C. Inside CSIS

Warrants and Warrant Statistics

Warrants are one of the most powerful and intrusive tools in the hands of any department or agency of the Government of Canada. For this reason alone their use bears continued scrutiny, a task the Committee takes very seriously. In addition, the review process provides insight into the entire breadth of CSIS investigative activities and is an important indicator of the Service's view of its priorities.

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

The Service did not seek renewal of any of its warrants during 1999–2000. The Federal Court issued 29 urgent warrants; however, none were renewed or replaced

during this same fiscal year. As of March 31, 2000, CSIS had in place a total of 238 warrants.

FINDINGS OF THE COMMITTEE

Although the data provides the Committee with an excellent profile of the Service's requests for warrant powers in a given year, comparisons year-to-year are less enlightening because the applications vary as a result of decisions by the Court and new kinds of powers sought. In addition, raw warrant numbers can be misleading because a single warrant can authorize the use of warrant powers against more than one person.

Allowing for these factors, the Committee concluded that the total number of persons affected by CSIS warrant powers remained relatively stable for the last two years and that foreign nationals continue to represent the overwhelming 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 1999–2000, no such regulations were issued.

FEDERAL COURT DECISIONS

None of the applications for, or execution of, certain powers contained in warrants were affected by Federal Court decisions in fiscal year 1999–2000.

Although no applications for new warrants were denied, the Federal Court of Canada in June 1999 declined to issue two replacement warrants based on an interpretation of paragraph 21(2)(a) of the *CSIS Act*. The Service reapplied to the Federal Court and the warrants were approved one month later. The first interpretation has not been adopted by the other designated judges.

WARRANT REVISION PROCESS

In last year's annual report, the Committee reported that, in 1998–1999, CSIS had begun a complete review of clauses and conditions in all existing warrants, with proposed changes to be approved by the Federal Court. During the period 1999–2000, CSIS completed the warrant revision process, and all changes reflected in subsequent warrant applications have been approved by the Federal Court.

CSIS Operational Branches

COUNTER TERRORISM BRANCH

The Counter Terrorism (CT) Branch is one of the two main operational branches at CSIS (the other being Counter Intelligence). Its role is to provide the Government of Canada with advice about emerging threats of serious violence, and about activities by foreign states or their agents in support of serious violence, that could affect the safety and security of Canadians and of Canada and its allies.

Table 1
New and Renewed Warrants

	1997–98	1998–99	1999–2000
New Warrants	72	84	76
Warrants Replaced/Renewed12	153	163	181
Total	225	247	257

The threat from international terrorism continues to be associated with what are termed "homeland" conflicts. Various domestic extremist groups are also regarded as potential threats to the security of Canada because of their capacity to foment violence.

Although the Branch reported that its focus and priorities remained relatively unchanged for much of the 1999–2000 fiscal year, the arrest of Ahmed Ressam in the United States for transporting bomb-making materials from Canada prompted the Service to refocus its efforts on the emerging threats of serious violence.

Threat Assessments

CSIS provides threat assessments to departments and agencies within the Federal Government based on relevant and timely intelligence. CSIS prepares these assessments upon request or on an unsolicited basis—dealing with special events, threats to diplomatic establishments in Canada, and other situations.

In 1999–2000, the Threat Assessment Unit produced a total of 524 assessments, down from 683 the year previous. The Committee recognizes that many factors influencing these numbers—the number of foreign visitors to Canada, requests received from other Government departments and agencies, special events and threats identified during the year—are beyond the control of the Service.

COUNTER INTELLIGENCE BRANCH

The Counter Intelligence (CI) Branch monitors threats to national security stemming from the espionage activities of other national governments' offensive intelligence agencies in Canada.

In last year's annual report, the Committee commented on the lack of training for CSIS intelligence officers in the area of transnational criminal activity. CI Branch has since sought enhanced training of its investigators in three specialized fields: counter proliferation, information operations and transnational criminal activity.

