



SECURITY INTELLIGENCE  
REVIEW COMMITTEE

# SIRC Report 2000-2001

An Operational Audit of the  
Canadian Security Intelligence Service

Canada





**SECURITY INTELLIGENCE  
REVIEW COMMITTEE**

# **SIRC Report 2000–2001**

**An Operational Audit of the  
Canadian Security Intelligence Service**

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 8:00 a.m. to 5:30 p.m. Eastern Standard Time.

© Public Works and Government Services Canada 2001

Cat. No. JS71-1/2001

ISBN 0-662-65978-3

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

30 September 2001

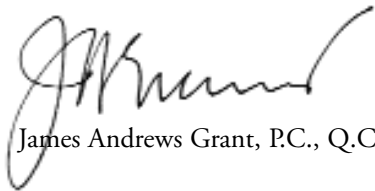
Dear Mr. MacAulay:

As required by section 53 of the *Canadian Security Intelligence Service Act*, we transmit to you the Report of the Security Intelligence Review Committee for the fiscal year 2000–2001, for your submission to Parliament.

Yours sincerely,



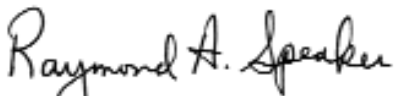
Paule Gauthier, P.C., O.C., O.Q., Q.C.  
Chair



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



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



Raymond Speaker, P.C., O.C.



Frank McKenna, P.C.

## Contents

---

Statement from the Committee .....	vii
How SIRC's Annual Audit Report is Organized .....	x
<b>Section 1: Review of CSIS Intelligence Activities .....</b>	<b>1</b>
<b>A. Areas of Special Interest for 2000–2001 .....</b>	<b>3</b>
CSIS Liaison with Foreign Agencies .....	3
Ministerial Direction, Revised and Updated .....	7
Domestic Exchanges of Information (5) .....	9
Review of Warrant Preparation .....	11
Security Screening Briefs to Citizenship and Immigration Canada .....	12
<b>B. Annual Audit of CSIS Activities in a Region .....</b>	<b>15</b>
Targeting of Investigations .....	15
Warrant Implementation .....	17
Audit of Sensitive Operations .....	18
Internal Security .....	19
<b>C. Inside CSIS .....</b>	<b>20</b>
Warrants and Warrant Statistics .....	20
CSIS Operational Branches .....	22
Arrangements with Other Departments and Governments .....	24
Collection of Foreign Intelligence .....	26

**Section 2: Security Screening and Investigation  
of Complaints** ..... 29

    A. Security Screening ..... 31

    B. Investigations of Complaints ..... 35

**Section 3: CSIS Accountability Structure** ..... 39

    A. Operation of CSIS Accountability Mechanisms ..... 41

    B. Inside the Security Intelligence Review Committee ..... 43

**Appendix A: Abbreviations** ..... 47

**Appendix B: SIRC Reports and Studies Since 1984** ..... 51

**Appendix C: Major Findings and Recommendations** ..... 61

**Appendix D: Complaint Case Histories** ..... 67

## Statement from the Committee

---

The events of September 11, 2001 in the United States will have put to rest any lingering doubts that the most serious threats to Canada's security and the safety of its citizens come in forms sharply different from those of an earlier generation. Some sixteen years ago when the country's security intelligence apparatus was last overhauled, the singular military politics of the Cold War were of preeminent concern. Today we all live in a world characterized by different and diverse forces, all in rapid flux.

People, capital, information, technologies and political ideologies are more mobile than ever before. The resulting influences are mostly welcome or at least benign, but others are decidedly not. And as a democratic country that encourages international contact and investment and welcomes visitors and immigrants, Canada opens itself to both the best and the worst of these influences.

This sea change in the nature of the threats is reflected wherever public policy touches on Canada's national interests and the safety and security of its citizens:

- At the level of Ministerial Direction to the nation's security intelligence community, politically motivated violence and terrorism are clearly identified as being the most serious threats to Canada and Canadians.
- The deployment of resources within the Canadian Security Intelligence Service, whether measured in person years or budget allocation, reflects the growing need to meet multiple terrorist threats.

- The Service's recent public annual reports are heavily weighted towards concerns about terrorism and an international security environment that makes it easier for terrorist activities to take place in Canada and abroad.
- Proposed and actual changes in legislation brought forward by the federal government (Bill C-16, an amendment to the *Income Tax Act*; and Bill C-11, an amendment to the *Immigration Act*) are both expressions of concern about politically motivated violence being directed or funded from within Canada.
- Parliament's most recent inquiry into security intelligence matters, the 1999 *Report of the Special Senate Committee on Security and Intelligence* (Kelly Report), was almost entirely taken up with the issues of terrorism and political violence and devoted little attention to espionage threats.

In short, CSIS has been transformed in a mere decade from a primarily anti-espionage organization working to block the intelligence-gathering activities of a fairly limited number of foreign governments into one in which terrorism and the politics accompanying it have become dominant.

This transformation is manifest in complex ways. Increasingly, the Service's "case load" involves the need to make nuanced judgements about politically motivated organizations and individuals—nuanced because the line between legitimate,

The Service's "case load" involves the need to make nuanced judgements about politically motivated organizations and individuals

political activity and illegitimate actions involving violence or threats of violence is frequently blurred. Because it is the Committee's task to review and assess the quality of the Service's judgements on these matters, as CSIS's priorities have shifted, so have our own.

Issues of legitimate versus illegitimate political activity and what constitutes "association" with a terrorist organization are taking on ever greater importance for the Committee in its review and complaints/tribunal functions. In both areas, the Committee's work has been fundamentally transformed from that of 15 or even 10 years ago and will evolve still further.

Terrorist threats, originating from new and divergent sources, put a premium on understanding developments across the globe as they unfold. As CSIS redirects its efforts, the Committee will continue to adjust its research focus and resources accordingly.



The complaints and tribunal side of the Committee's operations have seen considerable change as well. A rising proportion of complaints involve issues of immigration and security screening, most of which turn on Service assessments of politically motivated individuals and require lengthy inquiries into activities, intelligence sources and political cultures in other countries. Should Bills C-16 and C-11 come into force, the Committee expects the number of similar complaints to increase still further.

The Committee does not believe there is a magic policy or legislative remedy that will make these judgements any less fraught or the appropriate balance between national security and the protection of civil rights any easier to locate. Existing national policy instructs the Service to investigate those threats it believes the Government needs to know about, based on its professional assessment of the seriousness of the threat. SIRC's

The Committee does not believe there is a magic policy that will make these judgements any less fraught

assessments are similarly grounded in professional experience and knowledge, rather than in policy manuals. Nor does the Committee believe that precise definitions of "terrorist" or "association" or "extremism" would be very helpful, especially in a global environment where the velocity of change seems to increase daily.

However, SIRC does bring a special perspective to the dilemmas of security intelligence—just as Parliament intended. CSIS represents a government's right and responsibility to protect the lives of citizens, and to preserve law and order. SIRC, *inter alia*, embodies a legal principle at the core of Canadian democracy, namely that citizens have rights to privacy, civil liberties and freedom from untrammelled government power—the "liberty of the subject."

The complexity and ambiguity that have come to dominate security intelligence work means that an ever larger part of the Service's powers of judgement—and, therefore, those of the Committee—are focussed on decisions vital to preserving both Canadians' liberty and their security. Terrorism is an affront to democracy; confronting it will require both greatly increased international cooperation and strength of purpose, and an ongoing commitment to Canada's core values.

