



SECURITY INTELLIGENCE  
REVIEW COMMITTEE

# SIRC Report 2003–2004

An Operational Review of the  
Canadian Security Intelligence Service

Canada



Security Intelligence Review Committee  
P.O. Box 2430, Station "D"  
Ottawa ON  
K1P 5W5

Tel: (613) 990-8441

Fax: (613) 990-5230

Web Site: <http://www.sirc-csars.gc.ca>

Collect calls are accepted between 8:00 a.m. and 5:00 p.m. Eastern Standard Time.

© Public Works and Government Services Canada 2004

Cat. No. PS71-1/2004

ISBN 0-662-68381-1



**SECURITY INTELLIGENCE  
REVIEW COMMITTEE**

# **SIRC Report 2003–2004**

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

## The Committee

---



Photo: Couvrette/Ottawa

Chair: The Honourable Paule Gauthier (centre)

Left to right: The Honourable Baljit S. Chadha, The Honourable Raymond Speaker,  
The Honourable Roy Romanow, The Honourable Gary Filmon

September 30, 2004

The Honourable Anne McLellan, P.C., M.P.  
Deputy Prime Minister and Minister of Public Safety  
and Emergency Preparedness  
House of Commons  
Ottawa, Ontario  
K1A 0A6

Dear Minister:

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 2003–2004, for your submission to Parliament.

Yours sincerely,



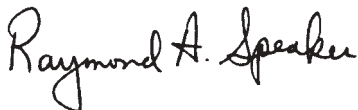
Paule Gauthier, P.C., O.C., O.Q., Q.C.  
Chair



Baljit S. Chadha, P.C.



Roy Romanow, P.C., O.C., Q.C.



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



Gary Filmon, P.C., O.M.



# Contents

---

<b>Statement from the Committee</b> .....	vii
<b>Section 1: SIRC Review and Complaints Functions</b> .....	1
<b>A. Reviews of CSIS Security Intelligence Activities</b> .....	3
How SIRC Carries Out Its Review Function—An Overview .....	3
The Committee's Role in CSIS's Accountability Structure .....	3
Identifying SIRC Studies—Choices and Challenges .....	3
SIRC Reviews in 2003–2004 .....	4
Front End Screening Program .....	5
CSIS Section 12 Operational Activity Outside Canada .....	10
Review of a Counter Intelligence Investigation .....	13
Review of a Counter Proliferation Investigation .....	15
CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post .....	17
Internal Security Breach in a CSIS Regional Office .....	20
Review of Foreign Arrangements .....	21
<b>B. Investigations of Complaints</b> .....	23
Report of Decision .....	25
Section 42 Denial of Security Clearance .....	25
<b>Section 2: CSIS Accountability Mechanisms</b> .....	27
<b>A. Policy and Governance Framework</b> .....	29
2003–2004 National Requirements for Security Intelligence .....	29
Ministerial Direction .....	30
Governor in Council Regulations and Appointments .....	30
Changes in CSIS Operational Policy .....	30
<b>B. Reporting Requirements</b> .....	31
CSIS Director's Annual Operational Report for 2002–2003 .....	32
Certificate of the Inspector General for 2003 .....	33
Unlawful Conduct .....	34
Section 2(d) Investigations .....	34
Disclosures of Information in the Public or National Interest .....	34
Section 38 Statistics .....	36

<b>C. CSIS Operational Activities</b>	.36
Counter Proliferation	.36
Counter Terrorism	.38
Counter Intelligence	.38
Research, Analysis and Production	.39
Security Screening	.41
CSIS Domestic and Foreign Arrangements	.47
Federal Court Warrants and Warrant Statistics	.49
 <b>Section 3: Inside the Security Intelligence</b>	
<b>Review Committee</b>	.51
Appointment of a New Member	.53
SIRC Staffing and Organization	.53
Research and Review Activities	.53
Security Intelligence Briefings	.54
Additional Committee Activities	.54
Budget and Expenditures	.55
SIRC Request for Increased Funding	.55
Inquiries Under the Access to Information and Privacy Acts	.56
 <b>Appendix A: Acronyms</b>	.57
 <b>Appendix B: SIRC Reports and Studies Since 1984</b>	.61
 <b>Appendix C: Key Findings and Recommendations</b>	.71
Front End Screening Program	.73
CSIS Section 12 Operational Activity Outside Canada	.74
Review of a Counter Intelligence Investigation	.74
Review of a Counter Proliferation Investigation	.74
CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post	.75
Internal Security Breach in a CSIS Regional Office	.75
Review of Foreign Arrangements	.76



## Statement from the Committee

---

Rarely have Canadians had as much cause to be concerned about the balance between rights and security as they had in 2003–2004: the deportation of a Canadian citizen to a country with a questionable human rights record; threats from Al-Qaeda to carry out terrorist acts against Canada; and allegations that Canadian officials exchanged information improperly concerning various individuals with the officials of foreign governments.

Such issues are at the heart of our mandate as members of the Security Intelligence Review Committee (SIRC) as we review the activities of the Canadian Security Intelligence Service (CSIS)—a function SIRC has now fulfilled for 20 years.

In July 1984, the *Canadian Security Intelligence Service Act* was proclaimed, creating CSIS to investigate, analyse and advise the Government of Canada on threats to Canada's national security. At the same time, Parliament put in place a comprehensive system of accountability for the new agency. The centrepiece of that accountability system is the ongoing external independent review of CSIS for which we are responsible.

It is worth recalling the events that led to the passage of this legislation, in circumstances not unlike those of today. Allegations of unlawful or improper behaviour by security intelligence officers of the RCMP prompted the government in 1977 to establish the Commission of Inquiry Concerning Certain Activities of the RCMP, chaired by Mr. Justice David McDonald. The Commission concluded that Canada needed an effective security service to protect itself, but recommended that, given the differences between security intelligence work and police work, the government separate the security intelligence function from the law enforcement function of the RCMP. The creation of CSIS and SIRC was the result.

In the 20 years since, SIRC has played an important role in the evolution of CSIS.

- In 1987, the government established a task force to review concerns raised by SIRC in the Service's early years. The task force's report led to significant changes at CSIS, including the disbandment of CSIS's Counter Subversion Branch.
- At about the same time, in response to more than 2000 complaints made by CSIS employees in 1985–86 and 1986–87 about the official languages practices of the Service, SIRC published a report on staff relations and language issues, *Closing the Gaps*, which had a major impact on how CSIS conducted its internal affairs.
- In 1992, after an extensive review of the 1985 Air India tragedy, the Committee reported that CSIS had not been in a position to predict that the Air India flight was to be the target of a terrorist bomb. SIRC also concluded that CSIS senior management had not provided adequate direction to employees concerning the Service's mandate and role in relation to the RCMP criminal investigation, and that CSIS policies in relation to the collection, retention and erasure of surveillance audiotapes were seriously deficient.
- In the early 1990s, SIRC examined CSIS's handling of the delicate balance between lawful dissent and political violence through studies regarding the Canadian peace movement, native extremism and university campuses. This issue remains pertinent now, as our recent studies on domestic extremism (2001–02) and domestic threats (2002–03) demonstrated.
- In 1994, the Review Committee investigated allegations that, among other things, a CSIS informant had created, funded and built the white-supremacist Heritage Front organization. The investigation required the review of 25 000 pages of documents, and interviews with more than 100 people. In a 200-plus page report to the Solicitor General, SIRC provided extensive detail on CSIS's investigation of the Heritage Front, and concluded that CSIS was correct to investigate the leadership of that extremist organization. Committee members later presented more than 16 hours of testimony on the case before the House of Commons Sub-Committee on National Security.
- In 2001, the Chair and another SIRC member appeared before the Special Senate Committee studying the *Anti-Terrorism Act* to provide their views on this ground-breaking piece of legislation. SIRC will undoubtedly also contribute to the upcoming review of the *Act* that Parliament agreed to.

During our 20 years of existence, many distinguished Canadians have given of their time to serve as members of the Review Committee, from all parts of the country and

from each major national political party. And SIRC has been productive, issuing to date 150 reports and studies, which are listed in Appendix B at the end of this report. It has also received over 3186 complaints in the past 20 years and produced written reports for 118 of these complaint cases.

Review Committee members and staff have endeavoured to contribute to public understanding of the security and intelligence issues facing Canada by testifying before Parliamentary committees, speaking at public events, issuing declassified versions of reports and studies, and producing 20 public Annual Reports.

We believe that our work remains as relevant now as it was two decades ago. In fact, in the heightened post-9/11 security environment of today, Canadians need to be especially vigilant in protecting the democratic rights and freedoms that set our country apart from so many others.

Events of 2003–2004 illustrate just how high a profile national security issues have attained in Canada.

- CSIS is now part of a new Public Safety and Emergency Preparedness portfolio, which integrates activities that secure the safety of Canadians and other activities that protect against and respond to natural disasters and security emergencies. The new portfolio reports to the Deputy Prime Minister.
- The Prime Minister created a new Cabinet Committee on Security, Public Health and Emergencies—chaired by the Deputy Prime Minister—and appointed a National Security Advisor to the Prime Minister in the Privy Council Office.
- The Prime Minister also proposed the creation of a National Security Committee of Parliamentarians, whose members would be sworn-in as Privy Councillors so that they could be briefed on national security issues.
- In April 2004, just after the end of our reporting period, the government issued *Securing an Open Society: Canada's National Security Policy*, which, in the words of the policy, “articulates core national security interests and proposes a framework for addressing threats to Canadians.”
- The government also announced, in January 2004, the creation of the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar. Mr. Justice Dennis O'Connor is inquiring into the actions of Canadian officials in the deportation and detention of Mr. Arar from the United States to Syria, and making recommendations concerning an independent, arm's-length review mechanism for the RCMP's activities with respect to national security.

We expect our work to provide input to the deliberations of the O'Connor Commission. In May 2004 we provided to the Minister of Public Safety and Emergency Preparedness a classified, comprehensive report on the role of CSIS in the Arar case, with the suggestion that the Minister share the report with the Commission of Inquiry. We also anticipate that our 20 years of experience in carrying out comprehensive review of CSIS will assist the Commission in formulating its recommendations regarding a review mechanism for the RCMP's national security activities.

We also note with interest that Mr. Justice O'Connor has appointed the Hon. Ronald G. Atkey *Amicus Curiae* or "Friend of the Court". Mr. Atkey, who served as our first Chairman from 1984 to 1989, is acting as counsel, independent from government, and his mandate is to test government requests for *in camera* hearings on the grounds of national security confidentiality.

It is in this environment that we are carrying out our ongoing work. In our studies this past year, we moved from the fairly intense focus on counter terrorism that marked our efforts for many months after September 11, 2001 to a more balanced review of the broad range of CSIS activities.

Our ability to shift our focus as required to address the concerns of Parliament and the public is an indication of the flexibility wisely built into the *CSIS Act* by its drafters. After 20 years we can say with confidence that the *Act* works well for both SIRC and CSIS. CSIS is a still-evolving—indeed, perpetually evolving—organization adapting necessarily to changes in the global environment, and SIRC must ensure that our evaluative activities evolve at the same pace. It is our intention in the year ahead to maintain our broad-based overview of the Service while preserving for ourselves the flexibility to respond to the sudden events and dislocations that have come to characterize the early years of the 21<sup>st</sup> century.

---

*For half its life, CSIS was led by Ward Elcock, who completed his 10-year term as Director in May of 2004. Members of our Committee met frequently with Mr. Elcock over the past decade, and found him to be a principled and determined advocate for the Service. He left CSIS a stronger and more professional organization than it was at the beginning of his term. We extend to him, and to his successor, our best wishes.*

---

## How SIRC's Report Is Organized

The Security Intelligence Review Committee was created to carry out a number of distinct but complementary functions as set out in the *CSIS Act*. The organization of the 2003–2004 annual report reflects the Review Committee's key findings and functions. Additional information that the Committee believes will provide useful background, historical or technical information is set apart from the main text in shaded insets. These insets are intended to be factual and do not reflect Committee opinions or conclusions.

As with previous annual reports, the format of this report distinguishes between Committee findings, observations and recommendations arising from in-depth reviews or complaint investigations, and more general background material collected to inform Committee Members and assist readers in understanding the broader context in which CSIS's security intelligence work is carried out.

### **Section 1: SIRC Review and Complaints Functions**

This section provides the reader with summaries of the six major reviews SIRC conducted during the period covered by this report. In addition, this section provides information regarding complaints received by the Committee and the conclusions arising from SIRC's investigation into the denial of a security clearance.

### **Section 2: CSIS Accountability Mechanisms**

Section 2 outlines those elements of Canada's security intelligence governance system that impact upon the legal and policy framework in which CSIS and SIRC carry out their respective mandates. This section also summarizes information provided to the Committee by the Service about branch investigations and changes in CSIS operational plans and priorities.