The Service reported mixed success in its efforts to explore common ground for co-operation and information-sharing with certain foreign intelligence agencies. On the domestic side, the Service claimed several successes in forging co-operative relationships with other government departments.

In co-operation with a federal department, the activities of a foreign intelligence agency in Canada were curtailed, and a formal section 17 co-operation agreement with another intelligence agency was brought closer to conclusion.

REQUIREMENTS, ANALYSIS & PRODUCTION BRANCH

The Requirements, Analysis & Production (RAP) Branch provides advice to government on threats to the security of Canada through *CSIS Reports*, *CSIS Studies* and *CSIS Intelligence Briefs*. In addition, the Service published a number of unclassified reports in its *Perspectives* and *Commentary* series.

In 1999–2000, RAP produced a total of 48 reports, a decline from 68 issued the previous year. Recent years have seen a downward trend in the number of reports produced.

CSIS also contributes to the intelligence community through its participation in the Intelligence Assessment Committee (IAC)—a body made up of senior officials from those departments and agencies of the Government of Canada most concerned with intelligence matters. During the past year, the Service took the lead in seven IAC reports and contributed to another nineteen.

In last year's annual report, the Committee presented the findings from an extensive review of the Branch. Among the Committee's recommendations was that the defunct Executive Intelligence Production Committee (EXIPC)[13] be reconstituted to help ensure that intelligence production was consistent with the requirements and priorities of the Government overall,

as well as with the needs of specific government clients. In 1999–2000, an EXIPC meeting was convened on one occasion and we hope this practice will continue.

Arrangements with Other Departments and Governments

CSIS RELATIONS WITH THE RCMP

The mechanisms to facilitate liaison and co-operation between CSIS and the RCMP are set out in the Memorandum of Understanding (MOU) between the two agencies. They include the assignments of liaison officers to both national headquarters and to each other's regional offices.

The Committee learned of several new initiatives to improve liaison and co-operation between the two agencies:

- the development of a staff exchange program;
- increased sharing of technical information and greater emphasis on the holding of joint training courses, presentations and conferences;
- the establishment in a region of a liaison committee tasked with addressing matters arising from the co-operation arrangement;
- implementation in a region of a tracking/diary date system to ensure that all RCMP requests for disclosure were followed up in a timely fashion.

The two organizations exchanged a total of 1518 documents in fiscal year 1999–2000. CSIS was responsible for providing more than half of the total (892). The Service also gave the RCMP 336 disclosure letters[14] and 39 advisory letters.[15]

Implications of an RCMP Internal Audit

Last year, the Committee stated that it would examine the results of a then upcoming RCMP internal audit[16] for their potential impact on Service activities. The RCMP's review included an examination of the CSIS–RCMP Memorandum of Understanding, and the functional working relationship between the two agencies.

The audit raised issues and problems similar to those examined in three of the Committee's own reviews:[17] tension between the two agencies regarding disclosure, possible overlap in investigating transnational criminal activity and misunderstandings in each agency about the other's mandate.

Among its recommendations, the RCMP report proposed several mechanisms to help the RCMP and CSIS better understand each other's roles and limitations. The report also recommended changes to the MOU dealing with disclosure issues and the importance of employing the Liaison Program to resolve conflicts between the two agencies.

Coincident with the internal audit, the Service embarked on several initiatives aimed at improving its working relationship with the Force. These initiatives included:

- resuming the meetings of the Senior Liaison Committee. Originally established as a forum to resolve problems and disagreements between the two agencies, the liaison committee had been inactive since 1993;
- raising the level of the CSIS liaison officer position to that of the RCMP counterpart so as to promote the working relationship and signal the importance of the position within the Service.

Stinchcombe and the CSIS–RCMP Memorandum of Understanding

In the past, the Committee has commented on concerns expressed by both CSIS and the RCMP that the existing MOU did not adequately address issues of disclosure of CSIS information to the Courts arising from the

Stinchcombe decision. The Service informed the Committee that it is currently negotiating possible changes to the MOU with the RCMP in this regard.

