



SECURITY INTELLIGENCE
REVIEW COMMITTEE

SIRC Annual Report 2004–2005

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

Website: <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 2005

Cat. No. PS105-2005

ISBN 0-662-69304-3



SECURITY INTELLIGENCE
REVIEW COMMITTEE

SIRC Annual Report 2004–2005

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

Canada

September 30, 2005

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 2004–2005, for your submission to Parliament.

Yours sincerely,



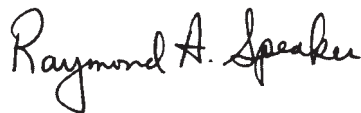
Gary Filmon, P.C., O.M.
Chair



Baljit S. Chadha, P.C.



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



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



M^{me} Aldéa Landry, P.C., Q.C.

Contents

Statement from the Committee	vii
About this Report	ix
How this Report is Organized	ix
Identifying SIRC Studies: Choices and Challenges	x
Section 1: A Year in Review 2004–2005	1
A. Reviews of CSIS Security Intelligence Activities	3
Overview: How SIRC Carries Out its Review Function	3
The Committee's Role in CSIS's Accountability Structure	3
SIRC Reviews in 2004–2005	4
Review of the Terrorist Entity Listing Process	4
Review of CSIS's Investigation of Transnational Criminal Activity	10
Review of a Counter-Terrorism Investigation	14
Review of Activities and Investigations in a CSIS Regional Office	17
Review of a Counter-Proliferation Investigation	20
Review of CSIS's Information Operations Centre	21
Review of CSIS's Exchanges of Information with Close Allies	23
Review of a Counter-Intelligence Investigation	26
Terrorist Financing Activities in Canada	28
CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post ..	31
Review of Foreign Arrangements	33
B. Investigation of Complaints	36
Reports of Decisions: Case Histories	38
Human Rights Complaint Referral	38
Report: Section 41 ("Any Act or Thing")	39
Report: Section 42 (Denial of Security Clearance)	39
C. Section 54 Report to the Minister of Public Safety and Emergency Preparedness	41
Section 2: CSIS Accountability Mechanisms	43
A. Reporting Requirements	45
Certificate of the Inspector General for 2004	45

CSIS Director's Annual Operational Report 2003–2004	46
Unlawful Conduct by CSIS	49
Section 2(d) Investigations	49
Disclosures of Information in the Public or National Interest	49
B. Policy and Governance Framework	50
Annual National Requirements for Security Intelligence	50
Ministerial Direction	53
Governor-in-Council Regulations and Appointments	53
Changes in CSIS Operational Policy	53
C. CSIS Operational Activities	54
Counter Proliferation	54
Counter Terrorism	55
Counter Intelligence	56
Research, Analysis and Production (RAP) Branch	56
Security Screening	58
CSIS Domestic Arrangements	66
Federal Court Warrants and Warrant Statistics	67
Section 3: Want to Know More? An Overview of SIRC	71
Committee Membership	73
Staffing and Organization	73
Research and Review Activities	73
Security Intelligence Briefings	74
Additional Committee Activities	74
Budget and Expenditures	75
Inquiries Under the Access to Information and Privacy Acts	76
Modern Comptrollership	76
Appendix A: Acronyms	77
Appendix B: SIRC Reports and Studies Since 1984	81
Appendix C: Key Findings and Recommendations	93
Review of the Terrorist Entity Listing Process	95
Review of CSIS's Investigation of Transnational Criminal Activity	95
Review of a Counter-Terrorism Investigation	96
Review of Activities and Investigations in a CSIS Regional Office	96
Review of a Counter-Proliferation Investigation	97
Review of CSIS's Information Operations Centre	97
Review of CSIS's Exchanges of Information with Close Allies	98
Review of a Counter-Intelligence Investigation	99
Terrorist Financing Activities in Canada	100
CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post	100
Review of Foreign Arrangements	101

Statement from the Committee

Twenty Years After the Establishment of the *CSIS Act*, Security Intelligence in Canada Faces New Challenges

Twenty years have passed since both the Security Intelligence Review Committee (SIRC) and the Canadian Security Intelligence Service (CSIS) came into being. Looking back over the span of those two decades, it would be an understatement to say that much has changed in the domain of national and global security. Yet what cannot be overstated is how much of that change has taken place just within the last five years. In Canada and around the world, many security intelligence services have had to evolve quickly from being primarily counter-intelligence organizations into ones whose main focus is combatting terrorism domestically and abroad.

The pace of this evolution gained momentum in 2001, immediately following the September 11th terrorist attacks, as Canadians saw the emergence of new measures in the form of the *Anti-Terrorism Act*. Today, information gathering and assessment activities are spread out among a number of federal organizations, with the result that the security intelligence environment is both more complex and more integrated. This has important ramifications for citizens and for policy-makers—after all, SIRC's raison d'être has been to provide a balance against the potent, intrusive powers conferred upon CSIS by the *CSIS Act*. Similar powers are now being exercised by other public bodies, some without the same level of scrutiny that SIRC imposes on CSIS.

SIRC applauds the government's commitment to achieve an effective integration of its operational intelligence apparatus. SIRC also endorses the logical next step, which is a comprehensive and more integrated review of that apparatus. As do many Canadians, we look forward to the findings of Mr. Justice Dennis O'Connor, whose policy review is charged with making recommendations for a review mechanism for the RCMP's national security activities.

The *Anti-Terrorism Act* not only supports Canada's domestic efforts to combat terrorism, but also has an important international dimension—that of harmonizing Canada's anti-terrorism laws with those of its global partners. It is this dimension that has broadened the limits of CSIS's intelligence collection efforts and has tested SIRC's ability to conduct a complete review of the Service's activities.

Indeed, for the first time in many years, SIRC finds itself in the unhappy position of not being able to review comprehensively certain activities by the Service—responsibilities that have been conferred on CSIS by the *Criminal Code*, as amended by the *Anti-Terrorism Act* (this issue is explored at length in this annual report on page 4). Although these activities represent a relatively small slice of CSIS's work, they have significant potential to affect individuals negatively.

To be clear, this is a matter not of CSIS's making. Nevertheless, this Committee believes it is of paramount importance that all of CSIS's activities, including any extension thereof, be subject to independent scrutiny. After all, the *CSIS Act* was passed by Parliament so that the Service's significant powers would be clearly defined and kept in check.

We believe it is important, therefore, that Parliament ensure that the laws governing review keep pace with legislative initiatives in support of intelligence capacity. Such vigilance will help avoid creating a vacuum in the area of security intelligence review.

Indeed, much has changed since 1984, but the framework that defines the powers and authority of both CSIS and SIRC is one that has stood the test of time. The past twenty years have seen both SIRC and CSIS evolve to meet the challenges of security intelligence in Canada, while building a legacy of commitment to rights and the rule of law. We look forward to playing a continuing vital role in Canada's security intelligence community in the years ahead.

About this Report

How this Report is Organized

The Security Intelligence Review Committee exists to provide assurance to the Parliament of Canada—and through it, to Canadians—that CSIS is complying with law, policy and Ministerial Direction in the performance of its duties and functions. SIRC has two key functions. The first is to conduct in-depth reviews of CSIS activities to ensure that they comply with the *CSIS Act* and the various policy instruments that flow from it, and with direction from the Minister of Public Safety and Emergency Preparedness. The second is to receive and investigate complaints by any person about any action of the Service.

The 2004–2005 annual report is organized to reflect the Committee's key findings. 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 publication distinguishes between Committee findings, observations and recommendations arising from in-depth reviews or complaints 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: A Year in Review 2004–2005

This section provides the reader with summaries of the eleven major reviews SIRC conducted during the period covered by this report. In addition, it provides information regarding complaints received by the Committee. Finally, this section summarizes a special report forwarded to the Minister of Public Safety and Emergency Preparedness in accordance with Section 54 of the *CSIS Act*.

How this report is organized *(continued)*

Section 2: CSIS Accountability Mechanisms

Featured in this section are descriptions of the policy and governance framework within which CSIS carries out its duties and functions. This section also outlines information provided to SIRC by the Service relating to their branch investigations and changes to CSIS operational plans and priorities.

Section 3: Want to Know More? An Overview of SIRC

This section provides details of the information gathering, outreach, liaison and administrative activities of the Committee, including SIRC's annual budget and expenditures.

Identifying SIRC Studies: Choices and Challenges

SIRC's research program is designed to address a broad range of subjects. In selecting these for review, the Committee takes into consideration:

- the scope of CSIS investigations;
- particular activities that could intrude on individual rights and freedoms, as well as priorities and concerns for Parliament and the Canadian people;
- the CSIS Director's classified report to the Minister on operational activities; and
- the importance of producing regular assessments of each of the Service's operational branches, and regional offices.

The Committee also considers a number of other factors when it approves specific areas for review:

- the Committee's statutory obligations as detailed in the *CSIS Act*;
- events with the potential to cause threats to the security of Canada;
- issues or concerns identified in previous Committee reports;
- commitments by the Committee to re-examine specific matters;
- issues identified in the course of the Committee's complaints functions; and
- new policy directions or initiatives announced by CSIS or the Government of Canada.

This approach allows the Committee to manage the inherent risk of being able to review only a small percentage of CSIS activities in any given year. However, SIRC is always prepared to adjust planned activities to respond to unforeseen events. One such special review was prepared in the period covered by this report. Also noteworthy, SIRC was able to expand its research program in 2004–2005, as a result of new resources received through Supplementary Estimates.

Each review produced by the Committee follows a detailed examination 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 Direction.

While SIRC has only a small team of researchers, it seeks to examine as broad a spectrum of CSIS's duties and functions as is possible. Over a period of years, the body of completed research projects has provided Parliament, and the Canadian public, with a comprehensive description and assessment of the Service's operational activities.

Section 1

A Year in Review 2004–2005

A Year in Review 2004–2005

A. Reviews of CSIS Security Intelligence Activities

Overview: How SIRC Carries Out its Review Function

THE COMMITTEE'S ROLE IN CSIS'S ACCOUNTABILITY STRUCTURE

The Security Intelligence Review Committee is the only independent, external body equipped with the legal mandate and expertise to review the activities of CSIS. The Committee was established under the *CSIS Act* (1984) to provide assurance to the Parliament of Canada and to Canadians that CSIS is complying with law, policy and Ministerial Direction in the performance of its duties and functions. In doing so, the Committee seeks to ensure that the fundamental rights and freedoms of Canadians are respected.

To fulfill its mandate, the Committee directs staff to undertake a number of review projects each year. These reviews provide a retrospective examination and assessment of specific CSIS investigations and functions. SIRC has virtually unlimited power to review CSIS's performance of its duties and functions. With the sole exception of Cabinet confidences, SIRC has the absolute authority to examine all information concerning CSIS's activities, no matter how highly classified that information may be.

Each review includes the Committee's findings and recommendations. Upon completion, the report is forwarded to the Director of CSIS and the Inspector General (IG), CSIS.

SIRC is also authorized under Section 54 of the *CSIS Act* to provide special reports to the Minister of Public Safety and Emergency Preparedness on any matter that Committee Members identify as having special importance.

This review function enables the Committee to inform Parliament and the Canadian public on the activities of CSIS and to assess whether the Service's actions were carried out in accordance with the laws of Canada, directions from the Minister, and CSIS operational policy.

The Committee is but one of several mechanisms designed to ensure CSIS's accountability. The Service also remains accountable for its operations through the existing apparatus of government, specifically the Minister of Public Safety and Emergency Preparedness, the Inspector General of CSIS, central agencies of the federal government, the Auditor General, the Information Commissioner, and the Privacy Commissioner of Canada.

SIRC REVIEWS IN 2004–2005

Review of the Terrorist Entity Listing Process

Report # 2004-03

In 2004–2005, SIRC conducted its first review of a CSIS function engendered by Canada's new *Anti-Terrorism Act*, specifically the Service's role in the Terrorist Entity Listing (TEL)¹ process.

The Committee's review identified two key issues:

- In 2004–2005, SIRC conducted its first review of a CSIS function engendered by Canada's new *Anti-Terrorism Act*.
- the authority under which CSIS collects information for the TEL process, and the extent of their collection activity; and
 - the constraints on SIRC's ability to reasonably undertake a review of the listing process.

CSIS's Authority for Engaging in the Listing Process

The TEL process is mandated under Section 83.05 of the *Criminal Code*, as amended by the *Anti-Terrorism Act*. CSIS's role in the TEL process is the creation of Security Intelligence Reports (or SIRs), considered by the Minister of Public Safety and Emergency Preparedness in her recommendation to the Governor-in-Council concerning whether or not an entity should be listed.

When examining the Service's role in the TEL process, SIRC asked:

- What is the Services authority to participate in the TEL process?;
- What is the meaning of "threats to the security of Canada," as defined in Section 2 of the *CSIS Act*?, and
- Is the definition of "threats to the security of Canada" in the *CSIS Act* consistent with the definition of "terrorist activity" in the *Criminal Code*?

These questions were necessary because there are several entities on the *Criminal Code* list (which included 35 groups as of March 31, 2005) that do not appear to fall within the definition of "threats to the security of Canada" under the *CSIS Act*. For example, Japan's Aum Shinrikyo cult and Colombia's Autodefensas Unidas de Colombia are each listed as terrorist entities, but neither organization has committed a terrorist act on Canadian soil, nor does either have any obvious presence or support apparatus in Canada.

