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 Point of Entry Alert (interdiction program)

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

The CSIS Refugee Watch List

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

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

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%.