### **Section 3: Inside the Security Intelligence Review Committee**

This section describes the information gathering, outreach and administrative activities of the Review Committee itself, including the appointment of a new Committee Member and SIRC's annual budget and expenditures.



## **Section 1**

---

### **SIRC Review and Complaints Functions**





## SIRC Review and Complaints Functions

### A. Reviews of CSIS Security Intelligence Activities

#### How SIRC Carries Out Its Review Function— An Overview

##### **THE COMMITTEE'S ROLE IN CSIS'S ACCOUNTABILITY STRUCTURE**

In creating SIRC, Parliament through the *CSIS Act* authorized SIRC to review the performance by CSIS of its duties and functions. To meet this legislated requirement, the Committee Members direct staff to undertake a number of research projects each year. These reviews provide a retrospective assessment of specific CSIS activities and investigations.

At the completion of each review, the Committee makes findings and recommendations and then forwards the reviews to CSIS and to the Inspector General. The Committee may also prepare special reports to the Minister on any matter that Committee Members identify as having special importance.

Through this review function, the Committee is able to advise Parliament and the Canadian public on the activities of CSIS and offer evidence as to whether the Service's actions were carried out in accordance with the laws of Canada, Directions from the Minister (formerly the Solicitor General, now the Minister of Public Safety and Emergency Preparedness), and CSIS operational policy.

The Committee is one of several accountability mechanisms designed to review CSIS's performance. The Service is accountable to the Minister of Public Safety and the Office of the Inspector General of CSIS. The Director of CSIS, under the direction of the Minister, is responsible for the control and management of the Service. For its financial administration, CSIS accounts to the government through the Minister of Public Safety and the central agencies of government, and to Parliament through the Office of the Auditor General of Canada. The Service is also accountable to Canada's Information and Privacy Commissioners.

##### **IDENTIFYING SIRC STUDIES—CHOICES AND CHALLENGES**

Each year, the Committee applies the principles of risk management in its selection of CSIS activities that will be the focus of detailed reviews. The Committee takes into consideration such matters as the importance and scope of CSIS investigations, the

## SIRC seeks to examine as broad a spectrum of CSIS's duties and functions as possible.

potential for particular activities to intrude on individual rights and liberties, priorities and concerns for Parliament and the Canadian people, the CSIS Director's report on operational activities, and the importance of producing regular assessments of each of the Service's branches.

Each report is the result of a detailed review of CSIS documents, interviews with Service staff and senior managers, and an assessment of the Service's actions in relation to applicable laws, policies and Ministerial Directions.

The Committee seeks to examine as broad a spectrum of CSIS's duties and functions as is possible with its small team of researchers. Over a period of years, the body of completed research projects has provided the Committee with a comprehensive assessment of the Service's operational activities and has given the Committee Members, Parliament and the public a thorough evaluation of the organization.

In addition to the need to ensure a comprehensive assessment of CSIS, the Committee considers a number of other factors when it approves specific areas for review:

- world events and their impact on threats to the security of Canada;
- trends or concerns identified in previous Committee reports;
- commitments by the Committee to re-examine specific issues or investigations;
- issues identified in the course of the Committee's complaints functions;
- new policy directions or initiatives announced by the Government of Canada; and
- the Committee's statutory duties under the *CSIS Act*.

Taking all these factors into consideration, the Committee identifies a number of specific projects at the beginning of each fiscal year. The research plan remains flexible throughout the year in order to respond in a timely fashion to unforeseen issues and events.

### SIRC REVIEWS IN 2003–2004

In the period following September 11, 2001, SIRC reviews focussed to a significant extent on the Service's Counter Terrorism Branch investigations, particularly investigations into Sunni Islamic extremism, because of the intense and immediate importance of those subjects to Canadians. In 2003–2004, we were able to return to a broader focus in our studies, in keeping with our interest in maintaining an overview of the Service's activities across the spectrum of its responsibilities.

Our studies included reviews of two relatively new areas of CSIS activity—its participation in the Front End Screening Program, which screens refugee claimants in Canada, and its Counter Proliferation Branch, which was created in 2002. Our findings here will provide a baseline for future reviews of these activity areas.

We also looked at the Service's handling of an internal security breach in a CSIS regional office, completing a review we had begun the previous year.

Intelligence from abroad is increasingly important in today's security environment. We examined CSIS section 12 investigative activities outside Canada, and reviewed the activities of a Security Liaison Post abroad. We also conducted our annual review of CSIS foreign arrangements.

We rounded out our review program with a study into a particular CSIS counter intelligence investigation.

## Front End Screening Program

---

### Report # 2003-01

---

#### Background

In our 1997–1998 Annual Report, the Committee expressed concern about the lack of systematic security screening of the large numbers of refugee claimants in Canada. Many enter Canada without adequate documentation and remain here until their claims are determined. We suggested the Service could and should assist Citizenship and Immigration Canada (CIC) to screen these individuals.

In 2001, SIRC reported that the Service and CIC had developed a Front End Screening (FES) Program for refugee claimants in Canada. Under the FES Program, CIC submits refugee applications to the Service during the initial phase of the refugee determination process. This allows CSIS to record identifying data on all claimants, including those who withdraw from the process prior to its completion. Applications go through an initial screening phase, and undergo further analysis if the initial screening raises security concerns.

This report provides the results of the Committee's first review of the FES Program. We also examined the existing Port of Entry Interdiction Program (POEIP), under which CSIS provides timely, verbal advice to CIC in screening persons, including prospective refugee claimants, whom CIC considers to be potentially inadmissible to Canada.

Under the POEIP, prospective refugee claimants may be interviewed before they have been determined eligible to file a claim.<sup>1</sup> Upon receipt of a request from CIC, a CSIS

---

1. According to the *Immigration and Refugee Protection Act* and its predecessor, the *Immigration Act*, a prospective refugee claimant must first be determined eligible to make a refugee claim, before an application may be submitted to the Immigration Refugee Board. Under this provision, a person may be deemed ineligible to make a refugee claim in Canada if there are reasonable grounds to believe that the person is inadmissible to Canada on security grounds.

investigator will review the case and, if sufficient security concerns exist, the investigator will attend a joint CIC/CSIS interview. Joint interviews at Ports of Entry are led by an Immigration Officer, with the Service investigator acting as an advisor.

Following a joint interview, the Service investigator may provide verbal advice to the Immigration Officer to assist CIC's admissibility determination under section 34(1) of the *Immigration and Refugee Protection Act (IRPA)*. It is important to note that, regardless of the advice provided by the Service, only CIC has the authority to determine a person's admissibility to Canada.

For the first year of its existence, the FES Program was carried out in the absence of program-specific operational policy. During this period, security screening analysts and investigators relied on directives from management, existing policies and prior experience with other similar programs such as POEIP that were covered by existing operational policies. In November 2002, the Service introduced a new operational policy governing both the POEIP and the FES Program.

We note that this review was concluded before the December 2003 announcement of the creation of the Canada Border Services Agency (CBSA), which now shares responsibility with CIC for screening visitors, refugee claimants and immigration applicants to Canada.

### **Methodology of the Review**

From November 1, 2001 to March 31, 2003, CSIS received 32 933 requests for screening under the FES Program. In the vast majority of these cases, the Service informed CIC following the screening process that it had no security concerns. We chose to review the 17 cases concluded during this period for which the Service provided advice to CIC by means of an inadmissibility brief, information brief, or incidental letter.<sup>2</sup> For each case, we examined all material used by the Service in support of its advice to CIC.

For the POEIP portion of the review, we examined 109 of the 527 interview reports that regional investigators submitted to CSIS Headquarters between November 1, 2001 and December 31, 2002. Under the POEIP, interview reports serve as a record of the advice CSIS investigators provided verbally to CIC. We also reviewed documentation related to the Service's overall co-operation with CIC.

During this review, we met with officials from the Service and CIC to discuss their respective roles in the POEIP and the FES Program.

---

2. For annual statistics on requests to CSIS for security screening, see Tables in the section on Security Screening. For descriptions of the types of advice provided by CSIS to CIC, refer to text box on page 46.

## Findings of the Committee

### ***The Screening Process***

CSIS processes an average of 7500 security screening cases each week. Under normal operating capacity, the caseload in Security Screening Branch at any given time is approximately 17 000 cases. FES is considered high priority relative to other immigration security screening programs, given the objective of providing advice prior to the refugee claimant's hearing before the Immigration and Refugee Board.

We found that CSIS's advice to CIC under the FES Program was appropriate and sufficiently supported by the information in the possession of the Service. There were no instances of unreasonable delay by the Service in the 17 FES cases reviewed.

The Service complied with the *CSIS Act* and operational policy when providing advice to CIC. There was no evidence that the Service has used the POEIP or FES Program as a pretext for other investigative activities.

The Service uses security profiles during the screening process. We are satisfied that these security profiles do not target individuals based on ethnicity or religion. The profiles allow the Service to identify, and focus its attention on, higher risk cases.

SIRC found the FES Program is an efficient means for the Service to provide timely, systematic security screening advice for all refugee claimants in Canada.

We found that the FES Program is an efficient means to ensure that refugee claimants in Canada are properly screened against the inadmissibility criteria of the *IRPA*. Under the POEIP and the FES Program, the Service provided CIC with valuable advice at key stages of the refugee application process.

### ***The Immigration and Refugee Protection Act: New Protection for Classified Evidence***

During the first year of the Front End Screening Program, the *IRPA* replaced the *Immigration Act*. While the criteria for inadmissibility to Canada essentially remained the same, the *IRPA* introduced a new provision for the protection of classified information in the course of admissibility hearings.

The Committee specifically examined the Service's assistance to CIC in a case involving the use of this new provision. The evidence package the Service drafted for use by CIC was well prepared. It demonstrated a timely, effective use of CSIS information in support of enforcement initiatives.

We continue to believe that subjects of admissibility hearings should be provided with as much information as possible about the government's case against them, to allow them reasonable opportunity to respond. However, this case demonstrates that the new *IRPA* provisions work. This case also demonstrated noteworthy co-operation between CSIS and CIC.

### ***POEIP Reporting***

We found that several of the POEIP reports reviewed did not indicate clearly the nature of the advice provided verbally by the Service to CIC. Consequently, we made the following recommendation which the Service advises it has accepted and implemented:

**We recommend that the Service develop a standard reporting format for POEIP interview reports that will include either a clear record of the advice provided verbally to CIC by CSIS investigators, or document that there was insufficient information for the Service to provide such advice.**

### ***Section 15 FES Interviews<sup>3</sup>***

As we have recommended several times in the past, we believe that verbatim records of the Service's section 15 FES interviews would be invaluable in the event that the contents of these interviews are disputed at a later date. Should the need arise, both the Service and the interviewee could refer to such records and they would enable SIRC to reconstruct more accurately what transpired during an interview.

**The Committee again recommends that the Service create verbatim records of its section 15 interviews.**

The Service, having received this recommendation, chose not to accept it for a number of reasons which have been shared with SIRC and the Minister. The Committee maintains that verbatim records of section 15 interviews would be useful.

### ***Effectiveness of FES***

Although FES is still relatively new, some cases have already gone through both FES and subsequent screening for permanent residence. We found that the FES Program is an efficient means for the Service to provide timely, systematic security screening advice for all refugee claimants in Canada. This is a clear improvement over previous refugee processing procedures which saw numerous refugee claimants residing in Canada for extended periods without having been screened by CSIS.

---

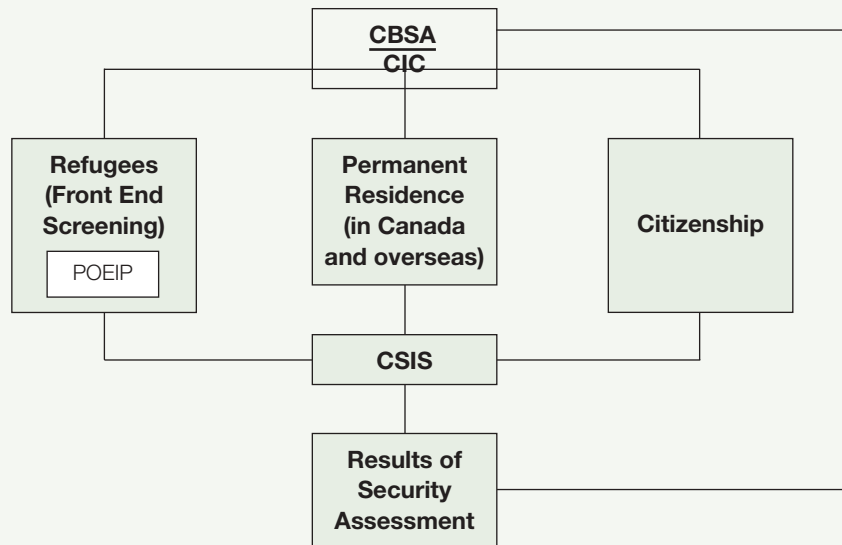
3. Section 15 of the *CSIS Act* authorizes the Service to conduct investigations for the purpose of providing security assessments or advice to Ministers.