1. The *Criminal Code* refers only to a "list of entities." The acronym TEL is employed strictly to assist readers.

Section 2 of the *CSIS Act* is very specific, owing to the importance Parliament has placed on clear, legislative boundaries to the Service's collection activities. The *CSIS Act* defines "threats to the security of Canada" as activities "against Canada," or "detrimental to the interests of Canada" (2a); activities "within or relating to Canada" (2b, 2c); or activities "directed toward undermining" the "established system of

More about the Terrorist Entity Listing Process in Canada

In Canada, there are two mechanisms for being listed as a terrorist entity through domestic legislation: via the *United Nations Suppression of Terrorism Regulations* (UNSTR) or through the federal *Criminal Code* as amended by the *Anti-Terrorism Act*.

A person or group is placed on the UNSTR list if the United Nations Security Council agrees to list an individual or entity pursuant to the UN Afghanistan Regulations, which permits the listing of individuals or groups associated with the Taliban or Osama Bin Laden. As a UN member nation, Canada automatically adopts the listing. Alternately, a person or group may be placed on Canada's UNSTR list based on a recommendation by Foreign Affairs Canada (FAC). Usually this process begins when FAC receives notification of another country's intention to list a terrorist entity. FAC convenes an interdepartmental meeting to discuss the proposed listing and provides its recommendation to the Governor-in-Council. There are currently more than 480 names on the UNSTR list.

The names put forward for consideration for listing in the *Criminal Code* process emerge from interdepartmental consultation within the Government of Canada. Once an entity is suggested, the Service prepares a Security Intelligence Report (SIR) on that entity. The SIR is considered by the Minister of Public Safety and Emergency Preparedness, who makes a recommendation to the Governor-in-Council concerning whether or not the entity should be listed. There are almost 40 names on this list.

The consequences of being listed are serious. Anyone convicted of dealing directly or indirectly in property owned or controlled on behalf of a terrorist organization is liable to a fine of up to \$100,000 and up to ten years in prison. The Office of the Superintendent of Financial Institutions (OSFI) maintains an entity list on its website (www.osfi-bsif.gc.ca) that includes all individuals and entities listed on both the *Criminal Code* and the UNSTR lists. Financial institutions are required to review their records on a continuing basis for names of persons on this combined list and to report immediately their findings to both the RCMP and CSIS.

government in Canada” (2d). Canada and Canadian interests are the common denominator in all four definitions of “threats to the security of Canada.”

In contrast, Section 83.01 of the *Criminal Code* defines “terrorist activity” as an “act or omission,” corresponding to the listed offences, that is committed “in or outside Canada.” While the *CSIS Act* specifies a particular relationship to Canada (i.e., “within or relating to Canada”), the *Criminal Code* definition for terrorist activity may or may

not relate to Canada, because it includes activities that may take place “outside Canada,” and that need not specifically relate to Canada. It is not necessary for a terrorist activity to have a clear relationship to Canada for it to meet the definition of “terrorist activity” as defined by the *Criminal Code*.

The *Anti-Terrorism Act* was designed to harmonize Canadian legislation with that of its international partners. But this international dimension of the listing process is not accounted for in the *CSIS Act*.

As the Department of Justice has noted, the *Anti-Terrorism Act* was designed to

harmonize Canadian legislation with that of its international partners.² But as a result of SIRC’s review, the Committee noted that this international dimension of the listing process is not accounted for in the *CSIS Act*, which was designed to limit the Service’s collection activity to national concerns.

What this Means from SIRC’s Perspective

The Committee contends that the listing process may require CSIS to collect, retain, and analyze information that does not fall within the definition of “threats to the security of Canada” as defined in the *CSIS Act*.

As an analogy, CSIS’s authority for investigating threats falls within two concentric circles. The inner, smaller, circle represents the Service’s activity authorized under Section 12, which is limited to “threats to the security of Canada.” The outer, somewhat larger, circle represents the Service’s collection, analysis, retention and advice concerning information and intelligence on “terrorist activity” for the TEL process as mandated under the *Criminal Code*.

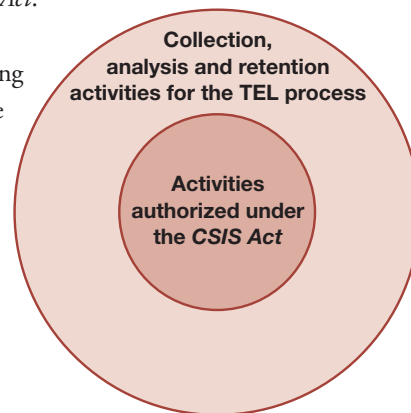


Figure: CSIS’s investigative activity falls within two concentric circles

2. See Department of Justice fact sheet “Canada’s Proposed *Anti-Terrorism Act*: Working with our International Partners” http://www.canada.justice.gc.ca/en/news/nr/2001/doc_27791.html (last updated April 24, 2003).

Much of the information in the two circles coincides and falls within the Service's mandate under the *CSIS Act*. But as a result of SIRC's review, the Committee concluded that there is an area where the two circles do not coincide.

SIRC recognizes that the Service has the statutory authority to collect information and intelligence for the TEL process, pursuant to Ministerial Direction to the Service. However, Ministerial Direction to CSIS cannot expand CSIS's mandate. It can only provide authority to CSIS to act within the limitations already established by the *CSIS Act*.

Overall, in the Committee's review of the Service's role in the TEL process, SIRC found that the Service's collection of information for the listing process was undertaken in accordance with Ministerial Direction—once this direction was provided³—and according to relevant operational policies. Nevertheless, SIRC concluded that the process required the Service to collect some information that does not fall under the authority set out in the *CSIS Act*, in regard to “threats to the security of Canada.”

SIRC concluded that the process required the Service to collect some information that does not fall under the authority set out in the *CSIS Act*, in regard to “threats to the security of Canada.”

The Committee is concerned by this extension of CSIS's collection activity, and by the lack of clear authority pertaining to that activity. After all, Parliament intended that the Service's collection activity would be precisely defined owing to the extraordinary powers exercised by CSIS.

SIRC's Ability to Review CSIS's Role in the TEL Process

The Special Senate Committee that originally examined Bill C-36 (the *Anti-Terrorism Act*) expressed concerns that the TEL process lacked adequate provisions for independent review. Senators were especially concerned at CSIS's involvement in the two-year review of the list, noting that, in effect, the list would be reviewed by the same people who created it.⁴ As a result, Senators recommended that an Officer of Parliament position be created to review the TEL process or, alternatively, that SIRC be responsible for its two-year review.⁵

At that time, the Minister of Public Safety and Emergency Preparedness (who was then the Minister of Justice and Attorney General of Canada) argued that existing

3. SIRC notes that for the first year of the TEL process, CSIS performed its new duties without formal Ministerial Direction. The *National Requirements for Security Intelligence 2003–2004* took effect April 1, 2003, fifteen months after passage of the *Anti-Terrorism Act*.

4. The Minister of Public Safety and Emergency Preparedness completed her first statutory review of the entity list on November 16, 2004.

5. Special Senate Committee on the Subject Matter of Bill C-36 “First Report” (November 1, 2001), page 5.

review mechanisms were sufficient. She stated: “We have ongoing oversight mechanisms that have proved effective, be that SIRC, be that the courts. Therefore, I would be disinclined to think about the creation of a new oversight mechanism that is separate and apart from those that exist.”⁶

In February 2005, Senators raised this concern again with the Minister (as Minister of Public Safety and Emergency Preparedness) during her address to the Special Senate Committee on the *Anti-Terrorism Act*. Again, she cited SIRC as one of the “important safeguards and accountability mechanisms” with respect to the *Anti-Terrorism Act*.⁷

Given that the Minister specifically cited SIRC’s ability to review the list as an important safeguard, the Committee believes it is important to note that although it can perform a fairly comprehensive review of the Service’s role in the TEL process, SIRC cannot

Although it can perform a fairly comprehensive review of the Service’s role in the TEL process, SIRC cannot perform a complete review because it cannot see the Security Intelligence Reports upon which the Governor-in-Council’s decisions are based, owing to Cabinet confidence.

perform a complete review because it cannot see the Security Intelligence Reports upon which the Governor-in-Council’s decisions are based, owing to Cabinet confidence. SIRC accepts that Section 39(3) of the *CSIS Act* prevents the Committee from gaining access to a Cabinet confidence. In the past, however, on the few occasions when SIRC has encountered an issue of Cabinet confidence, SIRC reached agreement with past Solicitors General to satisfy its concerns.

An additional, but lesser, concern in SIRC’s review of the TEL process is that another agency, such as the RCMP, could prepare a Security Intelligence Report. The section of the *Criminal Code* on judicial review of

the listing process refers to “any security or criminal intelligence reports considered in listing the applicant” (83.05 [6]a), but does not specify which Canadian department or agency might prepare those reports. The inclusion of the word “criminal” suggests the RCMP could play a role in this process.

In the event that the RCMP were to prepare a Security Intelligence Report for consideration by the Governor-in-Council in the TEL process, SIRC would have no jurisdiction to review the matter, since its mandate is restricted to CSIS’s activity.

6. Hon. Anne McLellan, appearance before the Special Senate Committee on the Subject Matter of Bill C-36 (October 29, 2001). She also said: “There are oversight bodies now. You have mentioned SIRC. SIRC will take up any enhanced obligations as a body of oversight as it relates to CSIS in their more concerted effort to root out and prevent terrorist activities.”

7. Hon. Anne McLellan, appearance before the Special Senate Committee on the *Anti-Terrorism Act* (February 14, 2005).

SIRC's Actions

On the issue of Cabinet confidence, SIRC has raised the issue directly with the Minister when the Committee Members met with her in February 2005. The Committee also summarized its concerns in two letters to the Minister in December 2004 and

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

CSIS derives its primary authority to collect, analyze and retain information and intelligence from Sections 2 and 12 of the *CSIS Act*. It is an essential feature of almost every review conducted by SIRC to determine whether the Service carried out its duties and functions in accordance with these two sections of the *Act*.

Section 12 of the *Act* states:

"The Service shall collect, by investigation or otherwise to the extent that it is strictly necessary, and analyze 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 and advise the Government of Canada."

Section 2 of the *Act* defines threats to the security of Canada as:

- 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.*

Lawful advocacy, protest or dissent, are specifically excluded, unless carried out in conjunction with the enumerated threats.

March 2005. This concern was reinforced by SIRC’s April 18, 2005, appearance before the Special Senate Committee on the *Anti-Terrorism Act*, and on June 8, 2005, before the House Sub-Committee. **The Committee is disappointed to note that, at the time of publication of this report, SIRC had still not received a response.**

On the issue of Cabinet confidence, SIRC has raised the issue directly with the Minister when the Committee Members met with her in February 2005.

As the Senate Committee noted in their original report on Bill C-36, “the erroneous placement of a person or group on this published list could cause irreparable harm.”⁸ The Committee recognizes the significant civil libertarian issues involved in the TEL process and takes seriously the concerns raised in this review.

Review of CSIS’s Investigation of Transnational Criminal Activity

Report # 2004-02

Background

This review assessed CSIS’s investigation of transnational criminal activities (TCA) and focussed on the Canadian-based activities of several foreign-based, transnational organized crime groups. This is the second SIRC study on this subject, following Report #107, issued in 1998 (SIRC 1998-01).

In 1995, member states of the G7 (including Canada) agreed to recognize international criminal activity as a national security threat. Since 1996, the Solicitor General of Canada (now the Minister of Public Safety and Emergency Preparedness) has directed CSIS to investigate TCA as part of its annual National Requirements for Security Intelligence. Accordingly, it has been identified as a subject of concern in the Service’s annual counter-intelligence (CI) planning since 1995–1996. Investigations are conducted by the Counter Intelligence Branch’s TCA Units, which are located in regions across Canada.

The investigations sampled for this review were national in scope and subject to Level II and Level III targeting investigations into suspected threat-related activities as described in Section 2(b) of the *CSIS Act*. This section of the *Act* defines the Service’s intelligence role in relation to TCA. The previous study by SIRC emphasized the need for the

8. The Special Senate Committee on the Subject Matter of Bill C-36 “First Report” (November 1, 2001), page 5.

Service to differentiate carefully its national security role from criminal investigations conducted by law enforcement bodies/agencies.⁹ In this review, SIRC was mindful of that finding.

Methodology

The review was undertaken pursuant to SIRC's mandate under Sections 38(b) and 40 of the *CSIS Act*. SIRC selected an eight-month review period from September 1, 2002, to April 30, 2003, and reviewed a list of the Service's TCA targets to select an issue-based targeting authority and four individual targets. This offered an opportunity to review various targeting processes outlined in operational policy, including the introduction of a new investigation, a renewal and an upgraded (Level II to III) investigation.

The review sought answers to the following questions:

- Did the Service have reasonable grounds to suspect a threat to the security of Canada?
- Was the level and intrusiveness of the investigation proportionate to the seriousness and imminence of the threat?
- Did the Service collect only that information strictly necessary to fulfill its mandate to advise the Government of a threat?
- Was information exchanged with domestic and foreign agencies carried out in accordance with Sections 13 and 17 of the *CSIS Act*, as well as operational policies?

