

## **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, which task the Committee takes very seriously. In addition, our review of the Service's handling of warrants provides insights into the entire breadth of its investigative activities and is an important indicator of the Service's view of its priorities.

The Committee compiles statistics quarterly on CSIS warrant affidavits and on warrants granted by the Federal Court. We track several kinds of information annually, including the number of persons and targeted groups subject to warrant powers. Table 1 compares the number of warrants issued over the last three fiscal years.

The Federal Court issued 32 urgent warrants during 2000–2001. No applications for warrants were denied by the Federal Court during the fiscal year under

**Table 1**  
**New and Replaced/Renewed Warrants**

|  | 1998–1999 | 1999–2000 | 2000–2001 |
|--|-----------|-----------|-----------|
| New Warrants                           | 84        | 76        | 56        |
| Replaced/Renewed Warrants <sup>3</sup> | 163       | 181       | 150       |
| Total                                  | 247       | 257       | 206       |

review, and none of the decisions issued by the Court impacted upon existing warrant powers.

### **OBSERVATIONS ON WARRANT NUMBERS**

Although the data collected by the Committee provide good insight into how the Service exercises its warrant powers in a given year, comparing them between years is more problematic. A range of factors as disparate as court decisions and new developments in technology introduce significant variations into how warrants are applied for and how they are implemented. Even raw warrant numbers can be misleading since a single warrant can authorize the use of warrant powers against more than one person.

Allowing for these factors, however, the Committee concludes that the total number of persons affected by CSIS warrant powers has remained relatively stable for the last 3 years, and that foreign nationals continue to represent 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 2000–2001, no such regulations were issued.

---

3. A replacement warrant is required when the Service changes the targets, the places or the powers of an existing warrant.

## CSIS Operational Branches

### COUNTER INTELLIGENCE

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

During the year under review, personnel and other resources were reallocated internally so as to meet what the Service regards as the increasingly complex challenges of the Counter Proliferation and Transnational Criminal Activity areas of CI's mandate. As is the case in other branches of the Service, CI Branch regards as a priority recruiting and retaining personnel with in-depth knowledge of computer and other sciences, international financial markets and other technical specialities. Specialized skills were added to the Branch's capacity through the use of secondees from other government departments.

The Service claimed success in curtailing the activities in Canada of a number of foreign intelligence services through continual efforts at forging constructive liaison relationships. CSIS also pointed to several examples where co-operation with domestic agencies, as well as allied foreign intelligence services, had yielded positive results.

### 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 denying 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.

## COUNTER TERRORISM

The role of the Counter Terrorism (CT) Branch is to advise the government on emerging threats of serious violence that could affect the safety and security of Canadians and of Canada's allies. Whether of domestic or foreign origin, addressing the threat of serious politically motivated violence continues to be one of the Service's chief priorities.

During 2000–2001, CT Branch made organizational and structural changes to reflect the evolving nature of the terrorist threat. The Service believes that one of the major challenges facing its counter terrorist efforts is the increasing use by extremists of advanced technologies to conduct, support and mask their operations.

### Threat Assessments

CSIS provides threat assessments to departments and agencies within the federal government based on relevant and timely intelligence. CSIS prepares these assessments—dealing with special events, threats to diplomatic establishments in Canada and other situations—either upon request or unsolicited. Threat assessments can play a crucial role, not only in advising authorities when an activity such as a demonstration is likely to degenerate into violence, but also in reassuring authorities about situations in which there is little likelihood of violence.

In 2000–2001, the Threat Assessment Unit produced 544 assessments—a slight increase over the previous year. The Committee recognizes that many factors influencing this total—the number of foreign visitors to Canada, requests received from other government departments and agencies, special events and new threats identified during the year—are beyond the control of the Service.

## REQUIREMENTS, ANALYSIS AND PRODUCTION

The research arm of CSIS, the Requirements, Analysis and Production (RAP) Branch provides advice to the Government on the threats to the security of Canada through the production of *CSIS Reports*, *CSIS Studies* and *CSIS Intelligence Briefs*. Using open source material, the Branch also produces two unclassified reports of security interest to both the intelligence community and the public, *Perspectives* and *Commentary*.

In 2000–2001, RAP produced 93 reports, almost double the number of the previous year and a significant reversal of the trend in recent years to issuing fewer reports. RAP publications generally fall under two categories:

- public safety reports examine the threat to Canadians at home and abroad from international terrorism;

- national security reports refer to the activities in Canada of other national governments' intelligence services, and global issues such as counter-proliferation and transnational criminal activities.

CSIS also contributes to the wider government intelligence community by participating in the Intelligence Assessment Committee (IAC). This body is made up of senior officials from departments and agencies of the Government of Canada most concerned with intelligence matters. In the year under review, RAP staff contributed to eight of the IAC's reports; these are distributed to a senior readership across government.

In an earlier report (*SIRC Report 1998–1999*), the Committee recommended reinvigorating the Executive Intelligence Production Committee (EXIPC), an internal CSIS body first set up in 1987 (but which had fallen into disuse) to help ensure that the intelligence produced conformed to the needs of the Service's various government clients. The Service has since decided to discard the annual planning cycle it originally envisaged for EXIPC in favour of more frequent monitoring of RAP's intelligence production activities with appropriate accountability to relevant senior Service managers. In future, formal meetings of EXIPC will be convened only as required.

## Arrangements with Other Departments and Governments

### 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. Co-operation is facilitated by the reciprocal assignment of liaison officers to the agencies' national headquarters and to all regional offices.

For the year under review, the Service cited several new initiatives aimed at improving co-operation with the Force:

- a staff exchange program between national headquarters with special emphasis on transnational criminal activity;
- exchanges of staff and agreements for future exchanges between several regional offices;
- “open houses” conducted by CSIS for the RCMP and other police forces at the regional level.