## How SIRC's Annual Audit Report is Organized

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 subsections 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—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.

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**

---

### **Review of CSIS Intelligence Activities**

## Review of CSIS Intelligence Activities

### A. Areas of Special Interest for 2000–2001

#### CSIS Liaison with Foreign Agencies

---

##### Report #2000-03

---

##### BACKGROUND

As stipulated in section 38(a)(iii) of the *CSIS Act*, SIRC reviews arrangements entered into by CSIS with foreign intelligence and police agencies and monitors the flow of information to agencies with which CSIS has co-operation and information-sharing arrangements.

This year, the Committee audited a Security Liaison Officer (SLO) post overseas that operates in an especially difficult working environment. Maintaining the security of the physical operating environment is a continual, major challenge and the situation is compounded by generally onerous working conditions.

CSIS opened the post in the belief that constructive engagement through dialogue and information exchanges would assist the Service in addressing its national security mandate. The Service has sought out specific areas of common ground in which the information exchanged can serve Canadian interests and characterizes its approach to the relationship as “cautious” and “measured”—one that encourages transparency and co-operation.

##### METHODOLOGY OF THE AUDIT

The Committee’s review encompassed three categories of material:

- all exchanges of information handled by CSIS SLOs at the post, including electronic exchanges;
- all correspondence with foreign intelligence agencies handled by the post;
- all instructions and reference materials provided to and originating with the SLOs, including their “Assessments of Foreign Agencies.”

The essential goals of the review were to ensure that relationships and contacts with the foreign agencies concerned corresponded to the specific liaison agreements

in place and that information disclosed to foreign agencies or received from them was properly handled by the Service.

More broadly, the Committee examined the activities of the selected post in the context of the Service's overall foreign liaison program, including Ministerial Direction and the Service's policies. As it has during previous reviews of CSIS foreign liaison activities, the Committee paid special attention to any information exchanges that might potentially result in abuses of human rights by other parties.

### **POLICIES AND ADMINISTRATION**

Foreign liaison policies are set out in Ministerial Direction. The relevant Direction, for the period under review, was issued in 1982. As prescribed by section 17 of the *CSIS Act*, the Service may enter into individual arrangements with agencies of other countries. These arrangements, which define the intended nature and scope of each co-operative relationship, are reviewed by the Committee.

Establishing liaison arrangements with foreign intelligence services must be approved by the Solicitor General after consultation with the Minister of Foreign Affairs and International Trade. The arrangement governing exchange activities at the post selected for this year's audit was signed during the past decade.

### **New Ministerial Direction**

As noted earlier, the Ministerial Direction relevant to the period under review was drafted in 1982. Since the Committee completed its audit of the selected SLO post, however, a new Ministerial Direction has been issued covering the entirety of CSIS operations, including foreign liaison arrangements. With particular reference to foreign liaison activities, the Committee in its 1997–1998 Report expressed concern about the need for the Government to update its Ministerial Direction and recommended that the Service re-examine all its liaison arrangements to ensure conformity with the new framework once issued. In light of these earlier comments, the Committee in its review of the new Ministerial Direction paid particular attention to those elements that pertain to foreign liaison. (For a full discussion of the new Ministerial Direction, *see* page 7.)

With respect to foreign liaison, the new Ministerial Direction appears to preserve the key policy elements of the earlier document, namely:

- arrangements are to be established as required to protect Canada's security;

- they are to be approved by the Solicitor General after consultation with the Minister of Foreign Affairs and International Trade;
- the human rights record of the country or agency concerned is to be assessed and the assessment weighed in any decision to enter into a co-operative relationship;
- the applicable laws of Canada must be respected and the arrangement must be compatible with Canada's foreign policy.

The one significant departure from earlier Direction is that the new document grants greater discretion to the Director of CSIS to manage the individual co-operative arrangements. Formerly, Ministerial Direction gave the responsibility for setting out the specific parameters of co-operation to the Minister. The new document states that "the Director will manage these arrangements subject to any conditions imposed by the Minister."

Since the new Direction was issued only in February 2001, it will be some time before the Committee can assess the implications of the revised policies, especially as they relate to the Director's increased discretionary authority.

The new document grants greater discretion to the Director of CSIS to manage individual arrangements

However, considered broadly, we believe the new Ministerial Direction is a substantial improvement over the earlier documents because the terminology employed is simpler and is consistent with that used in the legislation that governs CSIS activities as a whole.

In the Committee's 1997–1998 review of foreign liaison arrangements, and in anticipation of the new Ministerial Direction, we recommended that the Service systematically re-examine all foreign arrangements in light of the new Direction once it was issued, so as to ensure conformity. The Service has informed the Committee that it will conduct its next yearly evaluation of all liaison relationships within the framework of the new Direction.

## FINDINGS AT THE POST

### Overview

During the Committee's audit of the SLO post, we were struck by the substandard conditions in which Service staff were obliged to work. The poor physical facilities

at Canada's mission and an onerous workload, arising from increasingly large numbers of immigration and visa applications requiring security screening, combine to form an adverse environment. Notwithstanding these difficult circumstances, however, the SLO and staff are performing well.

We found that the SLO has made steady progress with foreign interlocutors; however, rising demands from the immigration side of the SLO's mandate left less time for developing relationships with other countries in the region for which the post is nominally responsible.

### Screening Activities

The Committee's review of the post's resource allocation showed a growing share of staff time being devoted to immigration and visa security screening. In a matter of a few months the immigration/visa screening workload had risen dramatically,

We were struck by the substandard conditions in which Service staff were obliged to work

to the extent that additional Service personnel were temporarily detailed to the post to provide assistance. Poor physical facilities and the challenging security environment complicated matters further.

The evident work overload gave rise to concerns on the part of the Committee that some of the post's important functions might not be being handled expeditiously. Service senior management told the Committee that it shared our concerns and believed that the immigration workload problem extended to certain other of its SLO posts as well.

In the early 1990s, CSIS and another federal agency jointly conducted a review of the immigration-related duties at posts abroad, which resulted in more focussed use of CSIS officers' services. It is the Committee's view that the Service might wish once again to review this element of its Foreign Liaison Program. For its part, the Committee intends to conduct audits of security screening functions at selected SLO posts abroad during the course of upcoming reviews.

### Information Exchanges

The Committee examined all documentation associated with operational co-operation and information exchanges involving the SLO post from March 31, 1998 through June 30, 2000. The Service's exchanges of information with the foreign agencies covered by the post were reviewed to ensure that the information disclosed to the foreign agencies or received from them was handled properly.

Our review identified only one problematic exchange. Information that tended to cast aspersions on a certain individual—but which in the Committee’s view was of doubtful reliability—had been passed on to Service clients. After bringing the matter to the attention of CSIS, we were provided with additional, clarifying information. We advised the Service that it should consider giving this new information to its clients so that the earlier advice would be regarded in its proper context.

### **Foreign Agencies and Human Rights**

Concerns about potential impacts on human rights figured significantly in the Committee’s audit of this particular post. Balanced against these concerns was the basic imperative for having arrangements with foreign intelligence agencies in the first place—the need for CSIS to collect information that protects Canadians.