To respond to these questions, SIRC examined all hard-copy and electronic documentation reported in the review period, and assessed these for compliance with the *CSIS Act*, Ministerial Direction, National Requirements and operational policy. Specifically, SIRC reviewed:

- targeting decisions and investigations of a sample selection of targets;
- the Request for Targeting Authorities (RTAs) and supporting operational reports; and
- cooperation and exchanges of information with domestic and foreign partners.

Overall, the operations reviewed were conducted in accordance with the *CSIS Act*, Ministerial Direction and operational policy and the techniques employed by the Service were consistent with the approved targeting levels.

9. SIRC *Annual Report 1998–1999*, page 7.

Findings

SIRC concluded that CSIS had reason to believe that the activities of the four individual targets were foreign-directed or undertaken on behalf of foreign interests, and generally represented a threat as defined in Section 2(b) of the *CSIS Act*. In addition, SIRC found that the Service complied fully with Ministerial Direction and operational policy in applying for targeting authorization. It also applied a level of intrusiveness proportionate to the suspected threats.

Overall, the operations reviewed were conducted in accordance with the *CSIS Act*, Ministerial Direction and operational policy and the techniques employed by the Service were consistent with the approved targeting levels.

Section 12 of the *CSIS Act* authorizes the collection of information on suspected threats to the security of Canada. The Service then advises the Government of Canada about activities that may be suspected of constituting threats to the security of Canada.

The Committee found that the Service’s investigative practices in the area of transnational criminal activities have improved considerably and that there were comparatively few cases where tactical information was collected or retained.

SIRC found that the vast majority of information collected by CSIS on TCA within the review period was, indeed, strictly necessary to fulfill its mandate.

However, SIRC did note one instance in which information collected under Section 15 was inappropriately transferred to a Section 12 investigation. Section 15 of the *CSIS Act* allows the Service to conduct investigations for the purpose of providing security assessments. SIRC was concerned that the transfer of information originally collected as part of a Section 15 interview did not always meet the threshold of “strictly necessary.”

In this instance, SIRC believes the Service unnecessarily transferred personal, professional and employment information from a Section 15 interview to the operational reporting for the TCA Section 12 investigation.

Since the subject of the interview was not a target, SIRC concluded that this reporting exceeded reasonable requirements for background data and context. SIRC intends to monitor the operational reporting of information collected in Section 15 interviews to ensure that the Service operates in compliance with the *CSIS Act* and operational policy.

In its 1998 review, the Committee concluded “that the investigative threshold meant to distinguish strategic from tactical intelligence was [not] adequately defined” and,

as a result, CSIS collected and retained information on “tactical, street-level criminal activities that were clearly not within the scope of the Service’s strategic objectives.”¹⁰

In this study, the Committee found that the Service’s investigative practices in the area of transnational criminal activities have improved considerably and that there were comparatively few cases where tactical information was collected or retained.

Information relevant to criminal investigations was provided to law enforcement agencies consistent with Section 17 of the *CSIS Act*. Similarly, foreign exchanges were within the scope of established arrangements with those agencies. SIRC found that exchanges of information between the Service and domestic and foreign partners were

Targeting

CSIS establishes a targeting level to investigate the activities of persons or organizations when it has reasonable grounds to suspect that these activities are a threat to the security of Canada. The conditions for approval of a targeting level are set out in detail in CSIS operational policy. Authority to administer, 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 (Department of Justice), and a representative of the Deputy Minister of Public Safety and Emergency Preparedness Canada.

There are three levels of investigation:

Level I

- Allows for the use of minimally intrusive investigation techniques. 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.

Level II

- Allows for the use of moderately intrusive investigation techniques. Investigations may include personal interviews and limited physical surveillance.

Level III

- 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 judicial controls.

10. SIRC *Annual Report 1998–1999*, page 7.

accompanied by appropriate caveats. Moreover, they complied with operational policy as well as relevant Memoranda of Understanding.

While reviewing the issue-based investigation, the Committee noted a series of events that demonstrated particularly effective use of domestic and foreign arrangements. In this case, the Service assessed that certain information provided to it by another domestic agency was a threat to the life of an individual. Although not obligated to do so, the Service quickly obtained permission from the domestic agency to disclose pertinent information and forwarded it to a foreign partner agency. These actions may have thwarted an attempt on the individual's life.

There were no recommendations arising from this review.

Review of a Counter-Terrorism Investigation

Report # 2004-05

Background

For this study, SIRC examined a CSIS counter-terrorism investigation that had not been the focus of a comprehensive SIRC review in over a decade, yet has remained a high priority of the Counter Terrorism Branch. This investigation was the subject of a Level III targeting authority for suspected threat-related activities as described in Section 2(c) of the *CSIS Act*.

Methodology

At the outset, SIRC examined lists of all CSIS targets, warrants and human sources related to the Service's investigation. The Committee then selected for in-depth review one issue-based target, one targeted organization, six individual targets, one warrant and six human source operations. For each file, all electronic and hard-copy documentation was reviewed for the period from January 1 to December 31, 2003. To ensure a thorough review, SIRC also examined some documentation that was outside the review period.

As in other 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;
- acquisition and execution of warrant powers and special operations;
- management of human sources and sensitive operations;

- cooperation and exchanges of information with domestic partners;
- cooperation and exchanges of information with foreign partners; and
- advice to government.

SIRC sought to determine whether:

- CSIS 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 information that was strictly necessary to fulfill its mandate to advise the Government of a threat.

Findings

SIRC found that, based on the information in the Service's possession, CSIS had reasonable grounds to suspect that the targets of the investigation posed a threat to the security of Canada. The level and intrusiveness of the Service's investigation were proportionate to the suspected threat.

SIRC did seek clarification as to why an individual remained a target of investigation for several months following his departure from Canada. The Service's explanation satisfied SIRC that the delay in terminating the investigation against this target was reasonable.

Overall, the Service's activities complied with the *CSIS Act*, Ministerial Direction and operational policy. CSIS collected only the information that was 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 found that CSIS had information to support all of the factual statements in the affidavit. Moreover, the affidavit was complete and balanced—the facts and circumstances of the case were fully, fairly and objectively expressed.

SIRC found that the Service, in implementing the powers authorized by the warrant, complied with the *CSIS Act*, operational policy and the conditions imposed by the Federal Court. However, SIRC found that existing operational policy did not provide sufficient guidance concerning certain administrative procedures related to the execution of some warrant powers. The Service advised that new operational policy

SIRC did seek clarification as to why an individual remained a target of investigation for several months following his departure from Canada.

to address this shortcoming had been approved. SIRC also followed up on an issue of non-compliance with operational policy by a CSIS regional office that was noted in SIRC Study 2003-04, and found no problems of this nature in this investigation.

The human source operations were well managed by the Service and complied fully with Ministerial Direction and operational policy. The administrative and financial files for each operation were in good order. Moreover, SIRC found that CSIS appropriately managed the relationships with sources used in sensitive areas.

SIRC found that existing operational policy did not provide sufficient guidance concerning certain administrative procedures related to the execution of some warrant powers.

SIRC also assessed, against the backdrop of evolving legislation, the adequacy of the Service's human source operations policies, and found that current policies were sufficient. The Committee will continue to monitor this operational activity closely in future reviews.

The Committee found no problems or issues of concern with respect to the Service's dealings with domestic and foreign partners.

Exchanges of information with these agencies complied with the *CSIS Act*, Ministerial Direction and operational policy. SIRC brought to the Service's attention a small number of administrative errors or omissions in operational reporting, which the Service has subsequently corrected.

Finally, SIRC pursued an issue raised in SIRC Study 2003-02 concerning the implications of the *Anti-Terrorism Act*. This study raised concerns regarding the payment of human sources. SIRC asked the Service if it had reviewed its policies or guidelines concerning source compensation. In reply, the Service informed the Committee that it had received legal advice which indicated that its approach was appropriate.

In future reviews, SIRC intends to monitor the Service's human source operations involving listed terrorist entities, to identify any issues of concern and to re-evaluate the adequacy of operational policy in this area. There were no recommendations arising from this study.

Issue-Based Targeting

This type of targeting authorizes an investigation to take place in circumstances where CSIS suspects that there is a threat to the security of Canada, but where the particular persons or groups associated with the threat have not yet been identified. As in any other targeting procedure, if warrant powers are requested, approval must be granted by the Federal Court of Canada. Operational policy dictates that as soon as individual persons, groups or organizations are identified as taking part in threat-related activities in connection with an issue or event, the Service will seek separate targeting authority.

It continues to be the Committee's practice to assess all issue-based investigations on a case-by-case basis to ensure they are conducted appropriately.

Review of Activities and Investigations in a CSIS Regional Office

Report # 2004-04

Background

SIRC endeavours each year to undertake a comprehensive review of CSIS's activities in a particular region of Canada. This type of review looks across the board at the targeting of individuals, implementation of warrant powers, use of human sources, as well as cooperation and exchanges of information with Canadian and foreign partners. It provides unique insights into the ways CSIS employs various investigative tools at its disposal—in addition to the standard assessment of CSIS's compliance with the *CSIS Act*, Ministerial Direction and operational policies.

Methodology

SIRC selected a regional office, examining its activities for the period April 1, 2002–March 31, 2003. As a first step, the Committee examined preliminary data on all active investigations in 2002–2003. Based on this examination, it decided to focus its review on a specific counter-terrorism investigation, which became a counter-proliferation investigation in July 2002.

SIRC reviewed all hard-copy and electronic documentation during the review period, pertaining to five types of CSIS operational activities:

- the targeting of individuals suspected of engaging in threat-related activities, as well as the targeting approval process;

- the implementation of warrant powers against authorized targets;
- special operations enabling the execution of warrant powers;
- the direction of human sources against authorized targets; and
- exchanges of information with other domestic and foreign law-enforcement and security intelligence agencies.

SIRC also reviewed CSIS's internal security measures for the region, as well as any security violations and breaches between April 1, 2000 and March 31, 2003.

As in all reviews, SIRC sought to answer three key questions:

- whether CSIS had reasonable grounds to suspect a threat to the security of Canada;
- whether the level of targeting authority was proportionate to the threat; and
- whether the Service only collected information strictly necessary for its investigation.

SIRC conducted an on-site visit to gain a better understanding of the nature of regional operations and of the unique challenges that Service investigators face in the region under review.

Findings

Overall, the region's investigative activities during the review period complied with the *CSIS Act*, Ministerial Direction and operational policy. SIRC found that CSIS had reasonable grounds to suspect that the authorized targets of investigation posed a threat to the security of Canada, and that the intrusiveness of the techniques used were proportionate to the suspected threat these targets posed.

Warrant powers, such as telephone intercepts, are the most intrusive investigative techniques available to CSIS. These powers are granted by the Federal Court of Canada. SIRC found that CSIS complied with the terms of the Federal Court warrant in executing warrant powers, as well as conducting special operations during the review period. CSIS only used warrant powers that were necessary to further its investigation. It did not renew them where the other powers available through the targeting authority were sufficient. The Service also acted appropriately and within the law in directing human sources, as well as in exchanging information with other agencies.

Section 12 of the *CSIS Act* restricts CSIS to collecting information that is "strictly necessary" for its investigations of threat-related activities. SIRC found that, in general, CSIS had collected only that information that was strictly necessary to its investigation. In one instance, however, the Committee believes CSIS collected and reported personal information that approached the limit of what is allowed under the *Act*.

During the review, SIRC's attention was drawn to the involvement of certain targets in a local organization—one that had multiple functions. CSIS assessed that certain activities taking place were not a significant aspect of the organization, believing that it served primarily one purpose.

SIRC carefully examined all documentation referring to the organization. It also looked at information on file from a previous review of the same investigation. Based on this, the Committee found that the organization had a dual function.

SIRC believes operational policy governing certain types of investigations should apply to this organization. CSIS disagreed with this finding.

The Committee recognizes that in such situations, it can be difficult to determine which operational policy is applicable. Accordingly, SIRC recommended that CSIS define one particular term in its operational policy.

The Committee also found one instance in which CSIS did not fully comply with operational policy. CSIS did not agree with this finding. Apart from these issues, SIRC noted a few administrative errors in CSIS's implementation of warrant powers, use of human sources, and exchanges of information. These errors were minor and did not affect CSIS's investigations. Further, the Committee was informed that CSIS has made changes to prevent their reoccurrence.

Also of note, SIRC reviewed security practices and procedures that had been in use in the region under review since 2000. There was one breach of security, which gave rise to a related complaint that was investigated by SIRC under Section 42 of the *CSIS Act*.¹¹

SIRC's attention was drawn to the involvement of certain targets in a local organization—one that had multiple functions. CSIS assessed that certain activities taking place were not a significant aspect of the organization, believing that it served primarily one purpose ... SIRC believes operational policy governing certain types of investigations should apply to this organization. CSIS disagreed with this finding.

11. Security violations are less serious than security breaches. Violations are defined as any contravention of security policies, such as the failure to lock-up classified information. Breaches occur when any classified information or asset is the subject of unauthorized access or disclosure.

