

## **Section 3**

---

### **CSIS Accountability Structure**

## CSIS Accountability Structure

The Service is an agency of the Government of Canada and through the Solicitor General is accountable to Parliament and to 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; a number of independently managed systems exist inside and outside the Service for monitoring CSIS activities and ensuring that they are conducted in a manner consistent with its mandate and the law.

A full description of Canada's security intelligence apparatus and the accompanying accountability mechanisms can be found in a new publication of the Privy Council Office, *The Canadian Security and Intelligence Community*, Ottawa, 2001.

Part of SIRC's task—the Committee itself being part of the accountability structure—is to assess and comment on the functioning of the systems that hold the Service responsible to its Minister.

### A. Operation of CSIS Accountability Mechanisms

#### MINISTERIAL DIRECTION

Under section 6(2) of the *CSIS Act*, the Minister can issue directions governing CSIS activities and investigations. The Committee is specifically charged with reviewing those directions when they are issued. In fiscal year 2000–2001, the Minister issued a new compendium of Ministerial Direction, which replaces the previous documents in their entirety. The subject of a special Committee review, the revised and updated Direction is discussed in greater detail on page 7.

#### CHANGES IN SERVICE OPERATIONAL POLICIES

In the fiscal year 2000–2001, the Service produced two new policies: one deals with preparing threat assessments, and the other with using the polygraph in CSIS operations. Another 14 policies were amended either to reflect changes in Ministerial Direction or to conform with current business practice.

#### DISCLOSURES IN THE PUBLIC INTEREST AND IN THE NATIONAL INTEREST

Section 19 of the *CSIS Act* prohibits information obtained by the Service in the course of its investigations from being disclosed except in specific circumstances. Under section 19(2)(d) the Minister can authorize the Service to disclose

information in the “public interest.” The Act instructs the Director of CSIS to submit a report to the Committee regarding all public interest disclosures.

The Service reported one such disclosure in 2000–2001. The disclosure was to counsel acting on behalf of a Minister of the Crown and related to a Service employee’s draft affidavit prepared in relation to legal proceedings.

In addition, CSIS acting as the Minister’s agent can disclose information in the “national interest” under specified circumstances. Service policy stipulates that the Committee must be informed when such disclosures occur. There were none during the year under review.

#### **GOVERNOR IN COUNCIL REGULATIONS AND APPOINTMENTS**

As set out in section 8(4) of the *CSIS Act*, the Governor in Council may issue any regulations to the Service in regard to the powers and duties of the Director of CSIS, as well as the conduct and discipline of Service employees. No such regulations were issued in fiscal year 2000–2001.

#### **CERTIFICATE OF THE INSPECTOR GENERAL**

The Inspector General of CSIS reports to the Solicitor General and functions effectively as the Minister’s internal auditor of CSIS, reviewing the operational activities of the Service and monitoring compliance with policy and the law. 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 annual 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 which involved an unreasonable or unnecessary exercise of powers. The Minister forwards the Certificate to the Review Committee.

The first certificate from the current Inspector General, who was appointed in July 1999, was issued in November 2000. In it, the Inspector General stated that he was fully satisfied with the Director’s annual report to the Minister and that in his opinion, “the Service ha[d] not acted beyond the framework of its statutory authority, ha[d] not contravened any Ministerial Directions, and ha[d] not exercised its powers unreasonably or unnecessarily.”

The Inspector General went on to state that he and the Director of CSIS had come to an agreement that future Director’s reports would be more concise and focussed than hitherto. Future reports would present “the highlights of the Service’s activities for the reporting period, and include any serious issues with respect to operational activities, public policy, potential controversy, and anticipated challenges in fulfilling the Service’s mandate.” Supplementary detailed data would continue to be available

for examination by the Deputy Solicitor General, the Inspector General's Office and this Committee.

The other matter addressed by the Inspector General concerned a security certificate signed by the Minister of Citizenship and Immigration and the Solicitor General based on a security intelligence report prepared by the Service. A subsequent Federal Court ruling quashed the certificate, judging it to be “not reasonable.”

The Inspector General conducted his own assessment of the CSIS security intelligence report and concluded that it was well founded, accurate and credible, and that it met the “reasonable grounds to believe” standard set out in section 19(1) of the *Immigration Act*. He also stated that he supported measures underway within the Service that would result in security intelligence reports that in future were “more cogent and compelling when presented to the Court.”

### **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 may have acted unlawfully in performing his or her duties and functions. The Minister, in turn, must send the report with his comment to the Attorney General of Canada and to the Committee.

In 2000–2001, we received one report of possible unlawful conduct by an employee of CSIS. At the time of publication of this Report, the Attorney General has not yet rendered a decision as to the disposition of the case. In last year's Report (*SIRC Report 1999–2000*), we cited an unresolved case of unlawful conduct dating back to 1997. The Attorney General has since decided not to proceed with prosecution.