On several occasions in recent years the Committee has expanded on its position regarding CSIS liaison with foreign agencies. We believe the Service should take all possible care to ensure that the information it provides is not used to assist in the violation of human rights. To that end, SLOs are obligated to give the rest of the Service timely and accurate assessments of an agency’s human rights record and of its propensity to pass information on to third parties without authorization. The Service must avoid situations in which it gives information to an agency that does not violate human rights, only to find that the data have been passed on to other organizations that do.

With respect to the SLO post under review, the Committee identified no information exchanges that failed to conform to these standards. It is satisfied that all human rights assessments of agencies were properly carried out.

## **Ministerial Direction, Revised and Updated**

In February 2001, the Solicitor General issued a revised compendium of Ministerial Directions governing control and management of the Service—a development the Committee has looked forward to for some time.

### **THE EVOLUTION OF MINISTERIAL DIRECTION**

Section 6 of the *CSIS Act* states that the Director of CSIS has the “control and management” of the Service under the direction of the Minister—specifically, the Solicitor General of Canada. The principal mechanism by which this direction is given is through written instructions or “Ministerial Direction.” The Act stipulates



that the Committee be provided with copies of such directions “forthwith” after they are issued.

Ministerial Directions govern a wide spectrum of Service activities ranging from strategic policy, to guidance on specific matters such as the conduct of investigations involving sensitive institutions. In past reviews, the Committee has examined the adequacy of particular Directions, the ways in which the Service has interpreted Ministerial Directions through its own policies and procedures and how the Directions were implemented in individual cases.

Of recurrent concern to the Committee has been the disparate and patchy nature of Ministerial Directions when viewed as a whole. Over the course of the Service’s 17-year history, individual ministers often issued Directions on specific matters as and when they arose. Some Directions, which are still valid as Ministerial

Ministerial guidance is streamlined, consistent in its use of language and presented in a cohesive document

guidance, actually predate the creation of the Service. The result has been a hodgepodge of policy guidance employing sometimes contradictory language and using terminology no longer consistent with legislation.

#### **NEW DIRECTION: AN OVERVIEW**

The new compendium (a classified document), which replaces the old Direction in its entirety, goes a long way to rationalizing the Government’s strategic guidance of the Service and, in the Committee’s view, reflects a maturation of the legal and policy framework that governs the Service’s work. Ministerial guidance is now considerably streamlined, consistent in its use of language and presented in a concise and cohesive document.

It is too soon to assess the effect of the revised Directions on the Service’s operations. However, the compendium’s relative brevity and the strategic nature of the direction given suggests that there will be an increased focus on the Service’s own Operational Policies as the source for specific instructions and guidelines for implementation. Also apparent is an overall shift in discretionary powers from the Office of the Solicitor General to the Director of CSIS, with respect to the day-to-day management of the Service. In the course of future audits, the Committee intends to pay particular attention to how the new guidance is interpreted and implemented across the range of CSIS activities.

## Domestic Exchanges of Information (5)

---

### Report #2000-01

---

#### BACKGROUND

In carrying out its mandate to investigate suspected threats to the security of Canada, CSIS co-operates and exchanges information with federal and provincial departments and agencies and police forces across Canada. Section 17 of the *CSIS Act* sets out the Service's mandate to enter into these arrangements. Section 19(2) of the Act allows CSIS to disclose information to various domestic departments and agencies "for the purposes of the performance of its duties and functions."

The Review Committee is charged, under section 38(a)(iii) of the Act, with the task of examining the co-operative arrangements the Service has with domestic agencies, as well as the information and intelligence it discloses under those arrangements.

#### AUDIT SCOPE AND METHODOLOGY

The Committee examined all Service exchanges of information, including incidental disclosures, with other domestic agencies for the fiscal year 1999–2000. In addition, the Committee conducted an on-site review of information exchange practices in one Service regional office.

The purpose of the review was to determine whether the Service exchanged information with domestic bodies in conformity with Ministerial Direction, existing Memoranda of Understanding (MOU) with government institutions and police services, CSIS operational policies, the *CSIS Act* and other relevant statutes. In particular, the Committee's enquiries sought to determine if:

- the threat necessitating the exchange sufficiently outweighed the public's reasonable expectation of privacy;
- the exchange of information was strictly necessary to meet the Service's operational requirements as per section 12 of the *CSIS Act*;
- the exchange of information involved the unnecessary use of personal and sensitive information;
- the information exchanged was reasonable and factually accurate;
- all disclosures of information by CSIS to other bodies accorded with the limitations set out in section 19(2) of the *CSIS Act*;
- all exchanges of information were tracked in a consistent manner.

## COMMITTEE FINDINGS

### Overall co-operation

For the period under review, the Committee identified two information exchanges that raised concern. All others complied with the Service's mandate and conformed to existing policy. The information exchanged was reasonable and accurate and did not involve the unnecessary use of personal and sensitive information, nor did it infringe unduly on personal privacy.

### Retention of unsolicited information

The two cases that drew the Committee's attention both arose from our on-site audit of a CSIS regional office and involved how information received from domestic agencies was managed.

In the first case, the Service's database holding the unsolicited material contained several items relating to individuals and organizations for which CSIS did not have targeting authorizations. We asked the Service to explain its reasons for retaining this material and were satisfied with the explanation. The Committee believes that in future, however, the rationale for retaining unsolicited information of a similar nature should be clearly set out in the relevant operational reports.

**The Committee recommends that the purpose for retaining information under a general collection category be clearly identified in operational reports.**

The Service has since concurred with our recommendation and advised that the relevant section of operational policy will be amended accordingly.

The second case that drew our attention concerned the appropriateness of retaining certain information received from a domestic agency. The files related to the activities of a small group of minors. The Service told the Committee that it originally retained the material because it showed a propensity on the part of the group to engage in serious violence against persons or property for the purpose of achieving a political objective—a threat that lies within the Service's mandate. CSIS then decided, based on further assessment of the information, that no further action was required; however, it retained the original exchange of information.

The Committee fully recognizes the Service's responsibility to investigate information received from other bodies that appears to fall within its mandate. However, we question the need, in this case, to retain the information once the determination not to investigate further had been made. It is the Committee's view that the information should be deleted from CSIS records.

For its part, the Service reiterated its position on the validity of retaining the information in the first instance and noted that, in continuing to hold the information, it is preserving a formal record of information received and actions taken. The Service did agree to modify the operational reports to reflect the decision it ultimately made that the information warranted no further action on its part.

**The Committee recommends that the service employ greater diligence in deciding whether to retain unsolicited information.**

## Review of Warrant Preparation

---

### Report #2000-05

---

To obtain warrant powers under section 21 of the *CSIS Act*, the Service prepares an application to the Federal Court accompanied by a sworn affidavit presenting the reasons why intrusive powers are required to investigate a particular threat to the security of Canada. Because properly prepared affidavits are key to the integrity of the process, the Committee periodically reviews a number of warrants selected from among a comprehensive list of all warrants active during the audit period.

Although it is the sole responsibility of the Federal Court to issue a warrant, and to attach whatever conditions it deems appropriate, the Committee's purposes in reviewing the Service's warrant preparation are twofold:

- to ensure that the facts presented in the affidavit are consistent with the information used as the basis for its preparation;
- to ensure that the facts, circumstances and statements of belief contained in the affidavit are presented fairly and objectively.