While the Service can track the number of inadmissible persons identified by FES, SIRC notes there is no reliable way to determine the number of potentially inadmissible persons the program did not identify. It would be unrealistic to expect the program to identify all inadmissible persons. Information about refugee claimants is usually scarce. In addition, refugee claimants often arrive in Canada without proper identification documents, and the situation in their countries of origin can make confirmation of their identities difficult if verification is sought.

CSIS and SIRC will be in a better position to determine the effectiveness of the FES Program once more refugees who have undergone FES apply for permanent residence and complete the next stage of screening.

### CSIS Advice to CIC and CBSA

This graphic illustrates the role of CSIS in advising Citizenship and Immigration Canada and the Canada Border Services Agency regarding applicants for refugee status, permanent residence and citizenship.



CBSA: Canada Border Services Agency  
 CIC: Citizenship and Immigration Canada  
 POEIP: Port of Entry Interdiction Program  
 (See description on pages 5–6)  
 CSIS: Canadian Security Intelligence Service

## CSIS Section 12 Operational Activity Outside Canada

---

### Report # 2003-02

---

#### Background

Since the terrorist attacks of September 11, 2001, Western countries have reassessed their intelligence agencies' abilities to discover and thwart threats to public safety and national security. This reassessment has included the examination of intelligence gathering capabilities beyond national borders.

CSIS has not been immune to this scrutiny. Some Canadian political leaders and media have called for the creation of a separate Canadian agency authorized to gather foreign intelligence abroad, or have advocated for increased powers to CSIS so that it may undertake investigative activities abroad. However, CSIS has consistently noted that it already has the mandate, and will continue, to conduct operations outside Canada.

Section 12 of the *CSIS Act* allows the Service to collect, analyse and retain information and intelligence respecting activities that may, on reasonable grounds, be suspected of constituting a threat to the security of Canada. The collection of section 12 intelligence has no geographic restrictions. Section 2 of the *Act* allows CSIS to investigate threats to the security of Canada "within or relating to Canada," which includes investigations of threats outside Canada's borders. It is within this context of CSIS operations abroad that this SIRC study was situated.

#### Methodology of the Review

The purpose of our study was to examine CSIS section 12 investigative activity outside Canada. The operational activities selected by the Committee for this review spanned the Service's operational branches and regions as well as investigations. We examined several investigative operations conducted between April 1, 2001 and March 31, 2002.

#### Findings of the Committee

Overall, we found that the operations reviewed were carried out in conformity with the *CSIS Act*, Ministerial Direction, CSIS operational policy and relevant legislation in managing section 12 investigative activities.

The review determined that CSIS has a clear mandate to conduct section 12 investigative activities outside Canada, and concluded that such operations will undoubtedly increase as the threat posed by international terrorism grows. It also identified a few issues which will merit continued interest by the Committee in future reviews, such as the implications of the *Anti-Terrorism Act* and co-operation with domestic partners.



We intend to increase our scrutiny of CSIS's investigative activities abroad to determine for Parliament and Canadians whether the Service is adhering fully to legislative and policy requirements.

This study provided us with an opportunity to examine the Service's role in collecting or receiving information from outside Canada related to the conduct of the international affairs of Canada or the defence of Canada. The Service may accept unsolicited information relevant to other investigations when conducting section 12 investigations abroad. When this occurs, the Service is authorized under section 19 to disclose that intelligence to the appropriate Government department.

The Committee will continue to maintain a watchful eye on CSIS investigative activities outside Canada.

We made two recommendations related to the administrative management of CSIS's investigative activities under section 12 of the *CSIS Act*.

SIRC will increase its scrutiny of CSIS's investigative activities abroad.

**The Committee recommended that the Service's policy for approving investigative activities outside Canada be amended to include certain information.**

**The Committee recommended that the Service amend its operational policy to enhance its administrative rigour.**

The Service has responded that, in its opinion, current policy addresses SIRC's first recommendation and that further to SIRC's second recommendation, the Service intends to propose a policy amendment.

## Collecting, Analysing and Retaining Information on Threats to the Security of Canada

The Service derives its primary authority to collect, analyse and retain information and intelligence from sections 2 and 12 of the CSIS Act. It is an essential feature of almost every study conducted by SIRC to determine whether the Service carried out its duties and functions in accordance with these two sections of the Act. The Service, relying on these two sections, may collect information anywhere in the world.

Section 12 of the Act states:

*“The Service shall collect, by investigation or otherwise to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada.”*

Section 2 of the Act provides four definitions of threats to the security of Canada. None of the definitions includes lawful advocacy, protest or dissent unless carried out in conjunction with the enumerated threats. The four definitions of threats to the security of Canada are:

- (a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage;*
- (b) foreign-influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person;*
- (c) 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, religious or ideological objective within Canada or a foreign state; and*
- (d) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada.*

## Review of a Counter Intelligence Investigation

---

### Report # 2003-03

---

#### Background

This report outlines the results of SIRC's examination of the Service's investigation of the threat-related activities of a foreign intelligence service in Canada. The Service has been monitoring the activities of this particular foreign intelligence service for several years. However, developments raised the profile of the threat posed.

#### Methodology of the Review

This review covered the period from April 1, 1999 to December 31, 2002. To ensure a thorough review, the Committee also examined some documentation that fell outside the review period.

SIRC examined all electronic and hard-copy documentation during the review period, related to the Service's investigation. As in all SIRC reviews of CSIS investigations, the Committee assessed the Service's compliance with the *CSIS Act*, Ministerial Direction and operational policy by examining key operational activities:

- targeting decisions and investigations;
- implementation of warrant powers and special operations;
- management of human sources and sensitive operations;
- co-operation and exchanges of information with domestic partners;
- co-operation and exchanges of information with foreign partners; and
- advice to government.

The Committee sought to ascertain if:

- the Service had reasonable grounds to suspect a threat to the security of Canada;
- the level and intrusiveness of the investigation was proportionate to the seriousness and imminence of the threat; and
- the Service collected only that information strictly necessary to fulfill its mandate to advise the Government of a threat.

#### Findings of the Committee

Throughout the review period, the foreign intelligence service was the subject of a Target Approval and Review Committee authorized Level III investigation for suspected threat-related activities as described in sections 2(a) and 2(b) of the *CSIS Act*.

SIRC concluded that, based on the information in the Service's possession, CSIS had reasonable grounds to suspect that this foreign intelligence service, or its agents, were involved in threat-related activities in Canada. The level and intrusiveness of the

Service's investigation was proportionate to the suspected threat, and the Service collected only that information strictly necessary to fulfill its mandate.

The Service's investigation during the review period was in compliance with the *CSIS Act*, Ministerial Direction and operational policy.

### SIRC concluded that the level and intrusiveness of the Service's investigation was proportionate to the suspected threat.

The human source operations reviewed were well-managed by the Service and complied fully with Ministerial Direction and operational policy.

The Service's co-operation and exchanges of information with domestic and foreign partners complied with the *CSIS Act*, Ministerial

Direction and operational policy. The Service relied heavily on information from foreign partners to develop its advice to client departments.

We noted a small number of administrative errors or omissions in the early operational reporting, which were subsequently corrected by the Service. We found no such problems in recent reporting.

There were no recommendations arising from this review.

## Targeting

CSIS establishes a targeting level to investigate the activities of persons or organizations when it has reasonable grounds to suspect that these activities represent a threat to the security of Canada. The conditions for approval of a targeting level are set out in detail in CSIS operational policy.

The authority to administer the application of the policy, provide direction and review and approve requests for targeting levels rests with the Target Approval and Review Committee. This committee is chaired by the Director of CSIS and includes several senior Service staff, General Counsel and a representative of the Deputy Minister. There are three levels of investigation:

### Level I

- A Level I targeting approval allows for the use of minimally intrusive investigation techniques. Level I investigations are for short durations and allow CSIS to collect information from open sources and from records held by domestic and foreign police, security or intelligence organizations.

**Targeting** *(continued)***Level II**

- A Level II targeting approval allows for the use of moderately intrusive techniques. Level II investigations may include personal interviews and limited physical surveillance.

**Level III**

- A Level III targeting approval allows for the use of the most intrusive investigation techniques available, as outlined in section 21 of the *CSIS Act*. The use of these techniques is subject to the most stringent legal controls and management challenges.

## Review of a Counter Proliferation Investigation

---

**Report # 2003-04**

---

**Background**

The proliferation of weapons of mass destruction (WMD) is a threat to international peace and security. Canada is a party to several international agreements that aim to prevent the proliferation of such weapons and the means to produce and deliver them.

Some foreign states attempt to obtain expertise and technology applicable to WMD and weapons delivery systems from Canada. The Government of Canada has directed CSIS to investigate this threat to Canadian security.

In July 2002, CSIS created the Counter Proliferation Branch, bringing together proliferation-related investigations that the Counter Terrorism and Counter Intelligence Branches had previously carried out. In 2003–2004, SIRC reviewed a CSIS counter proliferation investigation, offering us our first opportunity to examine the Service's counter proliferation activities under the new organizational structure.

For this study, SIRC reviewed the Service's investigation of the threat to Canadian security posed by the activities of one foreign state in support of its WMD programs. CSIS considered the activities of this particular foreign state to fall under the definition of threat-related activities as described in sections 2(a) and 2(b) of the *CSIS Act*.

### Methodology of the Review

At the outset of this review, SIRC examined lists of all CSIS targets, warrants and human sources connected to the Service's investigation. From this material, SIRC selected several files for in-depth review. For each file, we examined all electronic and hard-copy documentation covering the period from April 1, 2002 to March 31, 2003. To ensure a thorough review, we also examined some documentation that fell outside the review period.

As in all reviews of CSIS investigations, SIRC assessed the Service's compliance with the *CSIS Act*, Ministerial Direction and operational policy by examining key operational activities:

- targeting decisions and investigations;
- implementation of warrant powers and special operations;
- management of human sources and sensitive operations;
- co-operation and exchanges of information with domestic partners;
- co-operation and exchanges of information with foreign partners; and
- advice to government.

SIRC sought to ascertain if:

- the Service had reasonable grounds to suspect a threat to the security of Canada;
- the level and intrusiveness of the investigation was proportionate to the seriousness and imminence of the threat; and
- the Service collected only that information strictly necessary to fulfill its mandate to advise the Government of a threat.

### Findings of the Committee

SIRC concluded that, based on the information in the Service's possession, CSIS had reasonable grounds to suspect that each of the authorized targets of investigation posed a threat to the security of Canada. The level and intrusiveness of the Service's investigations were proportionate to the suspected threat and the Service collected only that information strictly necessary to fulfill its mandate.

**SIRC concluded that CSIS had reasonable grounds to suspect a threat to the security of Canada.**

Overall, the Service's investigation during the review period was in compliance with the *CSIS Act*, Ministerial Direction and operational policy.

The Service met all of the requirements of the *CSIS Act* and operational policy with respect to warrant acquisition. SIRC reviewed the Service's application to the Federal Court for warrant powers and found all of the statements in the affidavit to be reasonable

and adequately supported. SIRC found that, in implementing the powers authorized by the warrant, the Service complied with the *CSIS Act*, operational policy and the conditions imposed by the Federal Court. The Service managed human source operations well and complied fully with Ministerial Direction and operational policy.

In this investigation we found no problems or issues of concern with respect to the Service's co-operation with its domestic or foreign partners. Co-operation and exchanges of information with foreign partners were important components of the investigation. Overall, the Service's co-operation and exchanges of information with domestic and foreign partners complied with the *CSIS Act*, Ministerial Direction and operational policy.

We did find one case of non-compliance with operational policy by a CSIS regional office. CSIS has informed SIRC that the regional office has since amended its procedures to prevent similar problems from reoccurring. We also brought to the Service's attention a small number of administrative errors or omissions in operational reporting, which the Service has subsequently corrected.

During this review, SIRC noted references to the Service's activities under its Liaison Awareness Program. Under this program, the Service provides counter proliferation briefings to individuals working or studying in the private sector who might be vulnerable to targeting by foreign entities of proliferation concern. We did not identify any problems or issues of concern with respect to this operational activity.

There were no recommendations arising from this review.

## CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post

---

### Report # 2003-05

---

#### Background

Under sections 13(3) and 17(1) of the *CSIS Act*, the Service may enter into arrangements with foreign states or international organizations of states, or with their institutions. Section 13 arrangements authorize CSIS to provide security assessments, while section 17 arrangements help the Service perform its duties and functions under sections 2 and 12 of the *Act*. Both sets of arrangements specify the scope of activities and exchanges that may take place between the parties.

Our review of a Security Liaison Post addresses SIRC's obligation under section 38(a)(iii) of the *CSIS Act* to review arrangements entered into by the Service pursuant to subsections 13(3) and 17(1), and to monitor the provision of information and

intelligence pursuant to those arrangements. This year, we chose to review a Security Liaison Post that had recently assumed responsibility from another Post for managing section 17 arrangements with the foreign intelligence agencies of several countries.

