated a person believed to have been involved in activities on behalf of an international terrorist organization. In its request for targeting authority, the Service stated that the target held a position as a member of a sensitive social institution and had the potential to use the institution to further the objectives of the terrorist organization.

Explicit rules are in place which govern the Service's conduct of investigations dealing with members of sensitive social institutions

Explicit rules are in place which govern the Service's conduct of investigations dealing with members of sensitive social institutions and the Committee found that the Service acted in complete accordance with these policies. Because of the sensitivity of the institution to which the individual belonged, CSIS Headquarters issued specific parameters to the Regional office on how the investigation was to be conducted.

While the Committee did not identify any breaches of the directives, we did become aware of concerns expressed by the Region to CSIS Headquarters that the parameters it was directed to follow tended to limit the stated objective of the targeting authority — to understand whether the subject was improperly using the position in the sensitive institution. CSIS Headquarters responded to the effect that the limitations would not impact on the value of the investigation and, in any case, were appropriate given the nature of the institution involved.

The Committee concluded that the issue had been appropriately resolved.

Failure to Obtain an Authorization

The Committee identified one exception to the general conclusion that targeting decisions in the Region were authorized in accordance with the Service's internal rules and directives. Upon review of an investigation of a counter terrorism threat, the Committee found that contrary to Service policy, Regional investigators had failed to obtain a senior official's authorization before conducting interviews with a representative of a sensitive social institution. The Committee drew the attention of CSIS to the matter and we were subsequently informed that corrective action had been taken.

As we stated last year, the Committee strongly believes that CSIS needs to rigorously maintain precision in its affidavit drafting

Obtaining and Implementing Federal Court Warrants

Under the *CSIS Act*, only the Federal Court can grant CSIS the right to use warrant powers, such as telephone or mail intercepts. In requesting such powers, the Service presents an affidavit attesting to their need to the Court. Every year, the Committee audits a number of affidavits by comparing them with the information in the Service's files. We have three related questions in mind:

- do the facts stated in the affidavit accurately reflect the information used to substantiate the affidavit;
- is the case presented to the Court in the affidavit set out in its proper context; and,
- are the facts and circumstances fully, fairly and objectively expressed in the affidavit.

Committee Findings

In 1996-97, the Committee reviewed two warrant affidavits in depth, both investigations falling under the direction of the Counter Terrorism Branch. Both affidavits were large, with one having over 200 references and supporting documentation filling seven three-inch, loose-leaf binders.

Warrant Preparation

In the two affidavits, we found several cases where CSIS omitted information that would have added context to its attestations. While the Committee is not able to set out details because of national security requirements, we can say that in some instances information that may have been relevant to certain statements of fact was missing. In some other cases, the statements in the affidavits proved to be a combination of factual information and the interpretations of CSIS experts. It is evident that the merging of fact and belief served to strengthen the Service's case. The Committee is of the view that any statement of belief in an affidavit should be clearly identified as such.

Proper affidavit preparation lies at the core of the entire targeting and investigatory process. As we stated last year, the Committee strongly believes that CSIS needs to rigorously maintain precision in its affidavit drafting. The Committee will continue to monitor the Service's procedures for writing affidavits in order to ensure that all legal requirements are scrupulously observed.

The Warrant Process

In order to obtain warrant powers under Section 21 of the *CSIS Act*, the Service prepares an application to the Federal Court with a sworn affidavit justifying the reasons why such powers are required to investigate a particular threat to the security of Canada. The preparation of the affidavit is a rigorous process involving extensive consultations with the Department of Justice, and the Solicitor General, with the latter's approval being required before a warrant affidavit is submitted to the Court. The facts used to support the affidavit are verified during the preparation stage and reviewed again by an "independent counsel" from the Department of Justice to ensure that the affidavits are legally and factually correct prior to the submission to the Federal Court. This process has evolved over the past several years with a view to ensuring that the facts, and statements of belief based on those facts, are accurate.

Warrant Tracking

The process by which CSIS tracks warrant applications is also of interest to the Committee. Normally, warrant applications and affidavits are assessed by an independent legal counsel from the Department of Justice prior to submission to the Federal Court. The Committee identified no anomalies in warrant tracking procedures.

Approval of Warrants

The law requires the approval of the Minister for all warrant applications. We noted that the Minister issued instructions to the Service to the effect that he is to be informed in advance whenever the Service proposes modifications to warrant applications that involve targets, warrant powers or any other substantive matter. The Minister stipulated that he is to be advised, preferably in writing, but verbally if the changes involve unacceptable delay.

During the coming year, the Committee intends to examine the use of warrants and warrant provisions.