Review of a Counter-Proliferation Investigation

Report # 2004-09

Background

In July 2002, the Canadian Security Intelligence Service created the Counter Proliferation (CP) Branch, bringing together elements of investigations that were previously the responsibility of the Counter Terrorism (CT) and Counter Intelligence (CI) Branches. In 2004, SIRC undertook a review of this branch—its first opportunity to examine the Service’s counter-proliferation activities under the new organizational structure.

Methodology

This study examined the Service’s investigation, between January 1, 1999, and December 31, 2003, of the threat to Canadian security posed by activities related to the proliferation of weapons of mass destruction by persons or organizations linked to a certain country. To ensure a thorough review, SIRC also examined some material outside the scope of the review period.

The Committee reviewed the Service’s issue-based investigation. In addition, SIRC staff met with officials from the Service’s CP Branch to discuss certain aspects of this investigation.

As with all reviews of this nature, SIRC assessed the Service’s compliance with the *CSIS Act*, Ministerial Direction and operational policy by examining the following key operational activities:

- targeting decisions;
- investigative activities and operational reporting;
- cooperation and exchanges of information with domestic partners;
- cooperation and exchanges of information with foreign partners; and
- advice to the federal government.

SIRC sought to determine whether:

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

Findings

SIRC found that the Service complied fully with Ministerial Direction and operational policy with respect to the applications for targeting authorization. The statements made in the applications were supported by the Service's operational reporting. Based on the information in the Service's possession, SIRC concluded that the Service 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 investigation was proportionate to the suspected threat. CSIS collected only information strictly necessary to fulfill its mandate to advise the federal government of a threat.

SIRC endorsed the Service's approach of engaging relevant private-sector entities, undertaken via the Liaison Awareness Program (LAP). Providing CP briefings to the private sector not only assists the Service in meeting its operational requirements, but also provides a potentially valuable service to recipients who might be vulnerable to targeting by foreign entities. The LAP has provided leads in a number of cases and has fostered a cooperative spirit among industry representatives.

Overall, the Service's cooperation and exchanges of information with domestic and foreign partners complied with operational policy.

Overall, the Service's cooperation and exchanges of information with domestic and foreign partners complied with operational policy. SIRC found no problems or issues of concern with respect to the Service's cooperation with its domestic or foreign partners.

There were no recommendations arising from this review.

Review of CSIS's Information Operations Centre

Report # 2004-07

Background

In today's information age, hostile actors (e.g., extremists, terrorist groups, foreign intelligence services or armed forces) no longer need direct access to a computer to copy, destroy or manipulate data. Rather, a variety of techniques and software tools can be used to gain unauthorized remote access to exploit a targeted system. This type

of activity is called an “information operation,” and in some cases it can pose a threat to national security. Canada’s critical infrastructure¹²—which is dependent on computer networks—must be vigilant regarding such attacks. CSIS investigates the activities of those who are suspected of using information operations to threaten the security of Canada as defined under Section 2 of the *CSIS Act*.

Two thresholds must be met before CSIS begins investigating a suspected information operation:

- (1) there must be reasonable grounds to suspect that the activity is sponsored by a foreign state (or one of its agents), a terrorist group, or politically motivated extremists; and
- (2) the purpose of the attack must relate to espionage, sabotage, terrorism, foreign influenced activity or violence to achieve political, ideological or religious objectives.

In February 2002, to counter the threat posed by cyber-based attacks, CSIS established an Information Operations Centre (IOC), which is responsible for developing and using specialized investigative techniques.

Methodology

In 2004, SIRC undertook its first-ever review of CSIS’s investigation of threats against Canada’s critical information infrastructure. It did so with two objectives. First, SIRC reviewed the role of the IOC in investigating threats against Canada’s critical information infrastructure. Second, the Committee reviewed the IOC’s operations, examining one

In 2004, SIRC undertook its first-ever review of CSIS’s investigation of threats against Canada’s critical information infrastructure.

counter-intelligence investigation of an information operation for compliance with the *CSIS Act*, Ministerial Direction and Service operational policies.

The review covered the period between January 1, 2000 and December 31, 2003.

Findings

Notwithstanding two concerns identified below, SIRC found that in carrying out its duties and functions, the Service complied with the *CSIS Act*, Ministerial Direction and CSIS operational policies.

12. The Government of Canada has identified 10 critical infrastructure sectors: energy and utilities; communications and information technology; finance; health care; food; water; transportation; safety; government; and manufacturing (Government of Canada Position Paper on a National Strategy for Critical Infrastructure Protection, November 2004).

SIRC's first concern was that operational policy keep pace with the matter reviewed. The Committee recommended that the Service review its operational policies regarding Section 12 targeting in this area.

SIRC recommends that the Service review operational policy to ensure that it clearly incorporates certain matters in relation to Section 12 targeting.

The Committee's second concern was related to administrative errors. SIRC found four such errors. While three of these were minor, the fourth involved the Service's operational reporting—which could potentially affect the role of the targeting approval process as a mechanism for internal accountability. SIRC recommended that the Service review operational reporting policies to prevent a reoccurrence of this error.

SIRC recommends that the Service review operational policy to ensure that if it is necessary to cross-reference operational database reports recorded under one file number with reports recorded under another file number, this should be noted in the “Investigator’s Comments” section of the reports.

The Service has indicated that it will be examining ways to ensure the cross referencing operational database messages when they are transferred from one investigative file to another.

Review of CSIS's Exchanges of Information with Close Allies

Report # 2004-08

Background

In January 2004, the federal government created the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (O'Connor Commission). Former CSIS Director, Ward Elcock, defended CSIS's information-sharing practices, noting that SIRC had not made any criticism of the appropriateness or inappropriateness of any information CSIS had shared with any foreign agency in any cases it had reviewed since September 11, 2001.¹³

The case of Mr. Arar did, however, focus public attention on the use of information that may have been collected in Canada and then shared with Canada's foreign partners.

13. Public Hearing of Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, Transcript (June 22, 2004), page 277, line 21–23.

While SIRC has examined CSIS's information-sharing practices in the context of several past reviews, the Committee decided to undertake its first in-depth examination of CSIS's exchanges of information with close allied partners.

Methodology

Drawing on one of the Service's counter-terrorism investigations, SIRC chose to review CSIS's information exchanges with four allied agencies as the focus of the detailed review. This review covered the period June 1, 2003–December 31, 2003, but for thoroughness it also examined certain documentation that fell outside the review period. SIRC examined all relevant electronic and hard-copy documentation related to the investigation to determine if these exchanges about threats to the security of Canada were in accordance with the respective foreign arrangements for the four allied agencies and complied with the *CSIS Act*, Ministerial Direction and operational policy.

SIRC looked at:

- the scope of the foreign arrangement;
- the consent or approval required to disclose such information;
- any special conditions or limitations placed on the use of this information; and
- the nature of the information being shared.

Findings

In the context of the investigation that was reviewed, SIRC found that the Service's exchanges of information with allied agencies were in accordance with respective foreign

SIRC found that the Service's exchanges of information with allied agencies were in accordance with respective foreign arrangements and complied with the *CSIS Act*, Ministerial Direction and operational policy.

arrangements and complied with the *CSIS Act*, Ministerial Direction and operational policy. The Committee also found that the Service exercised due diligence in exchanging information about targets of investigation.

While the Service obtained appropriate approval prior to disclosing information to selected allied agencies, SIRC recommended that CSIS amend operational policy to indicate clearly the managerial level accountable for disclosures to foreign agencies. However, it was CSIS's position that ultimate accountability is clearly defined in policy.

SIRC recommended that CSIS amend operational policy to indicate clearly the managerial level accountable for disclosures to foreign agencies.

In this study, SIRC also examined how human rights were addressed within the context of foreign arrangements.

When CSIS initiates the process to enter into a new arrangement with a foreign agency, it informs Foreign Affairs Canada and the Minister of Public Safety and Emergency Preparedness that it will “closely scrutinize the content of the information provided to, or received from, a foreign agency in order *to ensure* [our emphasis] that none of the information sent to, or received from, that agency is used in the commission of, or was obtained as a result of, acts that could be regarded as human rights violations.”

SIRC took note of two issues arising from this statement.

First, the use of the term “ensure” implies that CSIS will make certain that the information shared does not lead to—or result from—acts that could be regarded as human rights violations. **However, the Committee concluded that CSIS was not in a position to provide such an absolute assurance.** As Mr. Elcock told the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, CSIS would not necessarily reject information that might have been obtained as a result of human rights violations. He explained that CSIS “[is] there to collect information... that may reflect on a threat to the security of Canada and we will look at information from any source in order to secure some information about threats to the security of Canada.”¹⁴

Second, while CSIS is cautious when sharing information with foreign agencies, it cannot determine in all cases how that information is used by the recipient agency. Similarly, the Service is rarely in a position to determine how information received from a foreign agency was obtained. As Mr. Elcock stated to the O’Connor Commission, when it comes to information that may have been the product of torture, “the reality is in most cases we would have no knowledge that it was derived from torture. You may suspect that it was derived from torture, but that is about as far as one will get in most circumstances.”¹⁵

The Committee found that CSIS’s assurance to the Minister could be misinterpreted as it is rarely in a position to determine how information that went to a foreign agency is used, or how information it receives was obtained.

14. Public Hearing of Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, Transcript (June 21, 2004), page 162, line 15–19.

15. Public Hearing of Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, Transcript (June 21, 2004) page 159, line 23–25; page 160, line 1–2.

In response to this study, the Service took the position that all correspondence between CSIS and the Minister of Public Safety and Emergency Preparedness reflects an ongoing monitoring of the situation. According to the Service, they advise the Minister that exchanges of information with an allied agency will be commensurate with the degree of trust established over a period of time and reflective of the political and human rights climate within a country.

SIRC acknowledges that CSIS must rely on information received from its foreign partners to fulfill its mandate, and that the exchange of information between security intelligence agencies is an essential investigative tool. However, the Committee found that CSIS's assurance to the Minister could be misinterpreted as it is rarely in a position to determine how information that went to a foreign agency is used, or how information it receives was obtained.

SIRC recommended that CSIS revise the content of the letters to Foreign Affairs Canada and the Minister of Public Safety and Emergency Preparedness to avoid leaving any impression that it can guarantee that information sent to, or received from, a foreign agency was not used in the commission, nor was obtained as a result of, acts that could be regarded as human rights violations.

Review of a Counter-Intelligence Investigation

Report # 2004-06

Background

In this review, SIRC examined a CSIS investigation of a foreign intelligence service.

Methodology

SIRC examined this counter-intelligence investigation for the period January 1, 2003 to December 31, 2003. The objective was to assess the Service's compliance with the *CSIS Act*, Ministerial Direction and all relevant operational policies.

SIRC reviewed hard-copy and electronic documentation that pertained to the following CSIS operational activities:

- targeting of individuals suspected of engaging in threat-related activities, as well as the targeting approval process;
- application for a Federal Court warrant;
- implementation of warrant powers against authorized targets;
- direction of human sources against authorized targets; and
- selected advice to government departments.

As in all reviews, SIRC sought to answer three key questions:

- whether CSIS had reasonable grounds to suspect a threat to the security of Canada;
- whether the level of targeting authority was proportionate to the threat; and
- whether the Service only collected information that was strictly necessary for its investigation.

Findings

Overall, the counter-intelligence investigation was in compliance with the *CSIS Act*, Ministerial Direction and operational policy during the review period. SIRC found that CSIS had reasonable grounds to suspect that the authorized targets of investigation posed a threat to the security of Canada.

Moreover, the Committee found that the intrusiveness of the techniques used were proportionate to the suspected threat that these targets posed. CSIS investigators only collected information that was strictly necessary for the investigation. They also acted appropriately and within the law in their use of human sources.

SIRC found that CSIS had reasonable grounds to suspect that the authorized targets of investigation posed a threat to the security of Canada.

SIRC found that the Service's description of threat-related activities in the warrant affidavit accurately reflected the information that CSIS held. The Service complied with all applicable operational policies in applying for the warrant, as well as conditions imposed by the Federal Court when the warrant was approved. SIRC also found that CSIS complied with the terms of the Federal Court warrant in executing authorized warrant powers and in conducting special operations.

The Committee observed, however, that the scope of the warrant was overly ambitious. Two CSIS regions identified human resource shortages that affected their ability to analyze certain information collected. SIRC also noted that CSIS introduced a new information collection technique during the review period, which will be monitored in future reviews.

SIRC paid particular attention to CSIS's investigation of interference activities.

Throughout the review, SIRC paid particular attention to CSIS's investigation of interference activities. To ensure compliance with the *CSIS Act*, the Service was careful to develop strict guidelines to manage this aspect of its investigation. However, SIRC

found that CSIS's operational policies covering these types of situations were incomplete. Because of this, the Committee recommended that:

CSIS review and amend, where appropriate, its operational policies relating to specific institutions to ensure that they cover all aspects of a given process.

Also of note, while SIRC found that CSIS acted appropriately in providing advice to Government of Canada officials on the foreign intelligence service's activities, the Committee nevertheless believes that the Service was overly cautious in deciding not to share information with one federal department. CSIS disagreed with this finding and believes that given the sensitivity of the investigation, the Service took a judicious approach in the dissemination of any information.