### **Methodology of the Review**

In reviewing the Post, SIRC sought to determine whether the Post's liaison arrangements and its exchanges of information with foreign agencies were within the scope of the government-approved liaison agreements in place. We also assessed the operations at the Post in relation to the *CSIS Act*, Ministerial Direction, and the Service's operational policies. Finally, we evaluated the security screening support provided to Citizenship and Immigration Canada (CIC) as well as the impact the screening workload had on the other functions of the Security Liaison Officer (SLO).

As has been the case in previous reviews of CSIS foreign liaison activities, we paid particular attention to any information exchanges that had the potential to result in abuses of human rights by other parties.

### **Findings of the Committee**

#### ***Compliance and Effectiveness***

SIRC noted the challenges facing the Post in liaising with the agencies involved, including concerns about the activities of one of the agencies, and weak co-operation

SIRC paid particular attention to any information exchanges that had the potential to result in abuses of human rights by other parties.

on the part of another. Despite these challenges, SIRC's observations, reviews of documentation, and interviews led us to conclude that the Post carried out its operations in accordance with the *CSIS Act*, Ministerial Direction and the Service's operational policies and procedures. We found that the Post had contributed to the

Service's ability to perform its duties and functions under the *CSIS Act*. We also assessed that CSIS had managed the arrangements with these foreign agencies effectively, collecting information in accordance with the applicable section 17 arrangements.

#### ***Human Rights Issues***

SIRC expects the Service to take all possible care to ensure that the information it exchanges with foreign agencies is not used in ways that could result in the violation of human rights. The SLO is responsible for regularly producing assessments of foreign agencies and promptly submitting these to CSIS Headquarters. The agencies are assessed both for their human rights records and their propensity, if any, to pass information on to third parties without authorization.



After reviewing the agency assessments prepared by the SLO, we concluded that the Post's staff were appropriately addressing human rights issues associated with the countries under the Post's purview. The documentation we reviewed indicated that the Service was diligent in ensuring that no information provided to or received from these countries' agencies was associated with human rights abuses.

We noted that the SLO was aware that what a foreign agency perceives as a threat to its security may not be comparable to the *CSIS Act's* definition of a threat to the security of Canada. In one case in which a foreign agency sought information on a political dissident, CSIS refused the agency's request.

### **Security Screening**

One of an SLO's functions is to assist CIC to screen potential immigrants to Canada. If CIC has security concerns about an applicant, it may refer the case to the SLO, who investigates the matter and may interview the applicant.

The security screening demands placed on an SLO vary from Post to Post. In previous reviews of SLO Posts, we have observed that CSIS has on occasion had to deploy staff temporarily from CSIS Headquarters to address backlogs and work volume. During this review, we examined the impact of security screening activity on the balance of the duties and functions of the liaison officer at the Post under review.

The SLO acknowledged that during his first year on the job there was a backlog of security screening files. However, he was able to address the backlog without additional resources.

At the beginning of his term, the SLO asked Headquarters for a list of all outstanding files requiring a security screening interview. We noted that the SLO had implemented an effective tracking system for all outstanding security screening referrals. However, we were concerned that no master list existed at the Post when the current SLO took office.

**The Committee recommended that the Service identify the reasons for the absence of a list and tracking system at the Post and determine whether other Posts would benefit from a uniform standard for managing security screening requests.**

In response to this recommendation, the Service informed SIRC that it had looked into the issue and that it believes that adherence to the tracking systems in place is sufficient to ensure proper record-keeping.

## The Role of Security Liaison Officers

Security Liaison Officers perform the following functions on behalf of the Service when based in foreign Posts:

- maintain and develop channels of communication with foreign agencies with which the Service has approved arrangements;
- carry out security screening activities in support of the Immigration Screening program;
- report to CSIS Headquarters on any matter related to Canadian security interests; and
- undertake specific reliability checks as requested by the Mission Security Officer.

Any operational assistance or investigative activity related to threats to the security of Canada (section 2 of the CSIS Act) that CSIS may undertake outside the country are separate and distinct from the Security Liaison Officer's functions and responsibilities.

## Internal Security Breach in a CSIS Regional Office

### Report # 2002-05

#### Background

In the course of SIRC review #2002-05, summarized in our 2002–2003 Annual Report, CSIS informed us of a security breach within the Service that resulted in an internal investigation by CSIS to determine the nature and scope of the breach. We determined that the matter of the breach deserved to be examined in detail.

#### Methodology of the Review

Our review sought to identify the nature of the breach; the Service's response to the allegations; the damage to CSIS operational programs or investigations and national security; and the adequacy of CSIS policies to address the breach and avoid similar problems in the future. We reviewed Service documentation related to the investigation, and assessed investigative procedures against operational policies in force at the time.

#### Findings of the Committee

We reviewed the documentation related to the internal investigation, and were satisfied with the Service's investigation of the allegations. We concluded that existing CSIS operational policies were adequate for the Service to investigate the breach and address the conduct of the officer in question. We found that the Service had taken appropriate measures to minimize the effect of the breach and had acted in accordance with operational policies governing security breaches and employee conduct.

## Review of Foreign Arrangements

In addition to its reports, SIRC conducted its annual review of foreign arrangements.

### Background

Under section 17 of the *CSIS Act*, the Service may, for the purpose of performing its duties and functions, “enter into an arrangement or otherwise co-operate with” institutions of the government of a foreign country or with an international organization.

An overview of CSIS foreign arrangements can be found in section 2 C of this Annual Report under the heading *CSIS Domestic and Foreign Arrangements*.

All section 17 arrangements require the approval of the Minister of Public Safety and Emergency Preparedness, after consultation with the Minister of Foreign Affairs. Unless a section 17 arrangement is in place, CSIS is not permitted to pass classified information to foreign agencies. It may, however, accept unsolicited information.

Section 38(a)(iii) of the *Act* directs SIRC to review all such arrangements. Our objective is to assess whether they are in compliance with the conditions set out in the *CSIS Act*, Ministerial Direction and CSIS Operational Policy. It is important to note that SIRC reviews new arrangements once they have been approved by the Minister of Public Safety and Emergency Preparedness and the Minister of Foreign Affairs. SIRC’s review of the arrangements does not include any review of exchanges of information; these exchanges are reviewed as part of SIRC’s reviews of the Service’s Security Liaison Posts.

Each year SIRC reviews a selection of these arrangements. During fiscal year 2003–2004, we reviewed 17 arrangements: 14 were new, one was an expansion of an existing arrangement and two were renewed arrangements.

### Methodology of the Review

For each arrangement, we examined:

- all relevant information provided to the Minister by the Service;
- all correspondence relating to consultations with the Minister of Foreign Affairs;
- the co-operation file for the foreign agency in question;
- the most recent assessment of the agency in question, written by the responsible Security Liaison Officer (SLO);
- the SLO’s overseas Post profile; and
- any documentation related to conditions that may have been imposed by the Minister.

**Findings of the Committee**

We found that the establishment of the new arrangements and the expansions of the existing ones were carried out in compliance with the *CSIS Act* and the Minister's conditions for approval as set out in Ministerial Direction.

When approving the establishment of a new foreign arrangement, the Minister may impose conditions or caveats governing the management and potential expansion of the arrangement. Such conditions vary from case to case in order to address matters such as political or social instability in the country in question, or human rights concerns. In the case of two of the arrangements, the Minister had directed the Service to review the arrangements, and the Service complied.

Ministerial Direction requires CSIS to pay particular attention to the human rights record of the country and the agency with which it liaises, and CSIS operational policy reflects this requirement. In conducting our review, we took special care to examine information relevant to the human rights records of the agencies' host countries, including open-source reporting from reputable international human rights agencies.

We found that the Service had informed itself of the human rights situation in all the countries in question and that it proceeded cautiously with activities and exchanges of information involving countries with a questionable human rights record.

We took note of eight new relationships in which SIRC believes the Service will need to exercise vigilance to ensure that no information it receives from an agency is the product of human rights violations, and that no intelligence CSIS transfers to an agency results in abuses. The Committee will review exchanges with these agencies in the future.

As noted, SIRC examines the substance of the information exchanged under foreign arrangements during the course of our regular reviews of individual Security Liaison Posts abroad. The summary of a review of a Post we conducted during 2003–2004 can be found in this section beginning on page 17.

## Policy Direction for Foreign Arrangements

The *CSIS Act* gives CSIS the authority to enter into arrangements with agencies of foreign governments and international organizations. Such arrangements must be approved by the Minister of Public Safety and Emergency Preparedness, after consultation with the Minister of Foreign Affairs.

Ministerial Direction dictates the procedures and conditions necessary to establish a new arrangement or to expand the scope of an existing one, and it gives the Director of CSIS authority to manage existing arrangements subject to any conditions imposed by the Minister.

Ministerial Direction requires that arrangements meet the following criteria:

- arrangements are to be established as required to protect Canada's security;
- arrangements must remain compatible with Canada's foreign policy objectives toward the country or international organization in question;
- the human rights record of the country or agency is to be assessed and the assessment weighed in any decision to enter into a cooperative relationship; and
- arrangements must respect the applicable laws of Canada.

The nature of the relationship between CSIS and a foreign organization is established when CSIS enters into an arrangement, which allows the Service to exchange information or cooperate in specific areas. CSIS may also expand arrangements to include specific exchanges of information or restrict them in certain areas.

## B. Investigations of Complaints

In addition to our review function, SIRC is responsible for investigating complaints from the public about CSIS. Four kinds of complaints may be directed to the Committee for investigation:

- complaints lodged by persons “with respect to any act or thing done by the Service” (section 41);
- complaints received concerning denials of security clearances to government employees or contractors (section 42);
- referrals from the Canadian Human Rights Commission of complaints made to it; and
- Minister's reports in respect of the *Citizenship Act*.

Where appropriate, we investigate complaints through a quasi-judicial hearing presided over by a Member of the Committee.

Through our investigations of complaints, SIRC determines whether the Service's activities have been carried out in accordance with the *CSIS Act*, Ministerial Direction and CSIS policy.

Following a section 41 investigation, we are required, under the *CSIS Act*, to provide the Minister and the Director of CSIS with a report containing the findings of the investigation and any recommendations the Committee considers appropriate. The *Act* also directs SIRC to report to the complainant our findings and, if the Committee considers it appropriate, any recommendations made to the Minister and Director.

Following a section 42 investigation, SIRC provides the Minister, the Director of CSIS, the deputy head of the government agency concerned and the complainant with a report containing any recommendations the Committee considers appropriate, and those findings the Committee considers fit to report to the complainant.

Table 1 provides the status of all complaints directed to SIRC over the past three fiscal years, including complaints that were either misdirected to SIRC, deemed to be outside the Committee's jurisdiction or investigated and resolved without a hearing (administrative review).

Following the table is a summary of the one investigation report issued by the Committee during the past year under section 42 "denial of security clearance". There were no reports last year on complaints made under section 41 ("any act or thing done by the Service"), or complaints referred from the Canadian Human Rights Commission or on Minister's reports.

**Table 1**  
**Resolution of Complaints\***

Description	2001–2002	2002–2003	2003–2004
Carried over	41	17	17
New	45	48	30
<b>Total</b>	<b>86</b>	<b>65</b>	<b>47</b>
Closed	69	48	31
Carried forward to subsequent year	17	17	16

\* Table 1 reflects all complaints received by SIRC. However, not all complaints received require further inquiry by the Committee nor does every complaint result in an investigation. Some are redirected to appropriate governmental bodies or are determined at the outset to be outside the Committee's jurisdiction, while others are investigated and resolved without a hearing.

## Report of Decision

### SECTION 42 DENIAL OF SECURITY CLEARANCE

The Committee reported a decision on one complaint for the period under review under section 42 of the *CSIS Act* respecting a denial of a security clearance. Our summary has been edited to protect the privacy of the complainant and to prevent disclosure of classified information.

The complainant applied for employment with an agency of the federal government, and the agency denied the applicant the required security clearance. The complainant contested the denial of the security clearance by filing a complaint with SIRC.

On the basis of a review of relevant documentation and after hearing the testimony of witnesses, we concluded that the decision of the federal agency in question to deny the security clearance was well-founded. The complainant was seeking a Top Secret security clearance. According to the *Government Security Policy*, a decision to grant a Top Secret security clearance must be based on adequate information, which requires a personal history check covering at least the previous ten years. The complainant had been in Canada for an insufficient period of time and the Service lacked adequate information to make a recommendation.

We determined that the agency demonstrated satisfactorily that the decision to deny the complainant a security clearance was based on reasonable grounds. We recommended that the decision of the responsible Deputy Head to deny the clearance be upheld.