[For more on the Service's handling of Federal Court warrants generally, and changes in warrant policies and procedures, please see page 46 of this report]

Quality Control in Reporting

Because intercept reports provide the basis for requests for warrant powers — and within CSIS, for targeting authorities — accurate reporting and transcription of material generated by warrant intercepts is vital. We found that the Region's past standard practice of ensuring quality control through a program of random testing had been interrupted for an extended period. We believe that this was the result of resource reductions in CSIS. The Service noted that the suspension of quality control procedures would be resumed at the earliest opportunity. The Committee will revisit CSIS quality control procedures during future regional audits.

Audit of Sensitive Operations

The very nature of sensitive operations dictates that they are the subject of relatively

frequent Ministerial consultations. In addition, policy for implementing sensitive operations is set out in some detail in the CSIS *Operational Policy Manual* and all requests for sensitive operations require at a minimum, depending on the level of sensitivity, the approval of Service senior management.

In the cases the Committee reviewed, no unwarranted collection of information involving sensitive institutions was identified

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

Committee Findings

Senior Management Approvals

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

The Committee did review a case in which the Service took three years to proceed with an authorization. The source in question was involved with religious institutions, and while the Service had initially decided that an authorization was not required, we disagreed with this position and so informed the Service.

Ministerial Approvals

According to Ministerial Direction, any use of a source on a university campus must be approved by the Solicitor General. As we reported last year, new Ministerial Direction on campus operations delegates authority to the Director of CSIS in "specified circumstances." In the cases we examined, we were satisfied with the Service's decisions to seek Ministerial authorization.

Administration of CSIS Sensitive Operations

CSIS sensitive operations require centralized control and management. We found that in almost all the cases that we reviewed, the operations conformed to policy. 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.

Sources in Conflict of Interest

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 instruction outlined the steps to be taken to avoid such situations and how to respond when they did occur. 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.

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 conditions[14] 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.

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

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*);

- 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 Immigration[19]

Immigration and refugee applications from within Canada for permanent residence

CSIS has the sole responsibility for screening immigrants and refugees[20] 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 Act[21]

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 Index[23]

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 quickly[25] since the objective is to obtain a voluntary departure, issue an exclusion order, or prepare a security certificate.[26]

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 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

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 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 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]

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

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.

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.

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

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

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

As a result of the Committee's research efforts during the past year, we came across some files the Service had inherited from the RCMP Security Service that did not appear to have been reviewed for possible disposal or archiving within their specified retention period. On pursuing the matter further, it turned out that one of the files had apparently been overlooked, sparking a comprehensive records check on the part of the Service. As a result, CSIS identified a block of files that had escaped notice for a second review by the file management system. The Service subsequently took measures to dispose of the files. The Committee will report on this activity in our next annual report.

File Disposition

During fiscal year 1997-98, CSIS National Archives Requirements Unit (NARU) reviewed 13,518 files which had come to their attention through the regular archival Bring Forward (BF) system. Of the 13,518 files reviewed, 7,312 files were destroyed, 6,206 files were retained and none were sent to the National Archives of Canada (NAC). However, 14 files were determined to be of archival value and they will be sent to the National Archives once their retention periods expire.

New File Statistics

In comparing the file statistics for 1996-97 and 1997-98, we noticed an increase in the number of files on foreign nationals visiting Canada where the issue was counter terrorism. The number of files on right-wing extremists declined, however. The security screening files showed only minor fluctuations in the categories of citizenship, immigration and refugees.

The Committee constantly monitors the Service's file management policies and practices to help ensure that no unnecessary information is improperly retained or distributed

The Committee is cautious about drawing conclusions from these observations. By itself, neither an increase nor a decrease in raw numbers reflects a change in the level or nature of threats to national security. Instead, the numbers may represent a higher degree of interest in a particular area (an increase) or a narrower focus on particular persons or groups (a decrease) on the part of the Service.

Personnel Recruitment and Representation Within CSIS

Recruitment of Personnel

CSIS held two Intelligence Officer Entry Training (IOET) classes for its new recruits in 1997-98. Thirty students graduated, and all met the criteria for bilingualism. There were no conversions from other job categories in the Service; all trainees were outside applicants. In addition, the Service

held two Intelligence Officer Investigator's Courses in 1997-98. Eighteen out of the nineteen students successfully completed this course.

Representation of Canadian Population in the Service

The female to male recruitment ratio this year was nineteen females to eleven males, a change from last year's ratio of seventeen to thirteen. There were three members of visible minorities employed by CSIS, a decrease of one from last year.

Over the last two years, the percentage of women in the intelligence officer category increased from 23.7 to 27.3%. In the same time period female recruitment in the senior management level rose to 11.5% from 9.5%. The number of visible minorities went from 1.3% to 2.5%.