From among the warrants issued in 1999–2000, the Committee selected two for detailed review; one a counter terrorism target, the other relating to a counter intelligence investigation. The Committee examined all CSIS documents relating to the preparation of the warrant affidavits: working files, “facing” binders, internal messages, Target Approval and Review Committee (TARC) minutes, Requests for TARC Authorities (RTAs) and the affidavits themselves.

In each of the cases selected, the Committee found that the affidavit the Service provided to the Federal Court was factually consistent with the supporting documentation and that the facts and circumstances presented in the affidavit were fairly and objectively expressed.

**REVISIONS TO WARRANT CLAUSES AND CONDITIONS**

As noted in last year's Report (*SIRC Report 1999–2000*), the Service has undertaken a broad revision of warrant clauses and conditions with a view to simplifying the terminology and bringing it into line with current legislation. Some operational and administrative procedures were also modified.

CSIS has informed the Committee that this process is now complete and that all Service personnel involved either with applying for warrants or implementing them have been fully briefed. All changes reflected in subsequent warrant applications have been approved by the Federal Court of Canada.

**Security Screening Briefs to Citizenship and Immigration Canada**

---

**Report #2001-02**

---

The aim of this study was to assess the information provided by CSIS to the Minister of Citizenship and Immigration Canada (CIC) in its mandated role to assist the government's immigration monitoring program by supplying security screening services. The Committee last examined the Service's role in immigration in its 1997–1998 Report. Our review this year focussed specifically on the nature and quality of the advice CSIS gave to CIC in the form of written briefs.

**METHODOLOGY OF THE AUDIT**

For this review the Committee examined 16 of the Service's immigration security screening investigations selected from the 166 briefs sent by CSIS to CIC in the 1999–2000 fiscal year. The sample consisted of nine inland cases and seven overseas-based cases. The Committee reviewed the briefs sent to CIC and all supporting documents relevant to each investigation.

**HOW THE SERVICE PROVIDES ADVICE**

CSIS has the sole responsibility to provide security screening assessments for immigration applications originating in both Canada and the US. For immigration applications originating elsewhere, it is up to the Immigration Program Manager at the Canadian overseas mission concerned to request a Service security screening assessment. In either case, regardless of the advice CSIS gives to CIC, the final decision on any potential immigrant's admissibility rests with the Minister of Citizenship and Immigration.

A typical immigration security screening investigation begins when the Service receives a request from either a Case Processing Centre (CPC) in Canada or an

Immigration Program Manager at a Canadian mission overseas. The investigation ends when the Service provides its advice to CIC in one of four forms:

**No Reportable Trace (NRT)**—a report given to CIC when the Service has no adverse information on the immigration applicant.

**Inadmissible Brief**—advice provided when the Service has concluded, based on information available to it, that the applicant meets the criteria outlined in the security provisions of section 19 of the *Immigration Act*.

**Information Brief**—advice provided by CSIS that it has information that the applicant is or was involved in activities as described in the security provisions of the *Immigration Act*, but that it is of the opinion that the applicant does not fall into the class of persons deemed to be inadmissible under the Act.

**Incidental Letter**—provided to CIC when the Service has information that the applicant is or was involved in non-security-related activities described in section 19 of the *Immigration Act* (for example, war crimes or organized criminal activity) or any other matter of relevance to the performance of duty by the Minister of Citizenship and Immigration, as set out in section 14(b) of the *CSIS Act*.

All the Service briefs to CIC were found to be accurate and adequately supported by the information collected

## FINDINGS OF THE COMMITTEE

### Nature of the Service's Advice

All the Service briefs to CIC in which the Service rendered an opinion were found to be accurate and adequately supported by the information collected. We identified one instance in which the Service was unable to provide meaningful advice because it lacked sufficient information.

Overall, the Committee noted that the Service prepared more briefs for inland cases than for overseas-based cases, despite the fact that most immigration cases originate overseas. This issue will be examined in a future review.

### Essential Statistics

During the year reviewed, the Service conducted 81 650 immigration security screening assessments, most of which resulted in a “No Reportable Trace” (NRT) response. The Service provided 166 briefs to CIC, 109 of which were inadmissible

briefs. The average time the Service needed to process an immigration security screening case that resulted in an information brief was 661 days. For cases generating an inadmissible brief, the average was 644 days. The Service's explanation for the turnaround times is found in Section 2: Security Screening, page 34.

### Recent Developments

In the Committee's Report for 1997–1998, we voiced concerns about flaws in procedures for the security screening of refugee claimants in Canada. We expressed the view that the Service could and should play a greater role in assisting CIC's efforts in this area.

### **“Grounds to Suspect” “Grounds to Believe” Threats to Security and Inadmissibility in Canadian Law**

The security screening assistance rendered by the Service takes the form of information sharing with CIC on matters concerning threats to the security of Canada, as defined in section 2 of the *CSIS Act*, and advice to CIC with respect to the inadmissibility classes in section 19 of the *Immigration Act*. These are separate Acts of Parliament and they contain distinct provisions—“threats to the security of Canada” and “inadmissibility to Canada”—each of which are brought to bear on immigration security issues.

An individual applying for immigration to Canada may be deemed inadmissible in accordance with criteria set out in section 19 of the *Immigration Act*. However, any individual (immigration applicant or otherwise) may also meet the criteria for being a threat to the security of Canada as defined in the *CSIS Act*.

The threshold for inadmissibility under the *Immigration Act* is higher than that for commencing an investigation under section 12 of the *CSIS Act*. To target an individual for a section 12 investigation the Service must have reasonable grounds to “suspect” that a person or a group poses a threat to the security of Canada. By contrast, for CIC to refuse admission for security reasons the Service's inadmissibility brief must help support its conclusion that there are reasonable grounds to “believe” that the applicant is a member of a class of inadmissible persons—a stricter standard to meet under the law.

In its briefs to CIC, the Service provides an assessment of an applicant's admissibility with reference to the *Immigration Act*. However, the Service's role in the process is not to provide advice on whether the applicant poses a threat to the security of Canada as defined in the *CSIS Act*.

The Committee has recently been advised that the Service and CIC have developed the “Front End Screening” program for refugee claimants in Canada. All refugee claimants would at the time of making a claim be subject to a screening process similar to that for applicants for permanent residence. The aim of the program is to prevent persons from being able to enter Canada and remain for an indefinite period of time without undergoing a security screening assessment—a significant risk under the procedures in place at the time of our earlier review.

This and other recent developments in the co-operative relationship between CSIS and CIC will be followed closely by the Committee.



## **B. Annual Audit of CSIS Activities in a Region**

Every year the Committee audits the entire range of CSIS's investigative activities—targeting, special operations, warrants, community interviews and sensitive operations—in a particular region of Canada. Such a comprehensive examination provides insight into how the Service employs the various investigative tools at its disposal and allows the Committee to assess the ways in which Ministerial Direction and CSIS policies are implemented by the operational sections of the Service.

### **Targeting of Investigations**

The targeting portion of the regional audit reviews how the Service applies its duties and functions as set out in sections 2 and 12 of the *CSIS Act*. The day-to-day management of investigations is governed by both Ministerial Direction and CSIS operational policies.

In reviewing the appropriateness of any Service investigation, the Committee uses three main criteria:

- 1) Did the Service have reasonable grounds to suspect a threat to the security of Canada?
- 2) Was the level and intrusiveness of the investigation proportionate to the seriousness of the target's threat-related activity?
- 3) Did the Service collect only that information strictly necessary to fulfill its mandate to advise the Government of a threat?