## Complaints About CSIS Activities Under Section 41

Under the provisions of section 41 of the *CSIS Act*, SIRC must investigate complaints made by “any person” with respect to “any act or thing done by the Service.” Before the Review Committee investigates, two conditions must be met:

- 1) The complainant must first have complained to the Director of CSIS and not received a response within a reasonable period of time (about 30 days), or the complainant must be dissatisfied with the Director’s response.
- 2) The Committee must be satisfied that the complaint is not trivial, frivolous, vexatious or made in bad faith. Under section 41(2) of the *Act*, the Committee cannot investigate a complaint that can otherwise be addressed under existing grievance procedures of the *CSIS Act* or the *Public Service Staff Relations Act*.

## Complaints About CSIS Activities Under Section 42

With respect to decisions by federal deputy heads to deny security clearances, section 42 of the *CSIS Act* says the Review Committee shall investigate complaints from:

- 1) any person refused federal employment because of the denial of a security clearance;
- 2) any federal employee who is dismissed, demoted, transferred or denied a transfer or promotion, for the same reason; and
- 3) anyone refused a contract to supply goods or services to the government for the same reason.

A complaint under section 42 of the *Act* must be filed within 30 days of the denial of the security clearance. SIRC can extend this period if valid reasons are presented.

For more information on how to make a complaint to SIRC, please visit our Web site at [www.sirc-csars.gc.ca](http://www.sirc-csars.gc.ca)



## **Section 2**

---

### **CSIS Accountability Mechanisms**



## CSIS Accountability Mechanisms

### A. Policy and Governance Framework

#### 2003–2004 NATIONAL REQUIREMENTS FOR SECURITY INTELLIGENCE

The Minister responsible for CSIS issues annual National Requirements for Security Intelligence to provide general direction to CSIS in its collection, analysis and advisory responsibilities as detailed in the *CSIS Act*. The 2003–2004 National Requirements were issued under the authority of the then Solicitor General of Canada, pursuant to subsection 6(2) of the *CSIS Act*.

The 2003–2004 Requirements acknowledge the current instability in the global security environment and direct CSIS to maintain flexible forewarning capability to address Canada's security intelligence needs with respect to threats to the security of Canada. In regards to counter terrorism, they direct CSIS to investigate threats of serious violence for the purpose of achieving political, religious or ideological objectives; to conduct research in support of the listing of terrorist entities; and to use CSIS intelligence to combat terrorist financing.

The National Requirements indicate that Canada is increasingly concerned with the proliferation of weapons of mass destruction (WMD), attempts to acquire WMD technology or materials, and the potential use of such weapons. To address this concern, CSIS is directed to continue its investigations of foreign governments and terrorist organizations engaged in the development of WMD programs. Through foreign and domestic exchanges of information, CSIS will continue to expand upon and share its knowledge of threats and emerging trends.

Many foreign intelligence services collect information covertly to meet their military, political and economic needs. The Service is directed to investigate and report on such threats as foreign-influenced activities, transnational criminal activity, clandestine or coercive attempts to obtain proprietary information and attempts to access, steal, alter or destroy information or critical infrastructures.

CSIS is further directed to continue to protect Canadian security through its screening program. Through this program, the Service provides advice on immigration and citizenship matters and on the security of specific sites. It also provides assessments of security standards and screening programs to the Government of Canada, nuclear power facilities and some provincial governments.

Finally, the National Requirements direct CSIS to assist the Ministers of Foreign Affairs and National Defence by collecting foreign intelligence in Canada; to continue to upgrade, expand and replace information systems and technical equipment; to prepare comprehensive, neutral intelligence assessments; to foster and enhance domestic and foreign liaison relationships; and to report regularly to the Minister.

### **MINISTERIAL DIRECTION**

Under section 6(2) of the *CSIS Act*, the Minister may issue directions governing CSIS's activities and investigations. The Ministerial Direction on National Requirements for Security Intelligence for 2003–2004 is described in the section above. No other directions were issued in 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 during 2003–2004.

### **CHANGES IN CSIS OPERATIONAL POLICY**

Together with the *CSIS Act* and Ministerial Direction, CSIS operational policy provides parameters and guidelines for the Service's activities and investigations. SIRC examines CSIS activities for their compliance with operational policies, as one way of reviewing the performance of the Service. We therefore track carefully any changes to existing policies or newly introduced policies. Changes in policies also provide us with insight into the evolving environmental factors that affect the Service.

In 2003–2004 we examined seven new operational policies issued by the Service and eight amendments to existing operational policies.

The new policies relate to two essential areas of Service operations: investigation techniques and warrants. Three policies direct CSIS staff on requirements for the collection or reporting of operational information.

Three other policies address the use of warrants in CSIS investigations. The first deals with procedures for acquiring warrants, while the second policy directs CSIS employees on how to execute these warrant powers. The third warrant policy addresses the management of information collected under these warrants.

The seventh and final new policy defines terms used in CSIS policies. This policy provides a quick reference guide and direction for CSIS officers on the meaning of acronyms commonly used by the Service.

The eight amended policies address co-operation with the Canada Customs and Revenue Agency, changes in investigative techniques, reporting of information and immigrant security screening. Other policy amendments reflect changes in the *Anti-Terrorism Act*, the *Immigration and Refugee Protection Act* and the *Security Offences Act*.

Five new policies were under development at the end of the fiscal year 2003–2004. These policies provide direction on the use of investigative techniques and outline procedures for the sharing of information with domestic and foreign agencies.

In our last annual report, we reported that three policies were under development at the end of the 2002–2003 fiscal year. One of these policies has since been implemented, and is included in the new policies described above.

For reasons of national security, we are unable to elaborate further on these additions to Service policy. We have examined them in detail and are satisfied that both the new and the revised policies are designed to enhance CSIS operational effectiveness and that they conform to the *CSIS Act* and Ministerial Direction.

## B. Reporting Requirements

Section 33(1) of the *CSIS Act* requires the Director to submit to the Minister and Inspector General, at least annually, a report on the operational activities of the Service. The Inspector General, after receiving the Director's report, is required to submit to the Minister a certificate explaining the extent to which the Inspector General is satisfied with the report. The Minister is then required to submit the Director's report, and the Inspector General's Certificate, to SIRC.

SIRC is required to review the Director's report and the Inspector General's Certificate under section 38(a)(i) of the *CSIS Act*. Historically, this examination has allowed the Committee to identify potential areas for future research and review. This year's review identified a number of topics of interest to the Committee. These will be included in our research plan for 2004–2005.

We also use the Director's report and the Inspector General's Certificate to make yearly comparisons of CSIS activities and to assess the performance of existing and new programs and sectors.

In this section, we review the Director's report and the Inspector General's Certificate, and note other CSIS reporting requirements.

**CSIS DIRECTOR'S ANNUAL OPERATIONAL REPORT FOR 2002–2003**

The Director's report summarizes the achievements realized and challenges encountered by the Service in the course of fulfilling its operational mandate, and information on each of the Service's key functions.

The 2002–2003 report describes in global and specific terms some of the opportunities and challenges faced by CSIS during that fiscal year.

As a result of legislative amendments by the Canadian government, the Director also reported on increased interdepartmental, domestic and international co-operation as well as new measures to fight terrorism, including the Terrorist Entity Listing process. The Director reported that all of these activities placed increased demands on Service resources.

During the period under review, the Service created the Counter Proliferation (CP) Branch, incorporating elements from two existing branches, in order to improve its efforts to investigate state-sponsored terrorism, as well as the foreign interference and espionage activities of specific foreign governments. The CP Branch also investigates proliferation activities, and contains the Integrated National Security Assessment Centre, created to allow the dissemination of information and intelligence between federal agencies with responsibilities in national security. The Director also reported on the creation of a unit within the Counter Terrorism Branch designed to provide the Government of Canada with intelligence on the nature and extent of a specific terrorist activity in Canada.

The report describes other new initiatives designed to provide timely assessments of specific threats to federal agencies that are involved in national security. These measures aim to prevent threats to national security or disrupt them at the earliest possible stage.

In addition, for each of the Service's branches, the report identifies the focuses of investigation, including specific threats, targets, priorities and operational activities. The report provides details about the Service's human source program, and includes a description of the program's compliance with Ministerial Direction and the National Requirements of the Government of Canada.

The developments cited in the 2002–2003 report—the creation of a new branch, increased domestic and international co-operation, the unrelenting threats from specific terrorist organizations—provide CSIS with continued operational challenges and opportunities. We will continue to monitor closely and assess these matters.

**CERTIFICATE OF THE INSPECTOR GENERAL FOR 2003**

The Inspector General of CSIS reports to the Minister of Public Safety and Emergency Preparedness and functions, in effect, as the Minister's internal auditor of CSIS, reviewing the day-to-day operational activities of the Service and monitoring compliance with policy and the *CSIS Act*.

Each year, the Inspector General (IG) must submit to the Minister a certificate stating the "extent to which the Inspector General is satisfied" with the Director's Annual Report to the Minister on the operational activities of the Service. The certificate must inform the Minister of any failures by CSIS to comply with the *Act* or Ministerial Direction, and of any actions that involved an unreasonable or unnecessary exercise of powers. As per section 33(3) of the *Act*, the Minister forwards the certificate to SIRC for its consideration.

In reviewing the Inspector General's certificate, SIRC noted that the IG followed a methodology consistent with previous years. His review consisted of the inspection of documentation supporting the Director's report to the Minister, an analysis of significant Service operations, and interviews with senior CSIS management at HQ and in the field.

The IG based his conclusions on a validation process that included an inspection of CSIS internal documents and a review of the documentation supporting affidavits for warrant applications, supplemented by the IG's annual program of review activities. For this reporting period, the program included a review of warrant and target samples as well as of human source management, a special study of the Service's domestic liaison arrangements, and briefings on the Front End Screening Program for refugee claimants.

In this year's certificate, the Inspector General stated that in the almost 20 years since the establishment of CSIS, the Service had "evolved from being a rather disorganized organization with significant weaknesses, to a highly professional and effective arm of government." He commended SIRC for contributing to this "maturing process."

With respect to the Director's Annual Report for 2002–2003, the IG declared himself to be "satisfied." He noted that during his review, various issues had been uncovered that required "further discussion," but felt that these issues had been "appropriately dealt with by the Service."

**UNLAWFUL CONDUCT**

Under section 20(2) of the *CSIS Act*, the Director of CSIS must submit a report to the Minister when, in the Director's 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 comments to the Attorney General of Canada and to SIRC.

In 2003–2004, the Service sent no reports of prohibited activity to the Minister. The Attorney General of Canada continues to consider an instance of unlawful conduct that the Committee originally reported in its 2000–2001 Annual Report.

**SECTION 2(d) INVESTIGATIONS**

The Service is authorized to collect, analyse and retain information and intelligence on activities that may be suspected of constituting a threat to the security of Canada. Section 2(d) of the *CSIS Act* defines a threat to include activities directed towards undermining or destroying the system of government in Canada. The Minister of Public Safety and Emergency Preparedness must authorize CSIS investigations of these threats. The Service reported that in 2003–2004, the Minister did not approve any investigations under subsection 2(d).

**DISCLOSURES OF INFORMATION IN THE PUBLIC OR NATIONAL INTEREST**

CSIS may disclose information it has obtained in the performance of its duties and functions only in accordance with the specific conditions set out in section 19 of the *CSIS Act*. Section 19(2)(d) of the *Act* authorizes the Minister to approve disclosures to individuals identified in the section where such a disclosure would be in the public interest and that interest outweighs the resulting invasion of privacy. The Service reported to SIRC that no such disclosures were approved in 2003–2004.



## Disclosure of Information by CSIS

Section 19 of the *CSIS Act* sets out four situations in which the Service may disclose information obtained in the performance of its duties and functions. These situations are defined under section 19(2) as follows:

- Section 19(2)(a) information that may be used in the investigation or prosecution of an alleged contravention of any federal or provincial law may be disclosed to a law enforcement agency having jurisdiction over the matter, the Solicitor General of Canada or the Attorney General of the province in question;
- Section 19(2)(b) information related to the conduct of Canada's external relations may be disclosed to the Minister of Foreign Affairs;
- Section 19(2)(c) information related to the defence of Canada may be disclosed to the Minister of National Defence; and
- Section 19(2)(d) information that, in the opinion of the Minister, is essential to the public interest may be disclosed to any minister of the Crown or employee of the Public Service of Canada. The Director of CSIS must submit a report to SIRC with respect to disclosures related to the public interest.

There have been two disclosures under section 19(2)(d). In 1998–1999, all federal government departments and agencies were asked to facilitate the RCMP Public Complaints Commission (PCC) inquiry into police conduct at an Asia-Pacific Economic Cooperation conference in Vancouver. In 2000–2001, disclosure was made to counsel acting on behalf of a Minister of the Crown.