DOMESTIC ARRANGEMENTS

In carrying out its mandate, CSIS co-operates with police forces, and federal and provincial departments and agencies across Canada. Pursuant to section 17(1)(a) of the *CSIS Act*, the Service may enter into co-operation arrangements with domestic agencies after having received the approval of the Minister.

CSIS currently has 19 formal MOUs with Federal Government departments and agencies and 8 with the provinces. CSIS also has a separate MOU with several police forces in one province. The Service signed no new MOUs with domestic agencies in fiscal year 1999–2000, nor were any existing arrangements with federal or provincial departments amended or terminated. The Service did receive Ministerial approval to negotiate an agreement with a provincial agency to conduct security assessments.

FOREIGN ARRANGEMENTS

Pursuant to subsection 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—to enter into an arrangement with the government of a foreign state or an international organization. During the initial phases leading to the approval of an arrangement, CSIS is not permitted to pass classified information to the foreign agency. However, it may receive unsolicited information.

As of March 31, 2000, CSIS had 217 liaison arrangements with 130 countries. Of this total, the Service judged 45 to be "dormant."[18] During fiscal year 1999–2000, CSIS received the Minister's approval for five new liaison arrangements, with the Minister turning down a Service request to expand the scope of an existing arrangement because of that country's unstable political environment. Nine other arrangements were amended so as to broaden the scope of information exchange, and the Service had 10 new arrangements under consideration.

An issue about which the Committee expressed concern in last year's annual report was resolved. In a review of the agreement that set out the terms of a particular foreign liaison arrangement, we noted that a single generic name used in the text in fact represented several different intelligence organizations within the foreign state concerned—in the Committee's view, a contravention of Ministerial Direction. The Service confirmed to the Committee that the Minister had been advised and the clarification noted. Only after these measures did active co-operation with the agencies begin.

MINISTERIAL DIRECTION

The Committee continues to regard the imminent release of a new Ministerial Direction on foreign arrangements as vital. Critical elements of the existing direction are outdated and the number of agreements between CSIS and foreign agencies during the past several years has increased dramatically. As of March 2000, no new Ministerial Direction had been forthcoming from the Solicitor General. However, we were again informed that the new Ministerial Direction is expected to be signed in the near future.

Collection of Foreign Intelligence

Report #117

Under section 16 of the *CSIS Act*, the Service—at the written request of the Minister of Foreign Affairs and International Trade (DFAIT) or the Minister of National Defence (DND), and with the written consent of the Solicitor General—may collect foreign intelligence. Under the *Act*, CSIS can make warrant applications for powers such as telephone intercepts and undertake other investigative activities at the request of these ministers.

Foreign intelligence refers to information or intelligence about the "capabilities, intentions or activities" of a foreign state. The *Act* stipulates that the Service's collection of foreign intelligence must take place in Canada and cannot be directed at citizens of Canada, permanent residents or Canadian companies.

METHODOLOGY OF THE AUDIT

The Committee's review encompasses all Ministerial "requests for assistance," all information about Canadians retained by CSIS for national security purposes and all exchanges of information with the Communications Security Establishment (CSE) in the context of foreign intelligence.[19]

The goal of the audit is to:

- assess CSIS involvement in section 16 requests so as to ensure compliance with the *CSIS Act*, directions from the Federal Court and the governing Memorandum of Understanding (MOU);
- determine whether the Service has met the various legal conditions necessary to collect information under section 16 operations;
- assess whether the nature of the Service's co-operation with the CSE is appropriate and in compliance with the law.

FINDINGS OF THE COMMITTEE

Ministerial Requests

A 1987 tri-ministerial MOU stipulates that any section 16 request likely to result in the inadvertent interception of communications to which a Canadian is party, should so state.[20] In last year's report, the Committee noted that some requests for assistance had not contained the required cautions and caveats about the targeting of, or the inadvertent collection of information about, Canadians. Although all Ministerial requests since August 1998 have contained such clauses, the Committee believes the declaration used currently concerning incidental interception requires additional clarification.