### **METHODOLOGY OF THE AUDIT**

Seven investigations were selected for this year's audit—five counter terrorism and two counter intelligence. The Committee examined all files and electronic documents associated with each of the seven cases. We interviewed both the regional managers directly responsible for the investigations and supervisory headquarters staff.

### **FINDINGS OF THE COMMITTEE**

Based on the information reviewed, the Committee was satisfied that in all seven cases the Service had reasonable grounds to suspect a threat to the security of Canada. Neither the files and operational messages we examined nor the interviews we conducted gave any indication that the levels of investigation were out of proportion to the perceived threats.

We also reviewed the information collected in all seven cases. In one instance, certain data collected raised concerns as to whether they met the “strictly necessary” test. Although the Service provided an explanation, the Committee was not

## **Management of Targeting**

### ***Target Approval and Review Committee***

The Service's 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 that are related to, or emanate from, that specific issue.

entirely satisfied with that response. We believe that the information collected did not meet the strictly necessary test, and we were not satisfied that, in this instance, the Service had adhered fully to the existing operational policies and guidelines governing collection.

## Warrant Implementation

Under section 21 of the *CSIS Act*, only the Federal Court can grant CSIS the warrant powers required to use the most intrusive investigative procedures available to it, such as telephone or mail intercepts. Every year the Committee reviews how warrants are implemented in a number of cases selected from the files of a particular region.

The Committee's review involves assessing:

- how the Region used the warrant powers granted by the Federal Court;
- whether the Region complied with all clauses and conditions contained in the warrants;
- whether the Region's implementation of the warrants was carried out in accordance with the Act, CSIS policy and Ministerial Direction.

## FINDINGS OF THE COMMITTEE

### Warrant Implementation

The Committee's review of the selected warrants and the associated investigation files revealed no instances of unnecessary use of warrant powers. All collection activities were carried out in accordance with the clauses and conditions contained in the warrants. However, with respect to the Service's collection and retention of product from certain warrants, the Committee identified possible anomalies in two of the cases reviewed.

All collection activities were carried out in accordance with the clauses and conditions contained in the warrants

In the first, the Committee questioned why the Service retained a particular kind of data beyond the standard period established in CSIS operational policies. In response, the Service advised the Committee that the special retention was authorized so that assistance could be rendered to an allied agency's investigation of a terrorist network.

The second case concerned the intercepting and reporting on the communications of persons not named in the warrant. In both instances where this appeared to have taken place, the Committee subsequently was satisfied with the Service's explanation that both interceptions were appropriate and within the law (one under the provisions of the "basket clause" and the other because the intercepted person qualified as a "Vanweenan").

### **Shortage of Special Resources**

The Committee's examination of the Region's investigation files showed that the Region suffered from the shortage of a particular expert resource. Although the resulting delays had no adverse effects in the cases we examined, the Committee would not wish to see a delay in processing unduly hinder the timely distribution of important information to appropriate officials. The Committee has expressed similar concerns in the past, and we are encouraged by the Service's initiatives to remedy the situation in this Region.

## **Audit of Sensitive Operations**

Using human sources in collecting information is essential to effectively investigating threats to public safety and national security. However, the sensitivity of such operations is such that they are the subject of special Ministerial Direction. In addition, the procedures for implementing sensitive operations are set out in some detail in the *CSIS Operational Policy Manual*. All requests for sensitive operations, or for investigations involving "sensitive institutions" require the approval of Service senior management.<sup>2</sup>

- 
1. The basket clause permits intercepting communications of persons who, while not named in a warrant, may be present at a location named in the warrant. The legality of the clause was upheld by the Supreme Court of Canada in *R v. Chesson*, [1988] 2 S.C.R. 148. Affirmed in the same judgement was the legality of intercepting a person named or described ("spouse" or "colleague", for example) in the warrant but not specifically targeted, likely to have regular contact with the target, and whose communications the investigating agency has reasonable grounds to believe may assist the investigation. The name of one of the parties to the "Chesson" case—Vanweenan—has since come to denote this category of persons.
  2. Sensitive institutions are defined as trade unions, the media, religious institutions and university and college campuses.

## METHODOLOGY OF THE AUDIT

The Committee reviewed a set of randomly selected human source operations as well as all requests to senior managers involving sensitive institutions. In each instance, we examined all files related to recruiting, developing and directing the human source in question. The purpose of the review was to assure ourselves that in handling human sources and conducting investigations involving sensitive institutions, the Service had complied with the Act, Ministerial Direction and its own operational policies.

## FINDINGS OF THE COMMITTEE

With respect to both the Region's development and direction of human sources and its investigations involving sensitive institutions, the Committee concluded that the Service's actions were reasonable, appropriate and necessary for properly fulfilling its mandate.

We did identify, however, an area where the Regional office had not fully complied with Service policies governing certain administrative procedures. The Committee believes that periodic verification by Regional office management could have avoided this administrative shortcoming.

## Internal Security

### OVERVIEW

The Committee's inquiries showed that, within the Regional office, the level of awareness about security was generally high, and that management had undertaken appropriate measures to ensure vigilance among Service employees. We did observe, however, that the Region had conducted significantly fewer random luggage searches of its employees than CSIS offices in other regions. The Service informed us that for fiscal year 2001–2002, the Region's objective is to conduct luggage searches monthly.

The breach occurred because the two Service employees involved left their vehicle out of sight and unattended

### A BREACH OF SECURITY

The Committee examined the files regarding a security breach case that occurred during the period under review. The breach involved the theft of classified assets and material from an operational vehicle. Our review showed that the Region and

CSIS Headquarters internal security representatives had effectively investigated the incident, and that appropriate remedial measures had been taken to reduce the potential for similar security breaches in the future.

Two matters concerning the case drew the Committee's attention. First, the breach occurred because the two Service employees involved left their vehicle out of sight and unattended, which was, in the Committee's view, a lapse in judgement. Second, although in the wake of the incident the Service subsequently made constructive changes to security policies and procedures, the Committee believes that some unnecessary ambiguities remained that had the potential to weaken the policy overall.

Responding to the Committee's observations, the Service asserted that the breach did not stem from a lapse in judgement, that its employees had taken all necessary precautions and followed all established procedures and, moreover, that no disciplinary actions were contemplated. The Service agreed to adjust its policy manual to reduce the possibility of misinterpretation.

## **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.

## **Section 2**

---

### **Security Screening and Investigation of Complaints**



## Security Screening and Investigation of Complaints

The Committee has a dual mandate under the *CSIS Act*: to review all CSIS activities and to investigate complaints about those activities. This section of the report deals with the second of the Committee's main responsibilities. In addition, since some of the complaints received arise out of the Service's security screening functions, our review of this part of the Service's mandate provides appropriate background and context for the subsequent discussion of complaints.

### A. Security Screening

The Service has the authority, under section 13(1) of the *CSIS Act*, to provide security assessments to federal government departments. In addition, the Service may, with appropriate Ministerial approval, enter into arrangements to provide assessments to provincial government departments or provincial police forces, as outlined in section 13(2). Arrangements for the provision of security screening advice to foreign governments, foreign agencies and international institutions and organizations are authorized under section 13(3).