**SECTION 38 STATISTICS**

Section 38 (a)(vii) of the *CSIS Act* directs SIRC to compile and analyse statistics on the operational activities of the Service. In this regard, CSIS provides data to the Review Committee on source payments during the fiscal year as well as the total number of human sources. Given the highly sensitive nature of these statistics, we are not able to disclose them publicly.

In addition, we compile and analyse other statistics on operational activities arising from the individual studies we undertake each year. In our review this past year of the Front End Screening Program, for example, we compiled statistics on advice CSIS provided to Citizenship and Immigration Canada (a summary of our report appears in Section 1 of this Annual Report).

**C. CSIS Operational Activities**

In addition to carrying out in-depth reviews of selected CSIS operations each year, the Committee requests written and oral briefings from the Service about several activities that are relevant to the Committee's mandate. The information we receive relates to the Service's plans and priorities, especially as they pertain to its main operational branches. Although this information is not independently verified unless it forms part of an in-depth Committee review, it nonetheless helps the Committee to stay apprised of and to monitor the Service's priorities and perspectives, from year to year.

This section of the Annual Report summarizes information the Committee received in written and oral briefings.

**COUNTER PROLIFERATION**

The goal of the CP Branch is to collect information related to the biological, chemical and nuclear weapons development programs of foreign governments. The Branch also investigates state sponsorship of terrorism.

Among CP's most important concerns is the potential threat posed by terrorist organizations that might manage to obtain weapons of mass destruction. Some foreign governments that support terrorist organizations continue to provide these groups with training, arms, money, materials and logistical support. The Service gathers information regarding these activities in order to advise the Government on possible threats to Canada's national security and public safety.

According to the Service, another key challenge has been to remain vigilant throughout significant changes in the international environment, such as the hostilities in Iraq and Libya's December 2003 declaration that it would dismantle its weapons of mass destruction program.

SIRC is always interested in assessing whether CSIS needed to change its priorities to address new operational considerations or unforeseen events. The Service reported that world events such as the ones described above had a definite impact on CP investigations. CSIS reallocated resources and adjusted its collection methods to ensure that it could continue to forewarn the Government of potential threats to national security. The Service also reported that the Branch reorganized itself to provide more focussed investigations of particular threats.

Acknowledging the international nature of the CP threat environment, the Service also reported that it continues to look beyond the borders of Canada to collect information related to Canada's national security interests, as per section 12 of the *CSIS Act*. CSIS reported that a key factor affecting its success abroad is CP's ability to train its personnel appropriately and to expand its relations with foreign agencies in order to exploit joint operational possibilities.

In last year's annual report, we commented that future in-depth reviews would include this new operational Branch. This year SIRC reviewed the Service's investigation of the threat to Canadian security posed by a foreign state's activities in support of its weapons of mass destruction program (see the summary of Report #2003-04 in Section 1 A). We will continue to report findings on the activities of the CP Branch in future annual reports.

Fiscal year 2003–2004 marked the first full year that CSIS's Threat Assessment Unit operated within the CP Branch. Working alongside other CSIS assessment groups, such as the Research, Analysis and Production Branch, the Unit co-operates with and draws upon operational areas at Headquarters, in the regions and at Security Liaison Posts. It provides tactical threat assessments that forewarn Government of Canada departments and agencies of threats to the security of Canada. These assessments can focus on activities of terrorist organizations, threats to diplomatic establishments in Canada and abroad, travel advisories for Canadian diplomats, and other situations affecting Canadian interests both directly and indirectly.

The Unit produced 650 threat assessments during the year. This represents a slight decrease from the 709 assessments produced in 2002–2003. As in the past, we continue to examine threat assessments that are relevant to our in-depth reviews of CSIS operational activities.

**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. Addressing the threat of violence used to support political, religious or ideological objectives continues to be one of the Service's chief priorities. These threats could originate in Canada or abroad.

As in 2001–2002 and 2002–2003, Sunni Islamic extremism remained a major focus of CT's operational activities. Additional challenges surfaced due to international events such as the war in Iraq, but the Service reported that the Branch's priorities remained unchanged during the year.

The Service reported no major structural changes to the Branch in 2003–2004 following the significant reorganization of the previous year. However, to adapt to the evolving threat environment and to better utilize resources, the Branch made some organization improvements.

In 2004–2005, we will review CSIS counter-terrorism investigations as well as the Service's advice to government with regards to terrorist financing. We will present the results of these studies in next year's Annual Report.

**COUNTER INTELLIGENCE**

The Counter Intelligence (CI) Branch investigates threats to national security from the hostile intelligence activities of foreign governments. These activities may include espionage, foreign-influenced activity, transnational crime and threats to Canada's social, political, and economic infrastructure.

The Service reports that foreign intelligence services continue to modify their collection methods in Canada. For example, CSIS has uncovered aggressive targeting of Canadian institutions by a foreign intelligence service, and has acted to counter it.

The CI Branch has to remain abreast of these methods and develop investigative strategies that will permit it to gather its own intelligence in an effective manner. It maintains close liaison with foreign and domestic security and intelligence agencies, and works closely with Canadian government organizations to help them guard against threats from hostile intelligence services.

As in previous years, our review of CSIS operations includes the Service's counter intelligence activities.

## RESEARCH, ANALYSIS AND PRODUCTION

The Service's Research, Analysis and Production (RAP) Branch is responsible for writing intelligence reports on threats to the security of Canada (see Inset on page 40 for a description of RAP reports). These reports provide senior federal decision-makers with policy-neutral assessments on a wide range of security intelligence issues. When appropriate, RAP products are distributed to external clients within the intelligence community.

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 address activities in Canada of the intelligence services of other governments, as well as global issues such as terrorism and transnational criminal activity.

According to the Service, international instability and evolving security concerns have increased demand for RAP assessments. Examples from 2003–2004 include support for the Canadian Forces mission in Afghanistan and reports on current events such as the security implications of SARS. RAP also plays a role in the wider government assessment community as a contributing member of the interdepartmental Intelligence Assessment Committee.

Sections 19 (2)(a) through (c) of the *CSIS Act* authorize the Service to disclose information obtained in the performance of its duties and functions to, respectively, Canadian law enforcement, diplomatic and defence personnel. CSIS makes such disclosures through RAP reports. CSIS advised us that in 2003–2004 RAP issued 1623 Section 19 disclosure reports under these sections, a two-fold increase from 2001–2002. We reported on disclosures under section 19(2)(d) on page 34.

SIRC uses RAP products to obtain context for our reviews of the Service's investigations, to identify the Service's perspective on specific threats, and to enhance our own knowledge of the nature of the analysis and advice CSIS provides the government.

## **RAP Intelligence Products**

Research, Analysis and Production Branch intelligence products originate from a number of sources and are produced either on the recommendation of an analyst; at the direction of a RAP supervisor or manager, or CSIS senior management; or at the request of an operational branch, region, or external client. They are defined as follows:

### **CSIS Study**

An analytical product resulting from extensive in-depth research encompassing all elements relating to a threat to the security in Canada. The intention is to provide a reference document for CSIS operational branches and to share this assessment with some external clients. A study contains an executive summary, is not limited in length, and may or may not be classified.

### **CSIS Report**

A concise analytical product that is the result of thorough research on a current security threat pertaining to the Service mandate. The aim is to explain the nature of the threat in some detail to internal and external readers. A report is usually classified and up to eight pages long.

### **CSIS Intelligence Brief (CIB)**

A concise analytical product designed to provide internal and external clients with an analysis of a current threat or a forthcoming event relating to the Service mandate. A CIB is usually classified and up to three pages in length.

### **Profiler**

Intended to provide well-focussed information on countries, individuals or groups of interest to the Service. The document is essentially a tool for Service investigators and operational analysts. A profiler is usually classified “CSIS Eyes Only” and is not released externally without prior removal of sensitive information and consultation with operational branches. Should not exceed three pages. Some profilers are unclassified but carry the added caveat “For Official Use Only”.

### **Counter Intelligence Note**

Captures a recent change or current development relating to counter-intelligence issues, e.g. the restructuring of the intelligence community of a given country and the impact on Canada. Usually classified “CSIS Eyes Only”.

### Fact Sheet

Designed to provide information about the past and current organizational structure of foreign intelligence and security services. Identifies the collection priorities they may be engaged in or relating to Canada. This product is also used to provide information on specific issues such as organized crime groups and oligarchs, and countries of proliferation concern. Restricted to CSIS employees only.

### Commentary / Perspective

*Perspective*, an open-source document, is produced by qualified analysts in RAP. *Commentary*, written by individuals hired on contract, provides information on a wide range of subjects that may have an influence on the security of Canada. Fundamentally a strategic document with wide domestic and international distribution.

### Special Report

A classified document intended for a very narrow or specific readership and usually the result of an event or an action request by a government department.

## SECURITY SCREENING

Section 13(1) of the *CSIS Act* authorizes the Service to provide security assessments to federal government institutions. The *Act* defines a security assessment in section 2 as “an appraisal of the loyalty to Canada and, so far as it relates thereto, the reliability of an individual.” The Service may also, under sections 13(2) and (3), enter into arrangements to provide assessments to provincial government institutions or police forces, or to foreign governments and international institutions.

Under sections 14 and 15 of the *CSIS Act*, the Service conducts security screening investigations and provides advice to CIC and the CBSA to assist in the processing of refugee and immigration applications. The Service’s advice in these cases is based on the classes of individuals deemed inadmissible under the *IRPA*. The Service also provides security assessments to CIC to assist the screening of citizenship applications pursuant to the *Citizenship Act*.

In this section, we refer to the Service’s median turnaround times for processing screening requests, rather than average (mean) times. We believe this represents more accurately the typical processing times by mitigating the impact of unusually short or lengthy processing times.

**Table 2**  
**Turnaround Times for Security Screening of Refugee Claimants**  
**and Immigration Applicants (2003–2004)**

CSIS Security Screening Programs	Median Turnaround (Days)		
	Non-adverse Advice	Information Briefs	Inadmissible Briefs
Front End Screening of Refugees	31	332	214
Applications for permanent residence within Canada—refugee determination program (EDE / hard copy)	53 (52 / 114)	472	419
Applications for permanent residence within Canada—immigration program (EDE / hard copy)	46 (42 / 133)	454	431
Applications for permanent residence from the USA (hard copy only)	153	557	599
Applications for permanent residence from outside Canada	5	238	106

### Government Security Screening

In 2003–2004, CSIS received a total of 74 835 security clearance and “site access” assessment requests, 4093 of which required field investigations. During the same period the Service issued 21 information briefs and four recommendations for denial of a security clearance.

The Service has reported that the creation of the CBSA has impacted both the Immigration and Government programs of the Security Screening Branch significantly. The Service also reported that, as a result of the changes in the Government in late 2003 and the establishment of the O’Connor Commission, the Security Screening Branch faced increased pressure to expedite the processing of several Level 3 Top Secret security clearance assessments.

### Security Clearances

The Service reported that it received 37 508 requests for new or updated security clearances—down from 51 262 during the previous fiscal year. The year under review, 2003–2004, saw an overall decrease in the median turnaround times for Levels I (Confidential) and II (Secret) assessments and a notable increase in the median turnaround time for Level III (Top Secret) assessments. The median turnaround times for the Service to provide its assessments to government clients can be found in Table 3.



**Table 3**  
**Turnaround Times for Security Screening of Government Clients**

Category	Level	Median Number of Days	
		2002–2003	2003–2004
DND	I (Confidential)	28	20
	II (Secret)	29	18
	III (Top Secret)	47	96
Other Government Departments and Agencies	I (Confidential)	5	7
	II (Secret)	13	11
	III (Top Secret)	51	82

### Site Access

In 2003–2004, the Service received 28 822 requests under the Airport Restricted Access Area Clearance Program. The median turnaround time for the Service’s response to these requests was 14 days.

The Service also received 8505 requests related to “site access.” These included requests from federal government departments and agencies, nuclear power facilities and the Parliamentary Precinct (which includes all facilities controlled by the Parliament of Canada). The median turnaround time for a response to a “site access” request was one day.

### Screening on Behalf of Foreign Agencies

The Service may enter into reciprocal arrangements with foreign agencies to provide security assessments on Canadians and other individuals who have resided in Canada. Under these arrangements the Service does not make recommendations to foreign agencies to deny security clearances, but simply reports its findings concerning the individual(s).

In 2003–2004, the Service conducted 1208 screening checks on behalf of foreign agencies, 48 of which included field investigations. This is down from 1797 screening checks and 177 field investigations during the previous year.

### Security Screening for Refugee and Immigration Applicants

CSIS received 96 477 requests for security screening of immigration and refugee applicants in 2003–2004. The Service provided immigration officials with a total of 221 information briefs and 99 inadmissible briefs—a decrease from the 247 information briefs and 215 inadmissible briefs issued during the previous year.

In 2003–2004 the Service also provided 19 incidental letters and 28 updates to briefs previously issued to CIC. A description of the types of advice CSIS provides to CIC can be found in the inset on page 46.