Terrorist Financing Activities in Canada

Report # 2004-10

Background

Since September 11, 2001, the international community has increased its efforts to combat terrorist financing. In December 2001, the United Nations Security Council passed Resolution 1373, calling on member states to freeze the assets of those who commit or facilitate terrorist acts, and to adopt measures to prevent and suppress the financing of terrorism. In response, the Government of Canada passed the *United Nations Suppression of Terrorism Regulations* (UNSTR) and the *Anti-Terrorism Act*.

Traditionally, CSIS had examined terrorist financing through the lens of its counter-terrorism investigations, but the growing international focus since September 11, 2001, necessitated the development of a dedicated level of expertise. In 2002, CSIS created the Terrorist Financing Unit within its Counter Terrorism Branch to identify and track the financial structures that support terrorist organizations. That same year, the Minister's *National Requirements for Security Intelligence* specifically directed CSIS, for the first time, to investigate and advise the Government of Canada about the threat arising from terrorist financing.

Methodology

The objective of this study was to examine CSIS's investigation of terrorist financing activities in Canada for in-depth review. SIRC selected one issue-based target, and five specific targets. In each case, the Committee assessed the Service's compliance with

the *CSIS Act*, Ministerial Direction and operational policy by examining the following operational activities:

- targeting decisions;
- investigative activities and operational reporting;
- cooperation and exchanges of information with domestic agencies; and
- cooperation and exchanges of information with foreign agencies.

SIRC's review period was January 1, 2003–July 31, 2004. However, to ensure a thorough review, the Committee also examined select documents that fell outside this period.

Findings

The Committee concluded that the Service had reasonable grounds to suspect that the activities of targeted individuals and groups posed a threat to the security of Canada. The level and intrusiveness of the Service's investigation were proportionate to the suspected threat, and CSIS collected only that information necessary to fulfill its mandate. The Service's activities complied with the *CSIS Act*, Ministerial Direction and operational policy.

SIRC also found that the Service complied fully with Ministerial Direction and operational policy with respect to applications for targeting authorizations and renewals. The statements made in the applications were supported by the Service's operational reporting.

Finally, SIRC was satisfied with the degree and nature of the Service's cooperation with domestic and foreign partners. Exchanges of information with these agencies complied with the *CSIS Act*, Ministerial Direction, and operational policy.

Implementation of the UNSTR

During this review, SIRC learned that the implementation of the UNSTR required CSIS to manage new responsibilities related to the listing of terrorist entities. The Committee did not undertake a comprehensive review of CSIS's involvement in the listing of entities pursuant to the UNSTR, as this was not within the scope of the study. However, SIRC noted that CSIS's involvement in this process raised important legal questions—similar to those identified in the Committee's review of the Terrorist Entity Listing Process.

The criteria for listing under the UNSTR are set out in Section 2 of the legislation, which states that a person or group can be listed when there are reasonable grounds to believe that this entity: (a) has carried out, attempted to carry out, participated in or facilitated the carrying out of a terrorist activity; (b) is controlled directly or indirectly by any person conducting any of the activities set out in paragraph (a); or (c) are acting

on behalf of, or at the direction of, or in association with any person conducting any of the activities set out in paragraph (a).

Entities can be listed in two ways. First, they can be placed under a UN Security Council resolution, in which case they are then automatically included as a listed entity under the *United Nations Afghanistan Regulations* (UNAR). Second, the Governor-in-Council, on the recommendation of the Minister of Foreign Affairs, can decide to place an entity on the UNSTR list. In such cases, Foreign Affairs Canada (FAC) convenes an interdepartmental meeting to discuss the proposed listing. If CSIS has security intelligence on the entity, it prepares an assessment for its Director, indicating whether there are reasonable grounds to support the listing. This assessment is provided to FAC, who may use the information, along with input from many other federal departments and agencies, to support its recommendation to the Governor-in-Council.

The Service told SIRC that it engages in the listing of entities pursuant to the UNSTR under Section 12 of the *CSIS Act*, which limits the Service's collection activity to *threats to the security of Canada*. However, SIRC noted that the Service's involvement in the listing process requires it to determine whether an entity meets the definition of a *listed person* under the UNSTR, which has no such geographic restriction. As a result—similar to SIRC's study on the Terrorist Entity Listing Process—it is possible that the

In response to SIRC's concern relating to the UNSTR listing process, CSIS stated that they are only collecting and analyzing open information. The Service does not agree that the collection and retention of open information that is available to the public is an extension of the Service's mandate.

Service may be required to collect and analyze information regarding an entity that meets the definition of a *listed person or group* under the UNSTR, but does not represent a *threat to the security of Canada*. SIRC found evidence of this problem in its review of operational reports.

In response to SIRC's concern relating to the UNSTR listing process, CSIS stated that they are only collecting and analyzing open information. The Service does not agree that the collection and retention of open information that is available to the public is an extension of the Service's mandate. Further, SIRC noted that the UNSTR does not specifically direct the Service to

participate in the listing process, nor has the Minister of Public Safety and Emergency Preparedness provided CSIS with specific direction to that effect. Indeed, the *National Requirements for Security Intelligence 2003–2004* only made reference to the *Criminal Code* listing process, requiring that CSIS continue to conduct research and analysis in support of the listing of terrorist entities pursuant to the *Anti-Terrorism Act*.

SIRC will continue to monitor this issue. As always, it will continue to examine the implications of new legislation on the Service's operational activities. There were no recommendations arising from this study.

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

Report # 2004-01

Background

Security liaison posts are located strategically to meet the needs of the Service most effectively. CSIS's Foreign Liaison and Visits (FLV) Branch, which oversees the security liaison posts abroad, bases its operations on the principle of reciprocity. The Service must be prepared to share information with foreign security and intelligence agencies to receive information in return. Activities and exchanges of this nature are generally handled by the Service's security liaison posts. With the exception of Paris, Washington, and London, the locations of these posts are classified.

At the direction of the FLV branch, Security Liaison Officers (SLO):

- carry out regular liaison with foreign security and intelligence agencies;
- provide security screening services in support of the immigration program;
- oversee the exchange of security intelligence information with approved agencies;
- provide advice to senior staff of the Canadian Mission or Embassy; and
- are accountable to the Director General of FLV, to HQ operational managers, and to the Head of Mission for the SLO's geographical area of responsibility.

SIRC regularly reviews the Service's security liaison posts, as required under Section 38(a)(iii) of the *CSIS Act*. This year, SIRC chose to review a recently established security liaison post.

Methodology

In its review, SIRC sought to determine whether exchanges of information from this post with foreign agencies were within the scope of the government-approved liaison agreements in place. The Committee also assessed the operations at the security liaison post in relation to the *CSIS Act*, Ministerial Direction, and the Service's operational policies and procedures.

SIRC conducted this study by reviewing documents at CSIS Headquarters and through an on-site visit to the security liaison post. For context, SIRC also reviewed this

post's operations, and evaluated them against issues raised in SIRC's ongoing statutory reviews of CSIS's Foreign Arrangements. Moreover, the report considered trends identified in SIRC's SLO studies over the previous five years.

The review concentrated on two main issues: security screening workload and security at the post.

Findings

a) Compliance and Effectiveness

There were not enough exchanges during the review period for SIRC to assess definitively whether the Service's exchanges with foreign agencies at the Post were in accordance with the *CSIS Act*, Ministerial Direction and the Service's operational policies. However,

The lack of updated CSIS documents to assess the liaison relationships at the post did cause SIRC some concern.

SIRC's review of the exchanges that did take place suggests that the Service has approached its new liaison relationship with appropriate caution.

However, the lack of updated CSIS documents to assess the liaison relationships at the post did cause SIRC some concern. While

there are written guidelines for the creation, submission and updating of these documents, there are no formal CSIS policies governing this activity. Owing to the situation SIRC observed at this post, and the Service's growing exchanges with foreign organizations, the Committee made the following recommendation:

The Committee recommended that the Service create policies for the preparation, updating and annual submission of CSIS documents used to assess exchanges with foreign agencies.

The Committee also recommended that the written guidelines the FLV prepares concerning procedures at security liaison posts be updated to reflect actual Service practices.

b) Security Screening

One of the functions of an SLO is to assist Citizenship and Immigration Canada and the Canadian Border Services Agency to screen potential immigrants to Canada. If the employees of either of these organizations responsible for immigration screening at a security liaison post have security-related concerns, they may refer the case to the SLO, who investigates the matter.

SIRC notes that the SLO's security screening workload has been raised as a concern in each of its SLO studies over the past five years. In its most recent report, SIRC again raised concerns related to security screening workload and suggested the Service adopt numeric benchmarks for tracking and addressing security screening workload issues.

c) Security at the Post

SIRC examined the environment in which the post operated. The Committee concluded that the SLOs at the post acted in accordance with CSIS security procedures.

The Role of CSIS Security Liaison Officers

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

- they maintain and develop channels of communication with foreign agencies with which the Service has approved arrangements;
- they carry out security screening activities in support of the federal Immigration Screening Program;
- they report to CSIS Headquarters on any matter related to Canadian security interests; and
- they 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 Canada are separate and distinct from the Security Liaison Officer's functions and responsibilities.

Review of Foreign Arrangements

Background

Under Section 17(1) of the *CSIS Act*, the Service may enter into an arrangement with the government of a foreign state, or an international organization of states (or an institution thereof), for the purpose of performing its duties and functions. While Ministerial Direction and Service operational policy outline the principles regarding the establishment and management of such arrangements, the foreign arrangement determines the nature and extent of the Service's cooperation and exchanges with a foreign agency. The arrangement identifies the specific types of information sharing that can occur.

Section 38(a)(iii) directs SIRC to review all such arrangements. The Committee examines both the establishment and enhancement of arrangements entered into between CSIS and foreign intelligence agencies.

As noted in previous reports, a Ministerial Direction Compendium came into effect on March 1, 2001. This gives the Director of CSIS more freedom to manage the Service's activities. For example, the Director can approve the expansion of an existing foreign arrangement (one that has previously been approved by both the Minister of Public Safety and Emergency Preparedness and the Minister of Foreign Affairs). CSIS does not need to consult with the Department of Foreign Affairs nor does it need to request the Minister's approval to do so. As a result, the Director has greater discretion in this area of Service activity.

Reviews During 2004–2005

During 2004–2005, SIRC undertook its first comprehensive review of the expansion process—a first since the Ministerial Direction Compendium came into effect.

SIRC undertook its first comprehensive review of the expansion process—a first since the Ministerial Direction Compendium came into effect.

SIRC focussed on the ten arrangements that were expanded between April 1, 2002 and March 31, 2003, to determine whether these complied with Ministerial Direction and operational policy. An enhancement or expansion occurs when the Service changes an existing arrangement. This defines the subject matter and extent of authorized exchanges.

For each foreign arrangement, SIRC staff examined:

- the rationale for requesting an expansion;
- Canada's national security interests;
- the request to expand the arrangement;
- the approval to expand the arrangement; and
- the Service's assessment of the agency (i.e., respect of the third-party rule, reliability, human rights issues, internal stability concerns, etc.)

Staff reviewed:

- all documentation on the establishment of the arrangement, as per Section 17 of the *CSIS Act* and Ministerial Direction;
- all documentation on the expansion of the arrangement;
- the cooperation file with the organization;
- the most recent agency assessment;
- the most recent post profile prepared by the Security Liaison Officer; and
- any other information related to the arrangement and its enhancement.

Findings

SIRC found that CSIS complied with the conditions set out in Ministerial Direction and operational policy regarding the expansion of the ten existing foreign arrangements.

With respect to expansion approvals, SIRC noted that the Service has no operational policy on what type of information must be contained in the request submitted to the Director. The Committee also noted that the assessment of agencies with whom the Service has arrangements were not always submitted on a yearly basis as required in the Foreign Liaison Post Procedures Manual—and, in some cases, were seriously outdated. The matter of agency assessments was the subject of a recommendation under study # 2004-01.

One agency assessment did not provide an adequate analysis of potential human rights issues.

Of greater concern to SIRC, however, was that one agency assessment did not provide an adequate analysis of potential human rights issues. As these expansions involve an increased level of cooperation with a foreign agency, SIRC believes that a comprehensive re-evaluation of the agency in question should be required at the time of expansion to ensure that arrangements continue to undergo rigorous scrutiny—particularly in the area of human rights.

It is CSIS's position that when consideration is being given to expanding the arrangement, FLV provides the requisite information so that the Director can make an informed decision as to whether a given arrangement should be expanded. According to the Service, the absence of an up to date Agency Assessment does not mean that a review of the arrangement has not been prepared for the Director.

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 an existing one. Moreover, 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:

- they must be established as required to protect Canada’s security;
- they must remain compatible with Canada’s foreign policy objectives toward the country or international organization in question;
- they must respect the applicable laws of Canada; and
- 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.

The nature of the relationship between CSIS and a foreign organization is established when CSIS enters into an arrangement that 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 its 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, SIRC investigates complaints through a quasi-judicial hearing presided over by a Member of the Committee.

Through its investigation 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 Section 41 investigations, SIRC is 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 its 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 misdirected to SIRC, deemed to be outside the Committee's jurisdiction or investigated and resolved without a hearing (administrative review).