For federal employment, CSIS security assessments serve as the basis for determining whether an individual should be granted access to classified information or assets. In immigration cases, Service assessments can be instrumental in Citizenship and Immigration Canada's decision to admit an individual into the country and in granting permanent resident status or citizenship.

### SECURITY SCREENING FOR FEDERAL EMPLOYMENT

#### 2000–2001 Key Statistics

- The Service received 36 803 requests for security screening assessments for clearances, levels one through three, new, upgraded and updated. A preponderance of the total were for Level II clearances. In addition, 418 requests were for action relating to administrative procedures, such as transfers and downgrades.
- The average time required to complete a Level I security assessment was 32 days; for Level II, 41 days; and for Level III, 113 days.

## 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*.

### ***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 that 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.

- Of the 3670 field investigations conducted, the largest number was for the Department of National Defence, followed by CSIS, the Department of Foreign Affairs and International Trade, the Communications Security Establishment and the Department of Public Works and Government Services.
- The Service received 37 128 requests for assessments under the Airport Restricted Access Area Clearance Program (ARAACP), which is under the authority of Transport Canada. The average turnaround time for a request under ARAACP was 32 days, a significant increase from last year's figure of 4 days. The Service attributed the difference to the volume of security screening requests and the resulting backlog of cases waiting to be processed.
- There were 1439 requests for security assessments related to "site access." These involve basic checks to provide clearances allowing an individual access to sensitive sites.
- With the RCMP acting as intermediary, the Service received 268 requests for accreditation to access the Parliamentary Precinct and 11 129 requests for accreditation to special events and functions to which access is controlled.

### **IMMIGRATION SECURITY SCREENING PROGRAMS**

Under the authority of sections 14 and 15 of the *CSIS Act*, the Service conducts security screening investigations and provides advice to the Minister of Citizenship and Immigration Canada (CIC). Generally speaking, the Service's assistance 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 the form of "assessments" with respect to the inadmissibility classes of section 19 of the *Immigration Act*.

### **Applications for Permanent Residence from Within Canada**

The Service has the sole responsibility for screening immigrants and refugees who apply for permanent residence status from within Canada. In 2000–2001, the Service received 44 278 such screening requests.<sup>7</sup> The median turnaround time for screening applications was 66 days—with an average of 60 days to process electronic applications and 195 days for paper applications.

---

7. This number includes 4217 requests for security screening of applications originating in the USA and processed in Canada.

### Applications for Permanent Residence from Outside Canada

Immigration and refugee applications for permanent residence that originate outside Canada or the USA are managed by the Overseas Immigrant Screening Program under which the Service shares responsibility for security screening with CIC officials based abroad. Generally, CSIS only becomes involved in the screening process if requested to do so by the Immigration Program Manager (IPM) or upon receiving adverse information about a case from established sources. This division of labour allows the Service to concentrate on the higher risk cases.

In 2000–2001, the Service received 25 109 requests to screen overseas applicants. Of these, CSIS reported that 4433 applicant files were referred by IPMs to CSIS Security Liaison Officers (SLOs) for consultation from April 1 to December 31, 2000.

### Nature of the Service's Advice to CIC

Requests for security screening in relation to immigration resulted in 216 CSIS briefs to CIC—167 inadmissible briefs and 49 information briefs. During the period under review, the average time taken for the Service to process a case involving a brief was about a year and a half. The Service sent 90 “incidental

letters” to CIC and 61 update letters. (See page 12 for a description of the Service's security screening briefs and other information-sharing mechanisms employed in aid of Canada's immigration programs.)

The times taken by CSIS to process requests from CIC rose significantly over those of previous years

### Security Screening: Increased Turnaround Times

Overall, the times taken by CSIS to process requests from CIC rose significantly over those of previous years. The Service cited two main causes for the increased delays, both of which it regards as temporary. There had accumulated a significant number of overseas, “hard copy” cases, which take significantly longer to process than the Canada-based electronic cases. CSIS assured the Committee that it has eliminated this backlog and taken steps to prevent future backlogs. In addition, problems during the year in implementing new software combined with the necessary adjustments for the Y2K problem created further delays. The software difficulties are in the process of being resolved.

### Citizenship Applications and the Watch List

As part of the citizenship application process, the Service receives electronic trace requests from CIC's Case Processing Centre in Sydney, Nova Scotia. The names of

citizenship applicants are cross-checked against the names in the Security Screening Information System database. The Service maintains a Watch List, which is made up of individuals who have come to the attention of CSIS through, *inter alia*, TARC-approved investigations and have received landed immigrant status.

In 2000–2001, the Service reviewed 161 895 citizenship applications. CSIS recommended that citizenship be denied in four instances and prepared information briefs in relation to 78 others. In one case, the Service sought Ministerial approval to defer its advice.<sup>8</sup>

### **A New Program: Refugee Screening**

As discussed in the Committee's review of immigration security screening briefs (*see* page 12) the Service and CIC have recently concluded an agreement to conduct "Front-End Screening" of refugee applicants. Starting as a pilot project, facilities for exchanging electronic information are to be installed at five CIC sites across Canada.

### **SCREENING ON BEHALF OF FOREIGN AGENCIES**

The Service may enter into reciprocal arrangements with foreign agencies to provide security checks on Canadians and other individuals who have resided in Canada. In the period under review, the Service concluded 995 foreign screening checks, 66 of which required field investigations. These investigations resulted in one information brief to the client.

## **B. Investigations of Complaints**

In addition to the Committee's audit and review functions, we have the added responsibility to investigate complaints from the public about any CSIS action. Three kinds of complaints come within the Committee's purview:

- 1) Acting as a quasi-judicial tribunal, the Committee is empowered to consider and report on any matter having to do with federal security clearances, including complaints about denials of clearances to government employees and to contractors.

---

8. 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.

- 2) The Committee can investigate reports made by federal ministers about persons in relation to citizenship and immigration, certain human rights matters and organized crime.
- 3) As stipulated in the *CSIS Act*, the Committee can receive at any time a complaint lodged by a person “with respect to any act or thing done by the Service.”

#### **FINDINGS ON SECTION 41 COMPLAINTS RE: “ANY ACT OR THING”**

During the 2000–2001 fiscal year, the Committee dealt with 69 complaints made in relation to section 41 of the *CSIS Act*. Of these, 52 were new complaints and 17 were cases carried forward from the previous fiscal year (*see* Table 2).

#### **Complaints Related to Immigration Matters**

Continuing a pattern set in recent years, many of the complaints conveyed to the Committee in 2000–2001 related to the Service’s role in Canada’s immigration program—34 cases in all.

#### **Complaints Concerning Improper Conduct and Abuse of Power**

The Committee dealt with 20 complaints in the period under review from persons who alleged that the Service had subjected them to surveillance, illegal actions or had otherwise abused its powers.

So as not to confirm indirectly which targets are of interest to the Service, the Committee does not as a rule confirm or deny if a complainant is the subject of a

**Table 2**  
**Complaints (April 1, 2000 to March 31, 2001)**

	New complaints	Carried over from 1999–2000	Closed in 2000–2001	Carried forward 2000–2001
CSIS activities	52	17	30	39
Security clearances	0	4	2	2
Immigration	0	1	1	0
Citizenship	0	1	1	0
Human rights	0	1	1	0

CSIS targeting authority. Although this information is not provided to complainants, the Committee thoroughly investigates the complainant's allegations.