Security screening of refugee and immigration applicants is carried out under the three main programs listed below. The graphic on page 9 illustrates the flow of information between CIC, the CBSA and CSIS.

**Table 4**  
**Security Screening of Refugee Claimants and Immigration Applicants (2003–2004)**

CSIS Security Screening Programs	Requests Received	Information Briefs	Inadmissible Briefs
Front End Screening of Refugees	22 681	66	26
Applications for permanent residence within Canada (including USA-based applications)	49 553	130	52
Applications for permanent residence from outside Canada	24 243	25	21
<b>Total</b>	<b>96 477</b>	<b>221</b>	<b>99</b>

### Front End Screening of Refugee Claimants

The Front End Screening (FES) Program, implemented by the Government in November 2001, aims to identify potential security concerns with refugee claimants in Canada as early as possible in the refugee determination process. For 2003–2004 the Service reported receiving 22 681 applications under the FES Program. During the same period, the Service provided its advice on 24 424 cases, which included 66 information briefs and 26 inadmissible briefs.

Under the FES Program, the median turnaround time for the Service to issue non-adverse advice was 31 days. Median turnaround times were 332 days for information briefs and 214 days for inadmissible briefs.

SIRC recently completed its first in-depth examination of the Service's role in the FES Program. The findings of this study can be found on pages 7–9 of this report.

**Applications for Permanent Residence from Within Canada**

The Service is responsible for security screening all persons who apply for permanent residence status from within Canada. In 2003–2004 the Service received 44 907 screening requests—28 401 under the immigration program and 16 506 through the refugee determination program. The Service also received 4646 requests to provide screening advice for applications submitted to Canadian Immigration offices in the United States.

The median turnaround times for the Service to provide its advice in these cases varied considerably depending on whether the Service received the request in hard copy (paper application) or via Electronic Data Exchange (EDE).

For the immigration program, the median turnaround time was 42 days for EDE requests and 133 days for hard copy requests. The median turnaround times for the refugee determination program were 52 days for EDE requests and 114 days for hard copy requests. In 2003–2004, all requests from Canadian visa offices in the USA were submitted in hard copy. The median turnaround time for these cases was 153 days.

In 2003–2004 the Service issued 130 information briefs and 52 inadmissible briefs in response to screening requests from within Canada and the United States. The median turnaround times for these cases ranged from 14 to 20 months.

**Applications for Permanent Residence from Outside Canada**

For permanent residence applications that originate outside Canada or the United States, the Service shares responsibility for security screening with immigration officials at Canadian missions abroad. For these cases, CSIS only becomes involved in the process upon receipt of a request from the Immigration Program Manager. This process allows the Service to focus on higher-risk cases.

In 2003–2004 CSIS received 24 243 requests for screening under this program. In addition, the Service's Security Liaison Officers were consulted on 4814 cases. The Service issued 25 information briefs and 21 inadmissible briefs. The median turnaround times were 238 days for information briefs, 106 days for inadmissible briefs and 5 days for non-adverse advice.

### Security Screening for Citizenship Applications

As part of the citizenship application process, CIC forwards electronic trace requests to the Service. The names of citizenship applicants are cross-checked against a security screening Watch List that contains the names of individuals who have come to the attention of CSIS through, *inter alia*, investigations approved by the Target Approval and Review Committee.

In 2003–2004 the Service received 203 356 trace requests for citizenship applicants. The Service provided CIC with 150 information briefs, and in four cases requested deferral of its advice in order to postpone the initiation of action on those cases.

### CSIS Advice to Citizenship and Immigration Canada (CIC)

The Service's security screening assessments are provided as advice to CIC in one of four forms:

- *Notice of Assessment—Checked on the Basis of Information Supplied (NOA—CBIS) / No Reportable Trace (NRT)*: a report given to CIC when the Service has no adverse information on the applicant.
- *Inadmissible Brief*: advice provided when the Service has concluded, based on information available to it, that the applicant meets the inadmissibility criteria outlined in the security provisions of the *IRPA*.
- *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 *IRPA*, 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 the *IRPA* (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*.

## CSIS DOMESTIC AND FOREIGN ARRANGEMENTS

### Domestic Arrangements

Under section 17(1)(a) of the *CSIS Act*, the Service may, with the approval of the Minister, conclude written co-operation arrangements with domestic agencies for the purpose of performing its duties and functions as outlined in section 12 of the *Act*.

In the year under review, CSIS had 16 domestic arrangements in effect with federal government institutions, and 10 with provincial government institutions. During the period under review, the Service did not enter into any new section 17 domestic arrangements, and no agreements were terminated. The Service amended one domestic arrangement with a department of the federal government.

### Relationships with the RCMP

In reviewing the Service's arrangements with domestic liaison partners, we have always paid particular attention to CSIS's relationships with the RCMP. The two organizations need to work closely together to protect the interests of Canada and Canadians, but at the same time they must maintain an appropriate separation between the law enforcement function of the RCMP and CSIS's national security mandate.

For the year under review, the Service recorded 613 exchanges of information (written and oral) originating with the RCMP. The Service, for its part, provided 215 disclosure letters to the RCMP (of which 18 related to Air India), 11 verbal disclosures and 15 advisory letters. A disclosure letter from CSIS to the RCMP allows the Force to use Service information to pursue a criminal investigation. If the RCMP wishes to use CSIS information in a court of law, it must request an advisory letter from the Service.

The Service reported on the secondment arrangements between CSIS and the RCMP. The Service noted that RCMP officers are now in four CSIS regional offices across the country and at Headquarters, whereas one year earlier, RCMP secondees were located in only three CSIS regional offices. The goal of this program, under which RCMP officers are seconded to CSIS, is to foster closer co-operation between CSIS and the RCMP.

The Service also reported to the Committee on the Integrated National Security Enforcement Teams (INSETs). The program, now in its third year, is still evolving. The Service expects that, over the long term, the program will enhance the relationship between the two organizations. It has already noticed improved understanding and appreciation in each organization of the strengths and challenges in the other, and greater dialogue on matters of mutual interest.

The Service reported that other initiatives are also facilitating liaison and co-operation with the RCMP. For example, the Joint Management Team, a management-level committee that meets several times a year, allows CSIS and RCMP employees at Headquarters to discuss informally topics of concern to both organizations. Similarly, RCMP representatives are among members of the Canadian security and intelligence community who attend the quarterly meetings of CSIS's new Threat Assessment Working Group.

The Service stated that it has placed considerable emphasis on nurturing relationships with the RCMP at both the working and management levels. The two organizations have worked together to address challenges, such as their divergent approaches to investigations, and CSIS indicates they have collaborated successfully in a number of investigations.

SIRC examines the substance of the information exchanged with the RCMP and the nature of co-operation between the two organizations during the course of regular reviews of regional offices and CSIS investigations. During the past year, we looked at the Service's relationship with the RCMP as part of our studies of Counter Proliferation and Counter Intelligence investigations, summaries of which can be found in Section 1 A of this report.

### **Foreign Arrangements**

Section 17(1)(b) of the *CSIS Act* allows the Service to enter into arrangements with the government or institutions of a foreign state or international organizations for the purpose of performing its duties and functions. An arrangement with a foreign agency enables CSIS to exchange information of mutual interest in relation to events or threats, provide or request assistance and discuss best practices.

At the end of fiscal year 2003–2004, the Service reported that it had 247 foreign arrangements in 140 countries. During that year, the Minister approved the establishment of 13 new liaison arrangements. CSIS also modified arrangements with five other agencies.

During the last fiscal year, 43 arrangements were regarded as dormant (dormancy is defined as no liaison contact for at least one year). The Service maintained restrictions on exchanges of information in the case of five of the 43 dormant arrangements due to concerns either about the agencies' human rights records, violations of the rule against transferring information to a third party, or their overall lack of reliability.

At the end of the fiscal year, CSIS had submitted requests for three proposed new arrangements to the Minister, and these were under consideration. Four additional arrangements were at the initial consultation stage with Foreign Affairs Canada.

As part of its foreign liaison program, the Service maintains liaison Posts abroad, normally co-located with Canadian diplomatic missions. CSIS opened a new Post during 2003–2004. The Service reported that the most significant challenge to the foreign liaison program, as in recent years, was the ever-increasing workload arising from its program of assistance to Citizenship and Immigration Canada.

SIRC conducted a review of a CSIS Security Liaison Post in 2003–2004, a summary of which can be found in Section 1 A (Report #2003-05). We will continue to examine security liaison Posts in 2004–2005.

### **FEDERAL COURT WARRANTS AND WARRANT STATISTICS**

Warrants are one of the most powerful and intrusive tools available to departments or agencies of the Government of Canada. They provide an organization with Court authorization to use investigative techniques, such as the monitoring of telephone communications, that would otherwise be illegal. For this reason alone, the use of warrants by CSIS bears continued scrutiny—a task that SIRC takes very seriously. In the course of our in-depth reviews of CSIS investigations, individual warrants are generally the subject of detailed examination.

Each year, we ask CSIS to provide statistics about CSIS warrant applications (the information CSIS provides the Court in seeking a warrant) and about warrants granted by the Federal Court. Table 5 compares the number of warrants issued in each of the last three fiscal years.

**Table 5**  
**New and Replaced/Renewed Warrants**

	2001–2002	2002–2003	2003–2004
New warrants	111	52	68
Replaced/renewed warrants	155	150	130
<b>Total</b>	<b>266</b>	<b>202</b>	<b>198</b>

According to the Service, the Federal Court issued 30 urgent warrants during 2003–2004 compared to 25 in the previous year. Although no applications for warrants were denied by the Court, CSIS reported seven instances where the presiding Federal Court Judge requested amendments prior to issuing the warrant.

The Federal Court did not impose any new conditions or revise any existing conditions on future warrants during the last fiscal year. The Service also reported that in 2003–2004 no judicial decisions affected its applications for warrants, the execution of powers contained in warrants, or the warrant process generally.

### **Warrant Statistics in Perspective**

The information collected by the Committee can provide insight into how often the Service seeks warrant powers from the Federal Court in a given year. However, any year-to-year comparison of these numbers must take into consideration a number of factors affecting the application for or renewal of warrants. Such factors as court decisions and new developments in technology can introduce significant variations in how often CSIS applies for warrant powers and how warrants are implemented. In addition, a single warrant can authorize the use of warrant powers against one person, several people or an organization.

Considered in isolation, therefore, warrant numbers are not a definitive indicator of the level of Service investigative activity. It is also important to note that CSIS has access to other investigative instruments, including physical surveillance and the use of human sources.



## **Section 3**

---

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



## Inside the Security Intelligence Review Committee

### APPOINTMENT OF A NEW MEMBER

In November 2003, the Governor in Council appointed the Honourable Roy Romanow, P.C., O.C., Q.C., as a Member of the Committee for a five-year term. Mr. Romanow was first elected to the Saskatchewan Legislature in 1967 and served as Deputy Premier from 1971 to 1982. He was acclaimed Leader of the Saskatchewan New Democratic Party in 1987, and became Premier of Saskatchewan following the October 1991 election. Mr. Romanow retired from politics as Premier in February 2001. He is currently a Senior Fellow in Public Policy at the universities of Saskatchewan and Regina and is also a visiting Fellow in the School of Policy Studies at Queen's University.

In June 2004, following the end of the 2003–2004 fiscal year, the Honourable Raymond Speaker, P.C., O.C., completed his five-year term on the Review Committee.

### SIRC STAFFING AND ORGANIZATION

As of March 31, 2004 the Committee had a staff of 14, comprising an Executive Director, Deputy Executive Director, Senior Counsel, Senior Paralegal (who also serves as Access to Information and Privacy Officer/Analyst), Research Manager, two Senior Research Advisors, one Senior Research Analyst, two Research Analysts, a Finance/Office Manager and three administrative support staff. The Senior Paralegal serves as Committee registrar for hearings.

Members of the Committee identify the research and other activities they wish to pursue and set priorities for staff accordingly. Management of the day-to-day operations of SIRC is delegated to the Executive Director with direction, as required, from the Committee Chair in her role as Chief Executive Officer.

### RESEARCH AND REVIEW ACTIVITIES

For each fiscal year, the Committee selects a number of CSIS investigations and areas of responsibility for detailed review. These selections may be supplemented during the year with additional priority projects identified by the Committee. SIRC researchers and analysts conduct the in-depth reviews of the selected areas, with direction from senior management and regular reporting to the Committee. Staff divide their time between SIRC's premises and fully equipped office space provided for the Committee's exclusive use at CSIS Headquarters.

**SECURITY INTELLIGENCE BRIEFINGS**

The Chair and Committee Members participate in regular discussions with staff from CSIS and with other senior officials within the security intelligence community. These exchanges are supplemented by discussions with academics, security and intelligence experts and relevant non-governmental organizations such as human rights groups in order to enrich the Committee's knowledge of a range of issues and opinions affecting the security and intelligence field. The Committee also schedules some of its regular meetings in different regions of Canada so that the Members can meet with CSIS regional office staff and receive briefings on local issues, challenges, priorities and perspectives.