Description	2002–2003	2003–2004	2004–2005
Carried over	17	17	16
New	48	30	30
Total	65	47	46
Closed	48	31	28
Carried forward to subsequent year	17	16	18

* The Table reflects all complaints received by SIRC. However, not all complaints received resulted in an investigation by the Committee. Some were redirected to the appropriate government institutions, or were determined at the outset to be outside the Committee's jurisdiction, while others were withdrawn by the complainants.

Reports of Decisions: Case Histories

The following are summaries of the three decisions rendered by SIRC during the period under review in response to complaints filed with the Committee.

REPORT: HUMAN RIGHTS COMPLAINT REFERRAL

SIRC reported a decision concerning a complaint that was referred to the Committee by the Canadian Human Rights Commission under Section 45 of the *Canadian Human Rights Act* (CHRA).

The complaint alleged discrimination in contravention of the CHRA by the Service. More particularly, the complainant—a former employee of the Service—complained

The Committee concluded that the Service did not fail in its duty to accommodate the complainant, and did not discriminate against the complainant on grounds prohibited by the *Canadian Human Rights Act*. However, the Committee noted that the Service could have been more sensitive in the manner in which it delivered its decision of not being able to accommodate the complainant with part-time employment.

that the Service had failed to adjust hours of work and to allow time away from work, and thereby failed in its duty to accommodate the complainant's physical and mental disabilities.

The complainant had been working a limited number of hours per week because of disabilities. The Service required the duties of the complainant's position to be performed on a full-time basis. To have those duties performed on a part-time basis would have caused undue hardship to the Service. The Committee concluded that the Service did not fail in its duty to accommodate the complainant, and did not discriminate against the complainant on grounds prohibited by the *Canadian Human Rights Act*. However, the Committee noted that the Service could have been more sensitive in the manner in which it delivered its decision of not being able to accommodate the complainant with part-time employment.

Further, the Committee determined that—given the national security concerns associated with the investigation of the complaint—neither the Canadian Human Rights Commission nor the Canadian Human Rights Tribunal could conduct a meaningful investigation or hearing concerning the complaint.

Accordingly, the Committee recommended that the Canadian Human Rights Commission dismiss the complaint.

REPORT: SECTION 41 (“ANY ACT OR THING”)

The Committee reported a decision concerning a complaint pursuant to Section 41 of the *CSIS Act*, which states that any person may make a complaint about “any act or thing done by the Service.”

The complaint alleged that a Service employee had improperly conducted immigration security screening interviews with the complainant. After holding a hearing and reviewing the evidence, SIRC concluded that the complainant had not presented any evidence that would suggest the interviews were improperly conducted.

The Committee determined that, due in part to the fact that the complainant’s first language was neither French nor English, the complainant suffered from misapprehension or confusion during the immigration screening process as a result of correspondence from CIC.

REPORT: SECTION 42 (DENIAL OF SECURITY CLEARANCE)

SIRC reported a decision on a complaint pursuant to Section 42 of the *CSIS Act*, concerning a denial of security clearance.

The complainant applied for employment with an agency of the federal government, which denied the applicant the required security clearance based on information given to it by CSIS. The complainant contested the denial of the security clearance by filing a complaint with SIRC.

The decision of the deputy head to deny the security clearance was reasonable and the Committee recommended that the decision be upheld.

The complainant was seeking a Top Secret security clearance. According to the *Government Security Policy*, a Top Secret security clearance may not be granted where there are reasonable grounds to doubt the applicant’s loyalty to Canada or reliability as it relates to loyalty.

The Committee concluded that there were reasonable grounds to believe that the complainant may have engaged in intelligence collection activities on behalf of a foreign state, and appeared to have maintained regular contact with foreign representatives, who may have been involved in intelligence collection activities. Therefore, the decision of the deputy head to deny the security clearance was reasonable and the Committee recommended that the decision be upheld.

Complaints About CSIS Activities Under Section 41

Under 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 SIRC 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 (approximately 30 days), or the complainant must be dissatisfied with the response; and
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.

Referrals Under the *Canadian Human Rights Act*

In the event that the Canadian Human Rights Commission receives—under Subsection 45 (2) of the *Canadian Human Rights Act*—written notice from a Minister of the Crown that the practice to which a complaint relates was based on considerations relating to national security, the Commission may dismiss the complaint or refer the matter to SIRC. On receipt of such a referral, the Committee carries out an investigation and after consulting with the Director of CSIS pursuant to Section 55 of the *CSIS Act*, reports its findings to the Commission, the Minister who referred the complaint, and the complainant.

C. Section 54 Report to the Minister of Public Safety and Emergency Preparedness

Pursuant to Section 54 of the *CSIS Act*, SIRC may report to the Minister of Public Safety and Emergency Preparedness on any matter relating to the performance and functions of the Service.

In fall 2003, SIRC determined that the events involving Maher Arar were sufficiently important to warrant a special report of this nature. While the report's specific findings cannot be discussed as the matter remains the subject of an ongoing inquiry by the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (O'Connor Commission), this case

illustrates the difficult dilemma often faced by the Committee. Because of SIRC's legal obligation to protect both national security and privacy concerns, it is often difficult to convey the thoroughness or complexity of SIRC reviews, or provide the details that might help to substantiate its findings and recommendations.

SIRC was unfairly criticized when the government released a heavily redacted version without consulting the Committee. SIRC has stated publicly that it would have “no objection” if a summary of its classified report is released by the O'Connor Commission, once its own investigation is completed.

SIRC launched its Section 54 review months before the Commission of Inquiry was established. The Committee reviewed all material available to it under the *CSIS Act*, and provided its findings to the Minister in May 2004. Although the entire report was shared with the Commission, SIRC was unfairly criticized when the government released a heavily redacted version without consulting the Committee. SIRC has stated publicly that it would have “no objection” if a summary of its classified report is released by the O’Connor Commission, once its own investigation is completed.

As noted, SIRC may review only the activities of CSIS. However, in carrying out its review, SIRC identified a number of issues that appeared to warrant examination by the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar:

- the role of other federal departments and agencies in Arar’s rendition to Jordan by U.S. authorities;
- Arar’s subsequent detention and interrogation in Syria;
- whether CSIS information was included in RCMP files that were shared with American authorities; and
- how the United States came into possession of Arar’s 1998 rental-lease agreement.

SIRC concluded that the O’Connor Commission might also wish to comment upon the protections offered to Canadian citizens by the new Consular Understanding between Canada and the United States, announced by Canada’s Foreign Affairs Minister on January 13, 2004.

Section 2

CSIS Accountability Mechanisms

CSIS Accountability Mechanisms

A. Reporting Requirements

At least once a year, the Director of CSIS is required to submit to the Minister a report on the operational activities of the Service in accordance with Section 33(1) of the *CSIS Act*, which in turn is given to the Inspector General. After receiving the Director's report, the Inspector General is required to submit to the Minister a certificate stating the extent to which she or he is satisfied with the report, and to inform the Minister of any unauthorized activities or any unreasonable or unnecessary use of powers. The Minister is then required to submit the Director's report and the Inspector General's Certificate to SIRC.

Under Section 38(a)(i) of the *CSIS Act*, SIRC is required to review the Director's report and the Inspector General's certificate. SIRC's examination of the Director's report and Inspector General's certificate has proven helpful in identifying potential areas for future research and review. The Committee also uses the Director's report and the Inspector General's certificate to make yearly comparisons of CSIS activities and to monitor the performance of existing and new programs and sectors.

This section of SIRC's annual report reviews the Director's report, the Inspector General's certificate and summarizes other CSIS reporting requirements.

CERTIFICATE OF THE INSPECTOR GENERAL FOR 2004

The position of Inspector General (IG) was established in 1984 under the *CSIS Act*. The IG functions as the Minister's internal auditor of CSIS, reviewing the Service's operations. The Inspector General is responsible to the Deputy Minister of Public Safety and Emergency Preparedness, providing an independent means of assurance that CSIS is complying with the *CSIS Act*, Ministerial Direction and operational policy.

The certificate issued in November 2004 was the first to be issued by the current IG, who was appointed in December 2003. SIRC noted that the IG has adopted the validation process established by her predecessor, which consists of the review of select information and intelligence collected and retained by the Service. It also includes an examination of branch accountability reports and the "facting" on which they are based.

The IG also chose to review:

- a selected sample of warrants, targets and human-source case management;
- a sample of CSIS's foreign arrangements;
- CSIS's assistance to the Departments of Foreign Affairs and National Defence in the collection of foreign intelligence in Canada; and
- CSIS's involvement in the Integrated National Security Assessment Centre, the security certificate process, and a counter-intelligence operation.

In the certificate, it was noted that the Director of CSIS also reported five incidents of non-compliance with operational policy for 2003–2004. The IG looked into each of these incidents and found that appropriate action had been taken in each case.

In this year's certificate, the Inspector General reported to the Minister that she was "as satisfied as she could be" with the Director's annual report on the Service's operational activities. She concluded that the Service had exercised its duties and functions with a commendable degree of professionalism.

CSIS DIRECTOR'S ANNUAL OPERATIONAL REPORT 2003–2004

Every year, as noted, the Director of CSIS prepares for the Minister of Public Safety and Emergency Preparedness a report on the operational activities of the Service, which is sent to SIRC for review. The report outlines the achievements realized and challenges encountered by the Service in the preceding period.

In the 2003–2004 edition of this report, the Director noted that CSIS resources have expanded since the September 11th attacks, and also addressed specific challenges in meeting the demands of the current threat environment. The Director noted that perhaps the greatest challenge is the international and transnational nature of threats to the security of Canada, which have broadened the platform of Service operations. He noted that, increasingly, the most effective means of acquiring threat-related information is to obtain it offshore. The Director also highlighted an increasing need for joint operations and the Service's efforts to build relationships for greater liaison capacity with domestic partners and foreign allies.

i. Counter Terrorism

The report noted that the Service's highest priorities continue to be public safety and safeguarding against terrorist attacks occurring in or originating from Canada. The report described the priority counter-terrorism (CT) investigation, Sunni Islamic extremism. Other ongoing CT investigations were summarized, including the initiation of a new investigation into the potential for violence related to instability and conflict

in a specific country. A reduced threat level led the Service to terminate one particular investigation. The Director also described targeting authorities for certain terrorist organizations, mainly with respect to fundraising and support activities being undertaken in Canada.

The activities of the Terrorist Financing Unit (TFU) within the Counter Terrorism Branch were also summarized. This unit provides the Government of Canada with intelligence on the nature and extent of terrorist financing networks in Canada. As of April 1, 2004, there were 24 organizations listed as a result of the terrorist entity listing process.

ii. Counter Proliferation

The Director's report outlined ongoing Counter Proliferation (CP) investigations, including state sponsored terrorism as well as the foreign interference and espionage activities of specific foreign governments. The CP Branch was also responsible for Counter Proliferation Operations, the Foreign Intelligence and Assessments section, and the Integrated National Security Assessment Centre, which was scheduled to be reorganized into the Integrated Threat Assessment Centre, under the direction of the Prime Minister's National Security Advisor.

CSIS's Counter Proliferation Branch investigated the continuing threat posed by the proliferation of weapons of mass destruction. The Director reported that the international nature of the threat meant that many of the Service's investigations in the counter-proliferation area required close cooperation with allied intelligence services.

iii. Threat Assessment Centre

Also featured in the report were the activities of the CP Branch's Threat Assessment Centre, which is responsible for the Threat Assessment Unit (TAU) among others. The TAU is responsible for analyzing potential threats to Canadian interests at home or abroad, as well as threats to foreign interests and internationally protected persons located or travelling in Canada. The report noted the introduction of defined threat levels and the creation of a working group within the TAU in Ottawa.

The Director reported that the CP Branch worked closely with Citizenship and Immigration Canada (CIC), the Canada Border Services Agency and the then-Canada Customs and Revenue Agency (CCRA) to deny or monitor the entry to Canada of individuals who might pose a threat to the security of Canada.

The report also detailed the Branch's activities in support of efforts to remove two individuals from Canada, and in providing litigation support in two other cases in which the assessment of danger is ongoing.

iv. Integrated National Security Assessment Centre

During 2003–2004, the CSIS Director also reported to the Minister on the work of the Integrated National Security Assessment Centre (INSAC), which became operational in February 2003. This group comprised federal agencies with various responsibilities in the national security area, and allowed participants to access, share, analyze and disseminate information and intelligence. INSAC's efforts focussed on specific subjects of immediate and near-term interest. The Centre has since been replaced by the Integrated Threat Assessment Centre (ITAC), under the policy direction of the Prime Minister's National Security Advisor. Functional, day-to-day responsibility for the ITAC lies with the Director, CSIS.

v. Counter Intelligence

The report highlighted the work of the Counter Intelligence (CI) Branch. This branch investigates the activities of specific countries that dedicate significant effort to the clandestine collection of information to further their political, military and economic intelligence goals, as well as interference in expatriate communities in Canada. The report outlined the activities of certain countries and noted additional countries that were the subject of CI investigations.

vi. Human Source Program

The Director's report also detailed the Service's human source program, providing information on the number of human sources and the cost of the program. The Director's exercise of delegated authority for certain source activities was also reported, along with instances of Ministerial approval required in specific circumstances.

vii. Other Key Points

The Director noted that the creation of the Canada Border Services Agency was one of the most significant developments for the Security Screening Immigration Program during the reporting period. The report outlined the activities in the Security Screening Branch's four components that comprise immigration screening.