### **SECTION 2(D) INVESTIGATIONS**

According to Ministerial Direction, any investigation of threats to the security of Canada as defined by section 2(d) of the *CSIS Act*—often referred to as the “subversion” clause—must be authorized by the Minister. The Minister authorized no such investigations in 2000–2001.

## **B. Inside the Security Intelligence Review Committee**

### **TRACKING AND TIMING OF FORMAL INQUIRIES**

In carrying out its review function the Committee sends questions to CSIS to request information or documents (or both) about its activities. In fiscal year 2000–2001

(April 1, 2000 to March 31, 2001), we directed 91 formal inquiries to the Service, which total does not include inquiries arising from complaints cases.

The Committee often makes additional informal requests of CSIS. During the year under review, the Service responded expeditiously to what were sometimes urgent inquiries.

### **RESEARCH AND REVIEW ACTIVITIES**

The Service makes available a separate office and computers at CSIS Headquarters for the exclusive use of SIRC staff and members. Reporting regularly to the Committee's senior management, SIRC's researchers and analysts divide their time between SIRC premises and the Committee's facilities at the Service.

### **BRIEFINGS**

At its monthly meetings, the Chair and Committee Members meet with government officials to keep the lines of communications open and stay abreast of new developments. When meetings of the Committee are held outside Ottawa, Members visit CSIS regional offices. In June 2000 and February 2001, the Committee met with senior CSIS regional managers in Toronto and, in September 2000, with Service officials in Montréal. The balance of the meetings were held in Ottawa.

### **SENIOR STAFF APPOINTMENTS AT SIRC**

In December 2000, Susan Pollak, Executive Director of SIRC, announced the appointment of Mr. Thomas Dastous as the Senior Counsel to SIRC. Mr. Dastous joined SIRC from the federal Department of Justice.

In January 2001, Ms. Kelly McGee joined SIRC as Research Manager. Previously, Ms. McGee was Senior Counsel and Director of Policy at the Regional Municipality of Ottawa–Carleton.

### **ADDITIONAL COMMITTEE ACTIVITIES**

- In September 2000, the Chair, Executive Director, Deputy Executive Director and Senior Counsel met in Ottawa with the recently appointed Inspector-General of Intelligence for South Africa to discuss the role and functions of the Security Intelligence Review Committee in Canada's system of government.
- A delegation from Denmark met with SIRC senior management in October 2000 to discuss the Committee's mandate and operations. The delegation was conducting research as part of a commission examining Denmark's intelligence services.

- The National Security Advisor to Mexican President Vicente Fox met with the Executive Director, Deputy Executive Director and Senior Counsel in February 2001 to discuss SIRC's mandate, structure and operations, and to share some of its experiences over the past 16 years.
- In March 2001, members of the Norwegian Committee for the Monitoring of Intelligence, Surveillance and Security met with SIRC senior management as part of the group's study tour in North America. The Norwegian Committee viewed the SIRC model as being of special interest in its survey of similar bodies.

### ON THE INTERNET

In fiscal 2000–2001, SIRC's Web site underwent major reconstruction to present a more attractive, more user-friendly source of information for Canadians. All SIRC Annual Reports, dating back to its establishment in 1984, are accessible through the redesigned site at [www.sirc-csars.gc.ca](http://www.sirc-csars.gc.ca). The site presents the latest news about Committee activities, as well as information ranging from biographical information on Committee Members to procedures for filing complaints about CSIS activities and the denial of security clearances. During the 2000–2001 reporting period, the site recorded 543 137 hits; some 45 000 per month or approximately 1500 per day.

### BUDGET AND EXPENDITURES

The Committee continues to manage its activities within the resource levels established in 1985. During 2000–2001, the Committee continued to deal with an increase in the number of quasi-judicial (complaint) proceedings with a concomitant effect on the Committee's non-discretionary expenditures (*see* Table 3).

**Table 3**  
**SIRC Expenditures**

	2001–2002 (\$ estimates)	2000–2001 (actual \$)	1999–2000 (actual \$)
Personnel	1 112 000	837 623	841 945
Goods and Services	962 000	953 592	821 055
Total	2 074 000	1 792 295	1 663 000

Other significant expenses included:

- upgrades to the in-house computer infrastructure to be able to meet current operational and security standards for handling large volumes of highly classified information;
- upgrades to the simultaneous translation system in the Committee hearing room;
- improvements to the public access areas and hearing rooms, aimed at creating a more welcoming and, at the same time, more functional environment;
- travel expenses within Canada for Committee hearings and Research staff audit activity;
- staff salaries and benefits.

#### **STAFFING AND ORGANIZATION**

The Committee has a staff of 16: an Executive Director, a Deputy Executive Director, a Senior Counsel, a Junior Counsel, one Complaints/Access to Information and Privacy Officer, a Senior Para-legal/Hearing Registrar, a Research Manager, a Senior Policy Advisor, four Research Analysts, a Financial/Office Administrator, an Administrative Assistant, and two administrative support staff to handle sensitive and highly classified material using special security procedures.

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