Through its investigations, the Committee assures itself that the Service's activities have been carried out in accordance with the Act, Ministerial Direction and CSIS policy. If we find that the Service has acted appropriately, we convey that assurance to the complainant. If the Committee identifies issues of concern, we share those with the Director of CSIS and the Solicitor General, and to the extent possible, report on the matter in our annual report.

During 2000–2001, most of the Committee's investigations into this type of complaint revealed that the Service was neither involved in, nor responsible for, the activities alleged by the complainant.

### **Complaints the Committee is Precluded from Investigating**

The Committee received 26 complaints that it was precluded from investigating because the criterion set out in section 41 of the Act, which requires that complaints first be sent to the Director of CSIS, had not been met. The Committee responds to such complaints by outlining the requirements of section 41 and providing the address to communicate with the Director. The Committee is also precluded from investigating complaints in which complainants are entitled to seek redress through a grievance procedure established under the *CSIS Act* or the *Public Service Staff Relations Act*.

### **Misdirected Complaints**

The Committee received 12 complaints that either did not involve the Service or were not related to matters of national security. In such cases, the Committee informs the individual that the complaint is not within our jurisdiction and, if possible, redirects the complainant to the appropriate authorities.

### **SECURITY CLEARANCE COMPLAINTS**

The Committee dealt with four complaints under section 42 of the Act relating to security clearances in 2000–2001. Two cases, involving the revocation of security clearances, were completed; in one instance the complaint was withdrawn and, in the other, the Committee investigated and reached a decision, which is summarized in Appendix D. The other two complaints concerned Service recommendations to deny security clearances; the Committee's inquiries into these complaints continue.

## **FINDINGS ON MINISTERIAL REPORTS**

### **Citizenship Refusals**

In the ongoing matter of the citizenship application of Ernst Zündel—a matter first brought before the Committee in 1995—we were notified in December 2000 that Mr. Zündel was withdrawing his application for Canadian citizenship, and that this withdrawal had been accepted by Citizenship and Immigration Canada. In light of this information, there was no basis for continuing to investigate the matter. The Committee will not, therefore, issue a report on the matter to the Governor in Council pursuant to section 19(6) of the *Citizenship Act*.

### **Reports Pursuant to the *Immigration Act***

The Committee received no such Ministerial Reports during the period under review. As discussed in last year's Report, a case relating to a SIRC decision issued in 1998 (Yamani) was referred back to the Committee in March 2000 for reconsideration. The Committee has since been advised that Citizenship and Immigration Canada has decided not to pursue the matter. As a result, the case is no longer before the Committee.

### **CANADIAN HUMAN RIGHTS COMMISSION REFERRAL**

The Committee received no Human Rights Commission referrals in the period under review. However, the investigation of a referral received last year was completed and reported to the Commission.



## **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.

## **Appendix A**

---

### **Abbreviations**



## Abbreviations

ARAACP	Airport Restricted Access Area Clearance Program
CI	Counter Intelligence Branch
CIC	Citizenship and Immigration Canada
CPC	Case Processing Centre (CIC)
Committee	Security Intelligence Review Committee (SIRC)
CSE	Communications Security Establishment (DND)
CSIS	Canadian Security Intelligence Service
CT	Counter Terrorism Branch
DFAIT	Department of Foreign Affairs and International Trade
Director	The Director of CSIS
DND	Department of National Defence
EXIPC	Executive Intelligence Production Committee
GSP	Government Security Policy
IAC	Intelligence Assessment Committee (Privy Council Office)
IPM	Immigration Program Manager (CIC)
MOU	Memorandum of Understanding
NRT	No Reportable Trace
RAP	Requirements, 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
TARC	Target Approval and Review Committee

## **Appendix B**

---

### **SIRC Reports and Studies Since 1984**

## 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* (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* (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* (UNCLASSIFIED)\* (86/87-04)
7. *Counter-Subversion: SIRC Staff Report* (SECRET) (87/88-02)
8. *SIRC Report on Immigration Screening* (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* (PUBLIC VERSION) \* (87/88-04)
10. *The Intelligence Assessment Branch: A SIRC Review of the Production Process* (SECRET)\* (88/89-01)
11. *SIRC Review of the Counter-Terrorism Program in the CSIS* (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* (SECRET) \* (89/90-02)

13. *SIRC Report on CSIS Activities Regarding the Canadian Peace Movement* (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* (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 (1996–97)* (SECRET) (SIRC 1997-02)
96. *Foreign Conflict—Part I* (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—Part I* (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)
106. *Foreign Conflict—Part II* (TOP SECRET) (SIRC 1997-03)
107. *Review of Transnational Crime* (SECRET) (SIRC 1998-01)
108. *CSIS Cooperation with the RCMP—Part II* (SECRET) \* (SIRC 1998-04)
109. *Audit of Section 16 Investigations & Foreign Intelligence 1997–98* (TOP SECRET) (SIRC 1998-07)
110. *Review of Intelligence Production* (SECRET) (SIRC 1998-09)
111. *Regional Audit* (TOP SECRET) (SIRC 1998-10)
112. *CSIS Liaison with Foreign Agencies* (TOP SECRET) (SIRC 1998-11)
113. *Allegations by a Former CSIS Employee* (TOP SECRET) \* (SIRC 1998-12)
114. *CSIS Investigations on University Campuses* (SECRET) (SIRC 1998-14)
115. *Review of Foreign Intelligence Activities in Canada* (TOP SECRET) (SIRC 1998-15)
116. *Files* (TOP SECRET) (SIRC 1998-16)
117. *Audit of Section 16 Investigations & Foreign Intelligence* (TOP SECRET) (SIRC 1999-01)
118. *A Long-Running Counter Intelligence Investigation* (TOP SECRET) (SIRC 1999-02)

119. *Domestic Exchanges of Information* (TOP SECRET) (SIRC 1999-03)
120. *Proliferation* (TOP SECRET) (SIRC 1999-04)
121. *SIRC's Comments on the Draft Legislation Currently Before Parliament—Bill C-31* (PROTECTED) \* (SIRC 1999-05)
122. *Domestic Targets* (TOP SECRET) (SIRC 1999-06)
123. *Terrorist Fundraising* (TOP SECRET) (SIRC 1999-07)
124. *Regional Audit* (TOP SECRET) (SIRC 1999-08)
125. *Foreign State Activities* (TOP SECRET) (SIRC 1999-09)
126. *Project Sidewinder* (TOP SECRET) (SIRC 1999-10)
127. *Security Breach* (TOP SECRET) (SIRC 1999-11)
128. *Domestic Exchanges of Information 1999–2000* (TOP SECRET) (SIRC 2000-01)
129. *Audit of Section 16 Investigations and Foreign Intelligence Reports 1999–2000* (TOP SECRET) (SIRC 2000-02)
130. *CSIS Liaison with Foreign Agencies* (TOP SECRET) (SIRC 2000-03)
131. *Regional Audit* (TOP SECRET) (SIRC 2000-04)
132. *Warrant Review* (TOP SECRET) (SIRC 2000-05)
133. *Review of CSIS Briefs to Citizenship and Immigration Canada 1999–2000* (TOP SECRET) (SIRC 2001-02)

## **Appendix C**

---

### **Major Findings and Recommendations**

## Major Findings and Recommendations

### CSIS LIAISON WITH FOREIGN AGENCIES

The Committee audited a Security Liaison Officer (SLO) post overseas that operates in an especially difficult working environment. Maintaining the security of the physical operating environment is a major ongoing challenge. The situation is compounded by generally onerous working conditions. The Committee was struck by the substandard conditions in which Service staff were obliged to work. The poor physical facilities at Canada's mission, a heavy workload arising from increasingly large numbers of immigration and visa applications requiring security screening all combine to form an adverse environment. Notwithstanding these difficult circumstances, however, the SLO and staff are performing well.