CSIS and the RCMP routinely exchange information about their activities pursuant to their respective mandates. The Service collects and disseminates information about threats to the security of Canada and the RCMP carries out its mandated law enforcement functions in relation to the same threats. During fiscal year 2000–2001, the two organizations exchanged 1678 documents, with CSIS responsible for generating more than half of the total (949). The Service also provided the RCMP with 330 disclosure letters<sup>4</sup> and 39 advisory letters.<sup>5</sup>

### **DOMESTIC ARRANGEMENTS**

In carrying out its mandate, CSIS co-operates with police forces, and with federal and provincial departments and agencies across Canada. Contingent on Ministerial approval, the Service may conclude written co-operation arrangements with domestic agencies pursuant to section 17(1)(a) of the *CSIS Act*.

Currently, CSIS has 19 formal Memoranda of Understanding (MOUs) with federal government departments and agencies, and 8 with provincial bodies. The Service has a separate MOU with several police forces based in one province.

In 2000–2001, the Service signed a new arrangement with a provincial agency to conduct security assessments and sought Ministerial approval to establish a liaison arrangement with another. No existing arrangements were altered or terminated.

### **FOREIGN ARRANGEMENTS**

Pursuant to section 17(1)(b) of the *CSIS Act*, the Service must obtain the approval of the Solicitor General—after consulting with the Minister of Foreign Affairs and International Trade—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; it may, however, accept unsolicited information.

During fiscal year 2000–2001, CSIS received the Minister's approval to establish five new liaison arrangements. Of the arrangements currently in force, the Service

---

4. Following a formal request by the RCMP, CSIS discloses information in a format that protects the identity of sources and the methods of intelligence gathering. The disclosure is made on the condition that the information can only be used for investigative leads and cannot be used in judicial proceedings.

5. Following a formal request by the RCMP—usually subsequent to a disclosure—CSIS gives permission in the form of an advisory letter for its information to be used in judicial proceedings, for example in obtaining warrants or as evidence at trial.

considers 44 to be “dormant.”<sup>6</sup> Six existing arrangements were expanded to broaden the scope of information to be shared and one dormant arrangement was reactivated to facilitate Service security screening and immigration activities in the country concerned.

No existing liaison arrangements were cancelled; however, the Service curtailed the level of exchange activity with two foreign agencies, in one case because of human rights concerns and, in the other, because of an assessment that raised questions about that agency’s reliability and stability.

### SERVICE LIAISON OFFICER POSTS

The Service operates Security Liaison Officer (SLO) posts overseas responsible for liaising with police, security and intelligence agencies in many countries. The

Foreign intelligence refers to information or intelligence about the capabilities, intentions or activities of a foreign state

authorities in the host countries are aware of the Service officer’s presence and functions, a necessary pre-condition for inter-agency co-operation. The number of SLO posts abroad was unchanged from the previous year.

## Collection of Foreign Intelligence

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 *CSIS 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.

---

6. A dormant arrangement is one in which there has been no contact for 1 year or more. Liaison arrangements become dormant for a number of reasons: a simple lack of need to exchange information, concerns by the Service about the other agency’s professional or human rights practices, or an assessment that the political situation in the other country is too unstable.

## 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.

CSE—an agency of the Department of National Defence—provides the Government of Canada with foreign signals intelligence, which it obtains by gathering and analyzing foreign radio, radar and other electronic emissions, sometimes in co-operation with allied agencies.

The goal of the audit is to:

- review CSIS involvement in section 16 requests so as to ensure compliance with the *CSIS Act*, directions from the Federal Court and the governing 1987 Memorandum of Understanding (MOU) between the Ministers of Foreign Affairs and International Trade, National Defence and the Solicitor General;
- determine whether the Service has met the various legal conditions necessary to collect information under section 16 operations;
- examine the nature of the Service's co-operation with CSE to ensure that it is appropriate and complies with the law.

## FINDINGS OF THE COMMITTEE

### Warrant Implementation

As in any intelligence collection activity that involves a Federal Court warrant, the Service is obligated to observe all conditions and restrictions contained therein. The Committee examined a selection of warrants directed at section 16 collection as well as the associated affidavits and working files. In the cases we reviewed, the warrants were correctly administered and the relevant conditions observed.

### Information Requests to the CSE

Information that CSE gives to the Service is routinely “minimized” to comply with the prohibition against targeting Canadian nationals and Canadian businesses. Thus, the name of a Canadian, which had been collected incidentally, would be shielded by employing, for example, the phrase “a Canadian business person.” Under specific circumstances, the Service may request the identities from CSE if it can demonstrate that the information relates to activities which could constitute a threat to the security of Canada as defined in section 2 of the *CSIS Act*.



As part of its audit, the Committee scrutinized these CSIS requests to ensure that they were appropriate, and in accordance with law and policy; three did not appear to meet the threshold set out in section 2 of the Act.

One request involved a prominent Canadian who had been approached by a foreign national. The second request concerned a sensitive institution (trade union, media organization, religious body or university campus) involved in political campaigns in a foreign country. We were informed by the Service that in both instances the information obtained was removed from its files following our review.

In the third request, the Service had retained in its files lists of individuals who had attended several social functions with foreign nationals. Records checks were conducted by CSIS on some of the individuals listed.

The Committee questioned the retention of this information, citing to the Service our view that the action did not appear to meet the “strictly necessary” test of the Act. The Service maintained that the information was retained because the individuals had relationships with a target who was already the subject of a section 12 investigation. The Committee was satisfied with the Service’s response.