CSIS provides security assessments for all federal government departments (excluding the RCMP), and has several site-access programs, a Provincial Government Program and reciprocal agreements with foreign agencies. Specific activities in relation to each of these programs were outlined in the report.

During the reporting period, CSIS managed 16 Memoranda of Understanding (MOU) with federal government departments and agencies and MOUs with eight provinces. The Director reported no significant issues in relation to these arrangements.

The report also outlined Service activities concerning the 247 foreign arrangements in place as of March 31, 2004, including 13 new arrangements and the consolidation of three existing arrangements. Also of note, the Director reported on the efforts and challenges facing the Scientific and Technical Services Branch.

UNLAWFUL CONDUCT BY CSIS

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 her comments to the Attorney General of Canada and to SIRC.

In 2004–2005, the Service reported no such activity to the Minister.

SECTION 2(d) INVESTIGATIONS

The Service is authorized to collect, analyze 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 by covert unlawful acts, or intended to lead to the destruction or overthrow by violence of, 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 2004–2005, 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 2004–2005.

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 Subsection 19(2) as follows:

- (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 Minister of Public Safety and Emergency Preparedness or the Attorney General of the province in question;
- (b) information related to the conduct of Canada's external relations may be disclosed to the Minister of Foreign Affairs;
- (c) information related to the defence of Canada may be disclosed to the Minister of National Defence; and
- (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 made in the public interest.

B. Policy and Governance Framework

ANNUAL NATIONAL REQUIREMENTS FOR SECURITY INTELLIGENCE

Background

Pursuant to Subsection 6(2) of the *CSIS Act*, the Minister of Public Safety and Emergency Preparedness 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 2004–2005 National Requirements direct the Service to continue to maintain a flexible forewarning capability and meet Canada's evolving security intelligence needs by relying on risk management. The Minister notes that this approach will allow the Service to concentrate its resources on the foremost threats, while retaining the ability to respond to emerging issues in a timely fashion. CSIS is directed to focus on security intelligence needs with respect to the security of Canada as set out in Section 2 of the *CSIS Act*.

For 2004–2005, the Minister has directed CSIS to pursue the enumerated priorities in accordance with its mandate, including:

- safeguarding against the possibility of a terrorist attack occurring in or originating in Canada or affecting Canadian citizens or assets abroad;
- assessing the potential for attacks involving weapons of mass destruction;
- providing advice on Canada's economic security;
- safeguarding confidential Government of Canada information; and
- advising on threats to critical infrastructure.

In the 2004–2005 National Requirements, the Minister notes that today's threat environment is increasingly international and transnational in nature—intelligence work cannot be suspended at the Canadian border. CSIS is therefore directed to pursue foreign sources of threat-related information. It is also directed to support the establishment and operation of an Integrated Threat Assessment Centre (ITAC), as part of the Government of Canada's commitment to enhanced information-sharing, and to ensure the timely distribution of ITAC assessments. ITAC will replace CSIS's Integrated National Security Assessment Centre (INSAC).

The National Requirements acknowledge the demonstrated willingness of individuals, groups and states to use violence in support of political, religious, ideological or territorial objectives. The Minister notes that preferred target venues include locations that will yield maximum destruction and casualties. Further, the National Requirements acknowledge that Canada's response to terrorist activities has raised Canada's profile with terrorist actors and proponents.

As has been previously acknowledged, a significant portion of the world's terrorist groups are represented in Canada. The Minister notes that these groups engage in such activities as fundraising, lobbying, document fraud, planning and staging of terrorist acts, manipulation of émigré communities, facilitation to and from the United States, and the procurement of dual-use materials.

To a lesser extent, Canada also faces domestic issues that may lead to extremist acts or threats of serious violence. Therefore, CSIS is directed by the Minister to investigate and advise the Government of Canada about threats arising from:

- religious extremism;
- state-sponsored terrorism;
- secessionist violence;
- domestic extremism; and
- terrorist financing.

The Minister notes that today's threat environment is increasingly international and transnational in nature—intelligence work cannot be suspended at the Canadian border.

The Minister has also directed the Service to continue to conduct research and analysis in support of the terrorist entity listing process; to support Department of National Defence deployments; to increase its liaison capacity with foreign partners; and to

work towards the prosecution, deportation and denial of safe haven to members of terrorist organizations in cooperation with other federal departments and agencies.

CSIS is directed by the Minister to continue to identify countries and groups engaged in developing weapons of mass destruction (WMD) and other weapons proliferation programs and to support Canada's obligations to stem the acquisition of WMD

and other forms of proliferation, through the provision of relevant intelligence. The Minister also notes the activities of countries that collect information in and about Canada in support of their military, political and economic needs. CSIS is directed to investigate these threats, including foreign-influenced activities; transnational criminal activities; clandestine or coercive efforts by foreign governments to gain access to intelligence, proprietary information or technology; and attempts to steal, alter or destroy information or critical infrastructures.

The National Requirements note that CSIS's security assessments, screening investigations and security advice on immigration and citizenship matters are an important part of the Service's mandate. CSIS is directed to continue advising the Government of Canada on these matters and to provide security assessments in relation to citizenship and immigration processes, airports, land borders, marine security, Parliamentary precincts, nuclear power stations, restricted areas at special events, Order-in-Council appointments, and certain provincial governments.

Finally, CSIS is directed to continue to provide the Government of Canada with relevant, comprehensive and policy-neutral intelligence assessments and to keep pace with the rapid development of new technologies. In addition to upgrading technical equipment and information systems, the Service is directed to collaborate with the RCMP, the Department of Justice, Industry Canada, the Department of Public Safety and Emergency Preparedness Canada and other departments and agencies to prepare policy and legislation ensuring that Canada's laws keep pace with evolving technologies.

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 2004–2005 is described in the section above. No other directions were issued in the year under review.

GOVERNOR-IN-COUNCIL REGULATIONS AND APPOINTMENTS

Under Section 8(4) of the *CSIS Act*, the Governor-in-Council may issue regulations to the Service concerning the powers and duties of the Director of CSIS, as well as the conduct and discipline of Service employees. No such regulations were issued in 2004–2005.

CHANGES IN CSIS OPERATIONAL POLICY

CSIS Operational Policy sets out the parameters and rules governing the entire range of the Service's operational activities. The Operational Policy is regularly updated to conform to changes in legislation and Ministerial Direction. All changes to this policy are reviewed by the Committee to ensure that they conform with law and Ministerial Direction. Applicable operational policies are also reviewed and CSIS compliance with those policies assessed in the course of each of the reviews carried out by SIRC.

The Service reported to SIRC on the new operational policies implemented in 2004–2005, together with new policies under development and revisions to existing policies. CSIS noted that the major factors influencing these developments included changes in existing legislation, passage of new legislation and changes in operational methodology. Revised policies in 2004–2005 covered such subjects as Section 12 warrant acquisitions and caveats used in the disclosure of operational information and intelligence.

Two policies were under development during fiscal year 2004–2005. The first concerned the acquisition of production orders and the second addressed certain operational reporting. The Service also reported that a number of existing policies were under revision during the reporting period. These addressed subjects such as targeting, foreign liaison and cooperation, warrant powers and approvals, cooperation with Citizenship and Immigration Canada and the Canada Border Services Agency, and operational reporting.

The Service reported to SIRC on the new operational policies implemented in 2004–2005, together with new policies under development and revisions to existing policies.

In addition, SIRC obtained an update from the Service on the status of policies that were under development at the end of fiscal year 2003–2004. Several of these have since been implemented. CSIS reported that one policy project was still ongoing, as it required considerable consultation and was affected by the restructuring of certain government departments. A second policy project, intended to revise certain information disclosure procedures, was on hold at the end of fiscal year 2004–2005.

C. CSIS Operational Activities

COUNTER PROLIFERATION

The Counter Proliferation (CP) Branch collects information related to biological, chemical and nuclear weapons development programs of foreign governments. It also investigates state sponsorship of terrorism.

This is a relatively new branch, created in 2002. As such, in 2002–2003, SIRC committed to undertake in-depth reviews of this group in future years. In 2003–2004, the Committee undertook a review of the Service’s investigation of the threat to Canadian security posed by one country’s weapons of mass destruction (WMD) program (*see SIRC study # 2003-04*). In 2004–2005, SIRC reviewed a CP Branch investigation of actions by another country regarding WMD.

In 2004–2005, the CP Branch produced 406 of these reports—a significant reduction from 650 in the previous fiscal year.

The branch’s Threat Assessment Unit produces threat assessment reports on a wide range of topics. In 2004–2005, the CP Branch produced 406 of these reports—a significant reduction from 650 in the previous fiscal year. CSIS reported that the reduction was attributable to a number of factors, including revisions to reporting practices, changes in staffing and the creation of the Integrated Threat Assessment Centre (ITAC) which, in 2004, replaced the branch’s Integrated National Security Assessment Centre.

The Service also briefed SIRC on the creation of a new unit that manages the Service’s investigations of certain foreign state-driven weapons of mass destruction (WMD) programs and proliferation-related activities.

As reported in previous SIRC annual reports, one of the priorities of CP Branch in 2004–2005 was the investigation of efforts by a certain country to advance its WMD programs and capabilities.

The Branch also expanded its intelligence collection regarding states that sponsor terrorism, as well as the terrorist groups that benefit from that support. The CP Branch reported to SIRC that it had succeeded in identifying, recruiting and directing human sources to report on these matters.

The Branch provided SIRC with information on the role played by CSIS in connection with the November 2004 visit to Canada by United States President George W. Bush. The Branch worked closely with other Service branches and government partners responsible for security during this event. The Threat Assessment Unit prepared numerous threat assessment reports, and the CP Branch seconded staff to the RCMP National Operations Centre for the duration of the visit.

The Service also reported on information provided to a government agency pertaining to efforts of a particular country to acquire restricted technology. Based on information from both domestic sources and a foreign intelligence agency, CSIS also learned of an institution operating in Canada which had possible links to a terrorist organization.

COUNTER TERRORISM

The role of the Counter Terrorism (CT) Branch is to advise the Government of Canada on emerging threats of serious violence that could affect the safety and security of Canadians and of Canada's allies. These threats could originate in Canada or abroad.

As reported in SIRC's previous three annual reports, Sunni Islamic extremism remained the major focus of the Counter Terrorism Branch's operational activities. It undertook certain restructuring to respond to the fluidity of this priority. Additional reassignments at the supervisory level were also implemented within the branch in 2004–2005.

It also reported on a new and growing extremist threat in Canada and other Western democracies, in which targets are in their twenties, technologically savvy and completely westernized.

The CT Branch also reported on support to the RCMP and a foreign intelligence service. A total of 137

Section 19 disclosure letters were issued by the Branch in 2004–2005. This section of the *CSIS Act* authorizes the Service to disclose information obtained in the performance of its duties and functions to Canadian law enforcement, diplomatic and defence personnel. The Branch also provided SIRC with details regarding the total number of individual and organizational targets that were the subject of ongoing investigations during the year under review.

A new and growing extremist threat in Canada and other Western democracies, in which targets are in their twenties, technologically savvy and completely westernized.

In 2004–2005, the Committee reviewed CSIS counter-terrorism investigations as well as the Service’s advice to the government concerning terrorist financing. The results of these studies are presented in this report. SIRC will continue to undertake reviews of CSIS’s counter-terrorism investigations in 2005–2006.

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 there have been no structural changes to the Branch and the 2005–2006 Annual Plan has made no changes to the priorities as outlined in the annual plan for the previous year. The Service notes that the espionage activities of CI’s targets continue to become more complex and sophisticated. CSIS reported to SIRC on the measures taken to address these challenges. The CI Branch continues to place great importance on human source recruitment to maximize its operational effectiveness.

During the year under review, the CI Branch did not issue any Section 19 disclosure letters or advisory letters. The Branch informed SIRC of the number of targets and level of targeting authority; these include individual, organization and issue-based targets.

RESEARCH, ANALYSIS AND PRODUCTION (RAP) BRANCH

RAP is responsible for producing security intelligence assessments to support the Service’s operations and the Government of Canada’s decision-making in relation to threats to national security. Given the nature of today’s security environment and

“The involvement of this many of RAP’s resources resulted in successfully satisfying the legislative requirements of the listing process; however, it did affect the ability of RAP to maintain its ‘normal’ research and production responsibilities.”

the immediacy of information, RAP must ensure that the information provided to decisionmakers is accurate and timely.

In fiscal year 2004–2005, RAP chose to focus on the production of strategic and operational analyses of current threats and emerging issues. The *Intelligence Briefs, Reports* and *Studies* remain core RAP documents, and are distributed widely throughout the security intelligence community, including SIRC.

In 2004–2005, responsibility for two programs was redirected to RAP. This branch is now the central point for the management

of all the information received from one of the Service's major allies and for the subsequent dissemination of this information on behalf of the CT, CI and CP branches.

The Research, Analysis and Production Branch took on responsibility for the Terrorist-Entity Listing Process this year, at the time of the two-year review of the listings process. As indicated in SIRC study # 2004-03, RAP described their involvement in the first two-year review of the terrorist list as a "major project." The review process involved five research librarians from the Information Centre, twelve RAP analysts, and four lawyers. RAP estimates that approximately ten days were necessary to research and write a two-year review SIR for each of the 35 entities listed. RAP noted that "the involvement of this many of RAP's resources resulted in successfully satisfying the legislative requirements of the listing process; however, it did affect the ability of RAP to maintain its 'normal' research and production responsibilities."