**ADDITIONAL COMMITTEE ACTIVITIES**

Each year, Committee Members and senior SIRC staff meet with representatives of the security intelligence community, including those from other countries, academia and non-governmental organizations to make presentations and exchange views.

In May 2003, the Chair, Committee Members and Executive Director discussed issues of common concern with their counterparts in Oslo, Norway and London, England.

In September 2003, the Executive Director gave a presentation to representatives from the U.S. National Committee on Terrorist Attacks.

The Chair and Committee members, together with the Executive Director, Deputy Executive Director and Senior Counsel, hosted the Swedish Defence Intelligence Commission in October 2003. That same month, the Executive Director and several SIRC staff attended the annual conference of the Canadian Association of Security and Intelligence Studies in Vancouver.

In October 2003 and again in March 2004, the Executive Director was a guest lecturer at Carleton University on the role of SIRC in the review of CSIS's activities, and in the investigation of complaints.

In November 2003, several SIRC staff attended the Canadian Centre of Intelligence and Security Studies (CCISS) Conference in Ottawa. The Executive Director sits on the Board of the CCISS.

In November 2003, the Chair was a guest lecturer at the Collège Militaire in Saint-Jean-sur-Richelieu, Quebec.

In December 2003, the Executive Director and senior staff received a delegation from the Comité permanent de contrôle des services de renseignements of Belgium.

In March 2004, officials from the United Kingdom's Intelligence and Security Committee met with the Executive Director and Deputy Executive Director.

The SIRC Chair gave a speech to the Peace and International Security Program at Laval University in Quebec City in March, 2004.

In late March 2004, the Executive Director attended a conference in Berlin entitled "Secrecy and Transparency: The Democratic Control of Intelligence Services in International Perspective".

### **BUDGET AND EXPENDITURES**

In fiscal year 2003–2004, the Committee once again managed its activities within approved resource levels. The chief expenses were for salaries and benefits as well as for travel within Canada for the Committee's hearings, briefings and review activities. This year's travel expenditures included the Committee Members' meetings in both Norway and the United Kingdom with oversight bodies for the security and intelligence organizations in those countries.

**Table 6**  
**SIRC Expenditures**

	<b>2003–2004</b> (Actual \$)	<b>2004–2005</b> (\$ Estimates)
Personnel	1 336 821	1 795 520
Goods and Services	751 627	1 019 000
<b>Total</b>	<b>2 088 448</b>	<b>2 814 520</b>

### **SIRC REQUEST FOR INCREASED FUNDING**

In the Committee's annual reports for both 2001–2002 and 2002–2003, we noted that the Government had increased the budget of CSIS by 30 percent. The direct result of this increase was a sizeable increase in the Service's investigative activity, which SIRC is legally required to monitor and review.

SIRC reviewed the impact of the expansion of CSIS on the Committee’s resources and on the Committee’s ability to meet its obligations to Parliament and the people of Canada. Following this review, the Committee made a formal request to Treasury Board for a resource increase of 16 percent. Treasury Board approved the increase in December 2003, to be effective April 1, 2004. This provides SIRC with new financial resources commensurate with the Service’s expansion in investigative activity. With the new funding we will expand our review and monitoring activities in the new fiscal year.

**INQUIRIES UNDER THE ACCESS TO INFORMATION AND  
PRIVACY ACTS**

SIRC receives requests for information under both the *Access to Information Act* and the *Privacy Act*. Table 7 indicates the number of requests we have received under each of these acts for the past three fiscal years.

The Committee receives numerous Access to Information requests for each of its studies. The work required to prepare a report for public release need only be done once, but this benefits all who request the report. The Committee therefore waives the application fees for all requests for access to its studies.

**Table 7**  
**Requests for Release of Material**

Year	<i>Access to Information Act</i>	<i>Privacy Act</i>
2001–2002	22	4
2002–2003	20	4
2003–2004	31	1

## **Appendix A**

---

### **Acronyms**





## Acronyms

ARAACP	Airport Restricted Area Access Clearance Program
CBSA	Canada Border Services Agency
CBIS	Checked on Basis of Information Supplied
CCRA	Canada Customs and Revenue Agency
CI	Counter Intelligence
CIB	CSIS Intelligence Brief
CIC	Citizenship and Immigration Canada
CP	Counter Proliferation
CSIS	Canadian Security Intelligence Service
CT	Counter Terrorism
DND	Department of National Defence
EDE	Electronic Data Exchange
FES	Front End Screening
HQ	CSIS Headquarters, Ottawa
IAC	Intelligence Assessment Committee
IG	Inspector General
IRPA	<i>Immigration and Refugee Protection Act</i>
INSETs	Integrated National Security Enforcement Teams
NOA	Notice of Assessment

NRT	“no reportable trace”
PCC	RCMP Public Complaints Commission
POEIP	Port of Entry Interdiction Program
RAP	Research, Analysis and Production
RCMP	Royal Canadian Mounted Police
SIRC	Security Intelligence Review Committee
SLO	Security Liaison Officer
WMD	Weapons of Mass Destruction

## **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 and 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 and 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 and 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 and 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)
134. *CSIS Investigation of Sunni Islamic Extremism* (TOP SECRET) (SIRC 2002-01)
135. *Source Recruitment* (TOP SECRET) (SIRC 2001-01)
136. *Collection of Foreign Intelligence* (TOP SECRET) (SIRC 2001-05)
137. *Domestic Extremism* (TOP SECRET) (SIRC 2001-03)
138. *CSIS Liaison with Foreign Agencies: Audit of an SLO Post* (TOP SECRET) (SIRC 2001-04)
139. *Warrant Review* (TOP SECRET) (SIRC 2001-06)
140. *Special Report following allegations pertaining to an individual* (TOP SECRET)\*
141. *Audit of Section 16 and Foreign Intelligence Reports* (TOP SECRET) (SIRC 2002-02)
142. *Review of the Ahmed Ressam Investigation* (TOP SECRET) (SIRC 2002-03)
143. *Lawful Advocacy, Protest and Dissent Versus Serious Violence Associated with the Anti-Globalization Movement* (TOP SECRET) (SIRC 2002-04)
144. *Regional Audit* (TOP SECRET) (SIRC 2002-05)
145. *Special Report (2002–2003) following allegations pertaining to an individual* (TOP SECRET)\*
146. *Front End Screening Program* (TOP SECRET) (SIRC 2003-01)
147. *CSIS Section 12 Operational Activity Outside Canada* (TOP SECRET) (SIRC 2003-02)
148. *Review of a Counter Intelligence Investigation* (TOP SECRET) (SIRC 2003-03)
149. *Review of a Counter Proliferation Investigation* (TOP SECRET) (SIRC 2003-04)
150. *CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post* (TOP SECRET) (SIRC 2003-05)

## **Appendix C**

---

### **Key Findings and Recommendations**



## Key Findings and Recommendations

### FRONT END SCREENING PROGRAM

This report provides the results of the Committee's first review of the FES Program for refugee claimants in Canada. We also examined the existing Port of Entry Interdiction Program (POEIP), under which CSIS provides timely, verbal advice to CIC in screening persons, including prospective refugee claimants, whom CIC considers to be potentially inadmissible to Canada.

We found that the Service's advice to CIC under the FES Program was appropriate and sufficiently supported by the information in the possession of the Service. The Service complied with the *CSIS Act* and operational policy when providing advice to CIC. There was no evidence that the Service has used the POEIP or FES Program as a pretext for other investigative activities.

The Service uses security profiles during the screening process. We are satisfied that these security profiles do not target individuals based on ethnicity or religion.

We found that the FES Program is an efficient means to ensure that refugee claimants in Canada are properly screened against the inadmissibility criteria of the *Immigration and Refugee Protection Act*. Under the POEIP and the FES Program, the Service provided CIC with valuable advice at key stages of the refugee application process.

We found that several of the POEIP reports reviewed did not indicate clearly the nature of the advice provided verbally by the Service to CIC.

**We recommend that the Service develop a standard reporting format for POEIP interview reports that will include either a clear record of the advice provided verbally to CIC by CSIS investigators, or document that there was insufficient information for the Service to provide such advice.**

As we have recommended several times in the past, we believe that verbatim records of the Service's section 15 FES interviews would be invaluable in the event that the contents of these interviews are disputed at a later date.

**The Committee again recommends that the Service create verbatim records of its section 15 interviews.**

**CSIS SECTION 12 OPERATIONAL ACTIVITY OUTSIDE CANADA**

Overall, we found that the operations reviewed were carried out in conformity with the *CSIS Act*, Ministerial Direction, CSIS operational policy and relevant legislation in managing section 12 investigative activities.

The review determined that CSIS has a clear mandate to conduct section 12 investigative activities outside Canada, and concluded that such operations will undoubtedly increase as the threat posed by international terrorism grows.

We made two recommendations related to the administrative management of CSIS's investigative activities under section 12 of the *CSIS Act*.

**The Committee recommended that the Service's policy for approving investigative activities outside Canada be amended to include certain information.**

**The Committee recommended that the Service amend its operational policy to enhance its administrative rigour.**

**REVIEW OF A COUNTER INTELLIGENCE INVESTIGATION**

SIRC concluded that, based on the information in the Service's possession, CSIS had reasonable grounds to suspect that this foreign intelligence service, or its agents, were involved in threat-related activities in Canada. The level and intrusiveness of the Service's investigation was proportionate to the suspected threat, and the Service collected only that information strictly necessary to fulfill its mandate.

The Service's investigation during the review period was in compliance with the *CSIS Act*, Ministerial Direction and operational policy. The human source operations reviewed were well-managed by the Service and complied fully with Ministerial Direction and operational policy.

The Service's cooperation and exchanges of information with domestic and foreign partners complied with the *CSIS Act*, Ministerial Direction and operational policy.

**REVIEW OF A COUNTER PROLIFERATION INVESTIGATION**

SIRC concluded that, based on the information in the Service's possession, CSIS had reasonable grounds to suspect that each of the authorized targets of investigation posed a threat to the security of Canada. The level and intrusiveness of the Service's investigations was proportionate to the suspected threat, and the Service collected only that information strictly necessary to fulfill its mandate.



The Service met all of the requirements of the *CSIS Act* and operational policy with respect to warrant acquisition. SIRC reviewed the Service's application to the Federal Court for warrant powers and found all of the statements in the affidavit to be reasonable and adequately supported. SIRC found that, in implementing the powers authorized by the warrant, the Service complied with the *CSIS Act*, operational policy and the conditions imposed by the Federal Court. The Service managed human source operations well and complied fully with Ministerial Direction and operational policy.

We did find one case of non-compliance with operational policy by a CSIS regional office. We also brought to the Service's attention a small number of administrative errors or omissions in operational reporting.

### **CSIS LIAISON WITH FOREIGN AGENCIES: REVIEW OF A SECURITY LIAISON POST**

SIRC's observations, reviews of documentation and interviews led us to conclude that the Post carried out its operations in accordance with the *CSIS Act*, Ministerial Direction and the Service's operational policies and procedures. We found that the Post had contributed to the Service's ability to perform its duties and functions under the *CSIS Act*. We also assessed that CSIS had managed the arrangements with these foreign agencies effectively, collecting information in accordance with the applicable section 17 arrangements.

We concluded that the Post's staff were appropriately addressing human rights issues associated with the countries under the Post's purview. The documentation we reviewed indicated that the Service was diligent in ensuring that no information provided to or received from these countries' agencies was associated with human rights abuses.

We noted that the Security Liaison Officer (SLO) had implemented an effective tracking system for all outstanding security screening referrals. However, we were concerned that no master list existed at the Post when the current SLO took office.

**The Committee recommended that the Service identify the reasons for the absence of a list and tracking system at the Post and determine whether other Posts would benefit from a uniform standard for managing security screening requests.**

### **INTERNAL SECURITY BREACH IN A CSIS REGIONAL OFFICE**

In the course of SIRC review #2002-05, summarized in our 2002–2003 Annual Report, CSIS informed us of a security breach within the Service that resulted in an internal investigation by CSIS to determine the nature and scope of the breach.

We reviewed the documentation related to the internal investigation, and were satisfied with the Service's investigation of the allegations. We concluded that existing CSIS operational policies were adequate for the Service to investigate the breach and address the conduct of the officer in question. We found that the Service had taken appropriate measures to minimize the effect of the breach and had acted in accordance with operational policies governing security breaches and employee conduct.

#### **REVIEW OF FOREIGN ARRANGEMENTS**

We found that the establishment of the new arrangements and the expansions of the existing ones were carried out in compliance with the *CSIS Act* and the Minister's conditions for approval as set out in Ministerial Direction.

We found that the Service had informed itself of the human rights situation in all the countries in question and that it proceeded cautiously with activities and exchanges of information involving countries with a questionable human rights record.