We found that while the SLO has made steady progress with foreign interlocutors, rising demands from the immigration side of the SLO's mandate left less time for developing relationships with other countries in the region for which the post is nominally responsible.

The evident work overload gave rise to concerns on the part of the Committee that some of the post's important functions might not be being handled expeditiously. Service senior management told the Committee that it shared our concerns and believed that the immigration workload problem extended to certain other of its SLO posts as well. It is the Committee's view that the Service might wish to review this element of its Foreign Liaison Program.

The Committee examined all documentation associated with operational co-operation and information exchanges involving the SLO post from March 31, 1998 through June 30, 2000. Our review identified only one problematic exchange. We advised the Service that it should consider providing updated information to clients so that earlier advice is regarded in its proper context.

Concerns about potential impacts on human rights figured significantly in the Committee's audit of this particular post. SLOs are obligated to give the rest of the Service timely and accurate assessments of an agency's human rights record, and of its propensity to pass information on to third parties without authorization. With respect to the SLO post under review, the Committee identified no information exchanges that failed to conform to these standards and satisfied itself that all human rights assessments of agencies had been properly carried out.

**MINISTERIAL DIRECTION, REVISED AND UPDATED**

In February 2001, the Solicitor General issued a revised compendium of Ministerial Directions governing control and management of the Service—a development the Committee has looked forward to for some time.

The new compendium (a classified document) goes a long way to rationalizing the Government's strategic guidance of the Service and, in the Committee's view, reflects a maturation of the legal and policy framework that governs the Service's work. Ministerial guidance is now considerably streamlined, consistent in its use of language and presented in a concise and cohesive document. Also apparent is an overall shift in discretionary powers from the Office of the Solicitor General to the Director of CSIS, with respect to the day-to-day management of the Service. In the course of future audits, the Committee intends to pay particular attention to how the new guidance is interpreted and implemented across the range of CSIS activities.

**DOMESTIC EXCHANGES OF INFORMATION (5)**

The Committee examined all Service exchanges of information with other domestic agencies for the fiscal year 1999–2000. In addition, the Committee conducted an on-site review of information exchange practices in one Service regional office.

For the period under review, the Committee identified two exchanges that raised concern. In the first case, the Service's database holding the unsolicited material contained several items relating to individuals and organizations for which CSIS did not have targeting authorizations. We asked the Service to explain its reasons for retaining this material and were satisfied with the explanation. The Committee believes that in future, however, the rationale for retaining unsolicited information of a similar nature should be clearly set out in the relevant operational reports.

**The Committee recommends that the purpose for retaining information under a general collection category be clearly identified in operational reports.**

The second case concerned the appropriateness of retaining certain information received from a domestic agency about the activities of a small group of minors. CSIS subsequently decided that no further action was needed but retained the original exchange of information in its files. It is the Committee's view that the information should be deleted from CSIS records. The Service did agree to modify

the operational reports to reflect the decision it ultimately made that the information warranted no further action on its part.

**The Committee recommends that the Service employ greater diligence in deciding whether to retain unsolicited information.**

#### **SECURITY SCREENING BRIEFS TO CIC**

The Committee examined a selection of the Service's immigration security screening investigations from the 166 briefs sent by CSIS to CIC in the 1999–2000 fiscal year. The Committee reviewed the briefs sent to CIC and all supporting documents relevant to each investigation. All the Service briefs to CIC in which the Service rendered an opinion were found to be accurate and adequately supported by the information collected.

The Committee has recently been advised that the Service and CIC have developed a “Front End Screening” program for refugee claimants in Canada. The aim of the program is to prevent persons from being able to enter Canada and remain for an indefinite period without undergoing a security screening assessment—a significant risk under the procedures in place at the time of a previous Committee review.

## **Appendix D**

---

### **Complaint Case Histories**



## Complaint Case Histories

This appendix summarizes complaint cases submitted to the Review Committee during the past year on which decisions have been reached. Not addressed here are complaints that were handled through administrative review, were misdirected or were deemed to be outside the Committee's jurisdiction.

Where appropriate, complaints are investigated through a quasi-judicial hearing presided over by a Member of the Committee. After the hearings are complete, the presiding member renders a decision that is provided to the Solicitor General and the Director of CSIS. After any information with national security implications is removed, the complainant also receives a copy of the decision.

The Committee reported on two decisions reached during the period under review: one was a section 42 (denial of security clearance) matter and the other concerned a complaint lodged in accordance with section 41—"any act or thing."

### **CASE #1**

The complainant was a former employee of the Service whose security clearance was revoked in 1999. As a result, the complainant was dismissed from the Service at which time the individual filed a complaint contesting the Service's denial of security clearance.

The Service's justification for revoking the clearance was based on the contention that the employee had failed to prevent classified information from being disclosed to the news media and, thus, had violated the professional oath taken by all Service employees. Since a security clearance was a prerequisite to being employed by the Service, dismissal followed immediately.

The complainant asserted that there was no justification for the Service's position in respect to the public disclosure. The complainant had contacted the news media to discuss a discrimination complaint against the Service. The complainant cast doubt on how thoroughly the Service investigated the matter and suggested, moreover, that the dismissal was carried out to hide errors made by the Service.

The Committee's investigation failed to find any information that supported the complainant's claims. The CSIS operation, which was the subject of the disclosure, was a legitimate activity undertaken in accordance with policy and the law.

Although the Service did make errors in managing the operation, this fact did not, in the Committee's view, absolve the employee of responsibility to protect classified information.

With regard to the Service's investigation of the unauthorized disclosure, our own inquiries showed that the Director's decision to revoke the security clearance was based on incomplete information. Nevertheless, the Committee found that the Director did have information sufficient to revoke the complainant's security clearance.

As the complainant's employment with the Service required a Level III clearance, the dismissal of the complainant subsequent to the revocation of the complainant's security clearance was inevitable. However, the Committee recommended that the Service facilitate the complainant's reassignment to another department of government, consistent with Government Security Policy. In addition, the Committee recommended that the Service reassess certain of its information management methods and procedures.

#### **CASE #2**

The complaint, lodged under section 41 of the *CSIS Act*, alleged that a particular Service operation had exposed the complainant to dangerous individuals, that a Service officer had behaved in a threatening and intimidating manner towards the complainant causing undue stress and anxiety and that the Service had ignored requests by the complainant for assistance. The complainant also made a claim for damages suffered as a result of lost income.

The Committee found no grounds to support the complainant's allegations. There was no evidence that the complainant had been put at risk by the Service, nor was there any evidence of malice or intimidation by the Service towards the complainant. The complainant admitted to the Committee that the Service officer had not in fact acted in a threatening or intimidating manner. The Committee also concluded that there was no basis for recommending the reimbursement of lost income.

Although the Committee found the complaint itself to be unfounded, we did note serious problems with the Service's supervision of the operation at issue. The Committee made a number of recommendations to the Service aimed at improving management and operating procedures in similar types of operations in the future.