Section 2: Investigation of Complaints

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

- The Committee is constituted as a quasi-judicial tribunal to consider and report on any matter having to do with federal security clearances, including complaints about denials of clearances to government employees or contractors.
- The Committee investigates reports made by Ministers about persons in relation to citizenship and immigration, certain human rights matters, and organized crime.
- As set out in the *CSIS Act*, any person may lodge a complaint with the Review Committee, "with respect to any act or thing done by the Service".

Section A below sets out the Committee's analysis of the numbers and types of complaints received during the 1997-98 fiscal year.

Section B reviews the complaints the Committee received in respect of Service's role in security screening for the Government of Canada.

During the 1997-98 fiscal year, we received 30 new complaints under section 41 of the *CSIS Act* ("any act or thing")

A. 1997-98 Complaints about CSIS Activities

Statistics

During the 1997-98 fiscal year, we received 30 new complaints under section 41 of the *CSIS Act* ("any act or thing") and one under

Table 2
Complaints (1 April 1997 to 31 March 1998)

	New Complaints	Carried Over from 1996-97	Closed in 1997-98	Carried to 1998-99
CSIS Activities	30	2	29	3
Security Clearances	1	0	0	1
Immigration	0	1	1	0
Citizenship	0	1	0	1
Human Rights	1	0	1	0

SIRC's Role Regarding Complaints About CSIS Activities

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

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

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

section 42 (denial of security clearance). In addition, we rendered a decision with respect to a Ministerial report pertaining to the *Immigration Act* and resumed an investigation of another Ministerial report under the *Citizenship Act*.

On April 30, 1998, the Supreme Court of Canada denied Mr. Ernst Zündel's application for leave to appeal the Federal Court of Appeal's decision.[30] The leave to appeal having been denied, the Federal Court of Appeal's decision stands: SIRC is duly authorized to conduct its investigation under the Citizenship Act.[31]

Findings on 1997-98 Complaints "with respect to any act or thing"

During fiscal year 1997-98, we received four complaints from persons who alleged that the Service had subjected them to surveillance, illegal actions or had otherwise abused its powers.

In response to complaints of this nature, the Committee as a general rule neither confirms nor denies that the person complaining is a target.[32] However, we do undertake a thorough investigation of the complainant's assertions in order to ensure that the Service has not used its powers unreasonably. If we find that the Service has acted appropriately, we then convey that assurance to the complainant. If there is any doubt, however, and pursuant to the procedures set out in the *CSIS Act*, we convey the results of our inquiries to the Solicitor General and the complainant.

The Committee noted this year an unusual departure from normal CSIS practice with respect to complaints. In response to a specific query, the Service deviated from its usual practice of neither confirming nor

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.

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

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 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 briefs[36] 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

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.

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.

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

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

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 important change to existing policy concerned a particular category of "sensitive institution"

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"

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*.

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

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

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

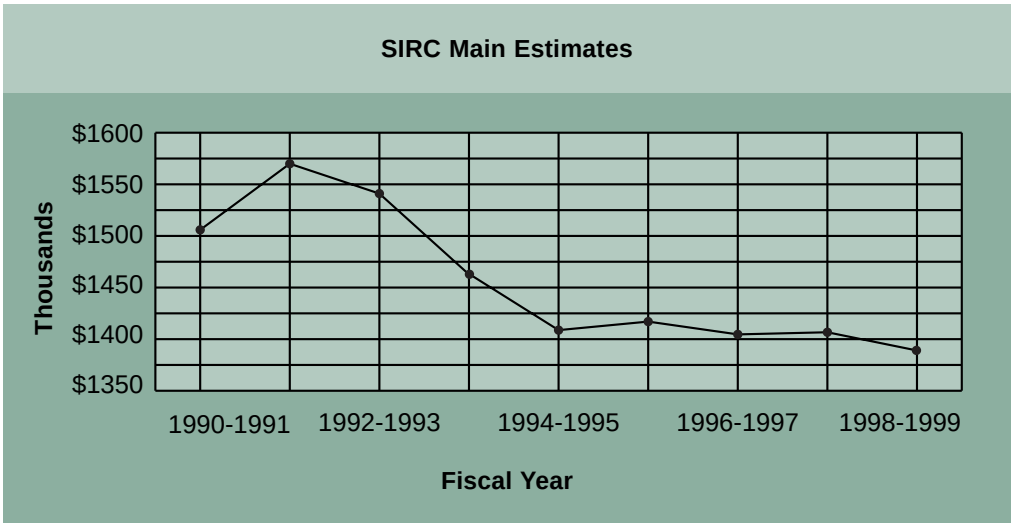
information technology so as to continue the steady increase in productivity seen over the last five years.

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

Appendix A: Glossary

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:

Table 2
Number of Briefs Issued by CSIS

Type	1995-96	1996-97	1997-98
Information Briefs	47	144	94
Inadmissibilty Briefs - No Threat	51	90	108
Inadmissibilty 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.