> **The Committee recommends that in requesting section 16 assistance, Ministers indicate explicitly those instances where there is a real likelihood that the communications of Canadians will be subject to incidental interception as part of the collection activity.**

A related concern arises with respect to CSIS warrant applications resulting from section 16 requests. Two applications examined by the Committee did not include, as stipulated in the tri-ministerial MOU, the mandatory caution against directing the collection of information at citizens, companies and permanent residents.

> **The Committee strongly recommends that all future CSIS section 16 warrant applications contain the required prohibition against directing the collection of information at Canadian citizens, companies or permanent residents.**

Retention and Reporting of Foreign Intelligence Information

The retention and reporting of information pertaining to Canadians, and collected by CSIS under section 16, continues to be of concern to the Committee. To ensure that no inappropriate data were retained in Service files or reported to other agencies, the Committee examined the special database holding foreign intelligence. In a few instances, in the Committee's opinion, information went beyond the definition of foreign intelligence as set out in policy and law and included information that identified

Canadians or gave information about their activities that had very little intelligence value. In one instance, the Service agreed and the information was removed.

It is the clear intent of the *Act* and of existing policy that, in the process of gathering foreign intelligence, the Service take steps to ensure that the collection of information about Canadians be kept to an absolute minimum. In this regard, the Committee had some concerns about the length of time the Service retained certain information; about 10 percent of its foreign intelligence records contained references—some five years old or more—to Canadian citizens or landed immigrants.

The Committee raised the matter with the Service, which stated in response that schedules for retaining and disposing of information already collected are set out in the *National Archives Act* and that it was in compliance with those rules.

The Committee also reviewed CSIS reports to requesting Ministries based on section 16 collection. Some contained information about Canadians that went beyond that necessary for the understanding and exploitation of the intelligence. Although these represented only a very small fraction of the total, the Committee believes that the Service could be more circumspect with little or no penalty to the quality of its analyses.

> **The Committee recommends that CSIS ensure that it is more circumspect and that reports to requesting agencies contain only that information absolutely essential for the exploitation of the foreign intelligence.**

Finally, the Committee was encouraged to observe that the incidental interception of information about Canadian businesses was minimal. The Members also found that the use made of section 16 information in certain types of ongoing section 12 (national security) investigations was insignificant. However, the Committee is alert to the possibility that this situation could change if, as we anticipate, the Service were to focus its section 12 investigations in new directions.

Management, Retention and Disposal of Files

Files are the essential currency of intelligence gathering. Each CSIS investigation and every approved target requires the creation of a file and a system for making the information in it available to those designated within the Service. Balanced against this information-gathering apparatus is the clear restriction on CSIS set out in the CSIS Act, that it shall collect information "to the extent that it is strictly necessary." The Committee closely monitors annually the operational files held by the Service.

FILE DISPOSAL

CSIS files are held according to predetermined retention and disposal schedules that are negotiated with the National Archivist. These define how long the files are to be retained after Service employees cease using them. When this period expires, the National Archives Requirements Unit (NARU) in CSIS consults with Service operations staff on whether to keep the file, destroy it or send it to the National Archives.

During fiscal year 1999–2000, NARU reviewed 44 223 files, which had come to their attention through the regular archival "Bring Forward" (BF) system. Most of the files reviewed by NARU were from the screening and administration sections of the Service.

Of the files that NARU and the operational staff reviewed, 33 920 were destroyed and 10 097 were

retained. CSIS informed us that 206 files were identified as having archival value. They were removed from the active file holdings and automated systems and will be sent to National Archives at a future date, according to the established schedules.

Overlooked Files–Follow Up

Last year the Committee reported on certain files that had been overlooked by the Service's file management system. The committee asked that CSIS reassess the files for their operational value and dispose of them appropriately.

The Committee has since been informed by the Service that of the sample we examined, all were either destroyed or transferred to the National Archives. Of the total files remaining in the overlooked category, approximately one-third have been retained because they contain information of operational value and the balance destroyed or sent to the National Archives.