Finally, RAP must report Section 19 disclosures. RAP discloses information to the RCMP under Section 19(2)(a), of which there were 155 disclosures in 2004–2005. The CT, CP and CI Branches reported to SIRC on their Section 19(2)(a) disclosures to law enforcement agencies. As for Section 19(2)(b) disclosures to Foreign Affairs Canada, the Service reported that there were 673 in 2004–2005. Finally, there were 384 disclosures to the Department of National Defence by RAP under Section 19(2)(c).

RAP Intelligence Products

Research, Analysis and Production Branch (RAP) 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 of Canada. The intention is to provide a reference document for CSIS operational branches and/or external clients. A CSIS study contains an executive summary, is not limited in length, and is usually classified.

CSIS Report

A concise analytical product that is the result of 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 CSIS report is usually classified and is up to eight pages long.

RAP Intelligence Products *(continued)***CSIS Intelligence Brief (CIB)**

A concise analytical product designed to provide internal and external clients with an analysis of a current threat or an emerging issue 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. Profilers do not exceed three pages. Some Profilers are unclassified but carry the added caveat “For Official Use Only.”

Fact Sheet

Designed to provide information about the past or current organizational structure of foreign intelligence and security services. It 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. Sheets are restricted to CSIS employees only.

Commentary

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. These are strategic documents with wide domestic and international distribution and are unclassified.

Special Report

This is a classified document intended for a very narrow or specific readership and is 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 Citizenship and Immigration Canada (CIC) and the Canada Border Services Agency to assist in processing refugee, immigration and citizenship applications. The Service's advice in these cases is based on the classes of individuals deemed inadmissible under the security-related criteria of the *Immigration and Refugee Protection Act*. CSIS also provides security assessments to CIC to assist in screening citizenship applications, pursuant to Section 19 of the *Citizenship Act*.

In 2004–2005, CSIS received a total of 101,097 government security clearance and “site-access” assessment requests. This represents a significant increase over the 74,835 requests processed in 2003–2004.

Table 2
Turnaround Times for Security Screening of Refugee Claimants and Immigration Applicants (2004–2005)

CSIS Security Screening Programs	Median ¹⁶ Turnaround (Calendar Days)		
	Non-adverse Advice	Information Briefs	Inadmissible Briefs
Front-end screening of refugees	27	336	248
Applications for permanent residence within Canada—refugee determination program	56	515	527
Applications for permanent residence within Canada—immigration program	44	511	333
Applications for permanent residence from the USA	150	599	642
Applications for permanent residence from outside Canada (excluding USA)	7	531	236

16. In this section of the annual report, SIRC refers to the Service's *median* turnaround times for processing screening requests rather than average or *mean* times. The Committee believes this represents more accurately the typical processing times by mitigating the impact of unusually short or lengthy processing times.

In 2004–2005, CSIS received a total of 101,097 government security clearance and “site-access” assessment requests. This represents a significant increase over the 74,835 requests processed in 2003–2004. Also of note during 2004–2005, the Service issued 39 information briefs and three recommendations for denial of government security clearances. For the same period, the Service received a total of 254,364 requests for immigration, refugee, front-end screening and citizenship screening.

There was one structural change within the Branch during the past fiscal year, to process site-access requests. The Branch reported that there were no changes to security screening priorities as outlined in their 2004–2005 annual plan.

Security Clearances

The Service reported that it received 36,519 requests for new or updated security clearances—down slightly from 37,508 during the previous fiscal year. In 2004–2005, there was a significant increase in the turnaround times for Level I (Confidential) and II (Secret) security assessments for the Department of National Defence (DND), and an improvement in the turnaround time for DND on Level III (Top Secret) clearances.

The Service reported that it received 36,519 requests for new or updated security clearances—down slightly from 37,508 during the previous fiscal year.

For the balance of federal departments and agencies, there was a small increase in the median turnaround for Level I and II clearances, with an improvement to Level III turnaround times.

The median turnaround times for the Service to provide its assessments to government clients can be found in Table 3 below.

Table 3
Turnaround Times for Security Screening of Government Clients

Category	Level	Median Number of Calendar Days	
		2003–2004	2004–2005
DND	I (Confidential)	20	49
	II (Secret)	18	63
	III (Top Secret)	96	70
Other departments and agencies	I (Confidential)	7	12
	II (Secret)	11	14
	III (Top Secret)	82	69

Site-Access Programs

The Service received a total of 64,578 site-access requests in 2004–2005. This is an increase compared to the 28,822 requests received in 2003–2004. Of these, the Service received 31,086 requests under the *Airport Restricted Access Area Clearance Program*. The median turnaround time for the Service's response to these requests was 24 calendar days.

Included in the 64,578 processed requests were 7,857 requests by 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 these site-access requests was one calendar day. The balance of the requests (i.e., those received from other government departments) were processed in one calendar day.

Table 4
Site-Access Programs

Program	Number of Site-Access Requests Processed	Median Turnaround Time (Calendar Days)
Parliamentary Precinct Program	1,110	1
Airport Restricted Area Program	31,086	24
Nuclear facilities	6,747	1
Other government departments	25,635	1

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 2004–2005, the Service concluded 869 screening requests on behalf of foreign agencies—down from the 1,208 checks concluded in 2003–2004. Field investigations were conducted in 151 of these screening requests.

Security Screening for Refugee Claimants and Immigration Applicants

In 2004–2005, CSIS received 97,761 requests for security screening of immigration and refugee applicants—a decrease of 3,529 applications from the previous fiscal year.

In 2004–2005, CSIS received 97,761 requests for security screening of immigration and refugee applicants—a decrease of 3,529 applications from the previous fiscal year.

The Service provided immigration officials with a total of 232 information briefs and 150 inadmissible briefs. In the previous fiscal year, CSIS produced 221 information briefs and 99 inadmissible briefs.

In 2004–2005, the Service also provided 16 incidental letters and 55 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 64.

Security screening of refugee and immigration applicants is carried out under the three main programs listed in Table 5 below.

**Table 5
Security Screening of Refugee Claimants and Immigration Applicants (2004–2005)**

CSIS Security Screening Programs	Requests Received	Information Briefs	Inadmissible Briefs
Front-end screening of refugees	22,871	115	69
Applications for permanent residence within Canada	38,628	84	65
Applications for permanent residence from outside Canada (including SLO referrals)	36,262	33	16
Total	97,761	232	150

Front-End Screening of Refugee Claimants

The Front-End Screening (FES) Program, implemented by the Government of Canada in November 2001, identifies potential security concerns about refugee claimants in Canada as early as possible in the refugee determination process. For 2004–2005, the Service reported receiving 22,871 applications under this program. During the

same period, the Service provided advice on 22,227 cases—including 115 information briefs and 69 inadmissible briefs.

Under the FES Program, the median turnaround time for the Service to issue

non-adverse advice was 27 days. Median turnaround times were 336 days for information briefs and 248 days for inadmissible briefs. This represents a small increase over last year's numbers of 332 days for information briefs and 214 days for inadmissible briefs.

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 2004–2005, the Service received 38,628 requests—24,389 under Canada's immigration program and 14,239 through the refugee determination program.

The median turnaround times for the Service to provide its advice in these cases varied considerably in 2004, depending on whether the Service received the request in hard copy or via Electronic Data Exchange (EDE). The Service noted that electronic exchanges are already well established for Canada's immigration program—with the exception of overseas immigration and vetting of visa applications. Ninety-five percent of inland Canada immigration applications were conducted electronically (EDE). For 2004–2005, the median turnaround time for hard-copy applications was 33 days, and 45 days for EDE applications.

Applications for Permanent Residence from Outside Canada

For permanent residence applications originating outside Canada or the United States, the Service shares responsibility for security screening with immigration officials at Canadian missions abroad. In such cases, CSIS only becomes involved in the process when they receive a request from the Immigration Program Manager. This process allows the Service to focus on higher-risk cases.

During this review period, the Service received 5,408 requests to provide screening advice for applications submitted to Canadian immigration offices in the

For 2004–2005, the Service reported receiving 22,871 applications under the Front-End Screening Program.

During this review period, the Service received 5,408 requests to provide screening advice for applications submitted to Canadian immigration offices in the United States.

United States. For these applications, the median turnaround time was 25 calendar days for electronic (EDE) applications and 288 days for hard-copy applications.

Forty-four percent of immigration applications originating in the United States were submitted electronically. The median turnaround time for immigration security screening cases that resulted in a *Notice of Assessment—Checked on the Basis of Information Supplied or No Reportable Trace* was 150 days.

For applications from outside Canada, other than the United States, the Service concluded 26,430 requests. Eighty-three percent of these applications were managed electronically by EDE. The median turnaround time for hard-copy applications was 38 calendar days—electronic applications took six calendar days. In addition, the Service's Security Liaison Officers were consulted on 4,593 cases. The Service issued 17 information briefs and 11 inadmissible briefs. The median turnaround times were 531 days for information briefs, 236 days for inadmissible briefs and seven days for non-adverse advice.

CSIS's advice to Citizenship and Immigration Canada (CIC)

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

- *Notice of Assessment—Checked on the Basis of Information Supplied and/or No Reportable Trace*: This report is 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 an applicant meets the inadmissibility criteria outlined in the security provisions of the *IRPA*.
- *Information brief*: Advice provided by CSIS when it has information that the applicant is or was involved in activities as described in the security provisions of the *IRPA*, but that the Service is of the opinion 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* (e.g., 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*.

Foreign Liaison and Visits (FLV) Branch

The Foreign Liaison and Visits (FLV) Branch is responsible for the Service's liaison with foreign agencies. It uses liaison channels to exchange information on threats to the security of Canada.

Under Section 17(1) of the *CSIS Act*, the Service may enter into an arrangement with foreign states—including foreign governments or international organizations of states or institutions thereof—for the purpose of performing its duties and functions. While Ministerial Direction and Service operational policy outline the principles regarding the establishment and management of such arrangements, the scope of a foreign arrangement determines the nature and extent of the Service's cooperation and exchanges with a foreign agency. The scope also identifies the specific type of information sharing that can occur.

At the end of fiscal year 2004–2005, the Service had 257 foreign arrangements with 143 countries. During that period, the Service received Ministerial approval to establish ten new arrangements and submitted a request for two others. CSIS also modified or expanded one foreign arrangement and asked for Ministerial approval to expand three others.

At the end of fiscal year 2004–2005, the Service had 257 foreign arrangements with 143 countries.

Of the Service's 257 foreign arrangements, 42 were identified as dormant (with dormancy defined as no liaison contact for at least one year). The Service continues to maintain restrictions on exchanges of information in the case of five of these dormant arrangements, due to:

- concerns about the foreign agency's human rights record;
- one or more violations of the rule against transferring information to a third party;
- or
- an overall lack of reliability of the liaison contact.

The Service can opt to re-activate dormant arrangements in cases where regional conflicts and political events that may affect Canadian national security interests may transpire.

The FLV Branch is also responsible for security liaison posts. As part of its foreign liaison program, the Service maintains security liaison posts abroad, normally co-located with Canadian diplomatic missions. The Service relies heavily on its security liaison posts to assess the usefulness of individual CSIS Section 17 foreign arrangements, as well as the reliability of those foreign agencies. These posts also provide significant

support to Citizenship and Immigration Canada related to Sections 14 and 15 immigration screening requirements (*see Report # 2004-01 in this year's annual report*).

The FLV also coordinates visits to CSIS Headquarters and CSIS Regional Offices by foreign agency representatives, including foreign ambassadors, as well as travel abroad by Service representatives.

CSIS DOMESTIC ARRANGEMENTS

The discharge of the Service's mandate under Sections 12–16 of the *CSIS Act* routinely requires cooperation among governments at the federal and provincial level, as well as with police services in a given province. Cooperation can take the form of exchanges of information, providing operational assistance, or conducting joint operations. CSIS does not require a formal arrangement when disclosing information to any domestic government department, agency or police service in accordance with its responsibility

to advise government. Classified information passed under these circumstances to any federal department or agency is protected under normal provisions of the Government Security Policy.

However, under Section 17(1)(a) of the *CSIS Act*, the Service may, with the approval of the Minister, conclude written cooperation arrangements—referred to as memoranda of understanding—with domestic agencies for the purpose of performing its duties and functions.

CSIS entered into an arrangement with the Prime Minister's National Security Advisor in the Privy Council Office with respect to the establishment and management of the Integrated Threat Assessment Centre.

In the year under review, CSIS entered into an arrangement with the Prime Minister's National Security Advisor in the Privy Council Office with respect to the establishment and management of the Integrated Threat Assessment Centre, making a total of 17 such arrangements with federal institutions. The number of domestic arrangements with the provinces (10) remained unchanged. There were no terminations or amendments to existing arrangements.

Relationship with the RCMP

Among domestic arrangements, the Memorandum of Understanding between CSIS and the RCMP figures most prominently in SIRC's review because of the volume of exchanges between these two organizations and their ongoing history of joint operations.

In 2004–2005, there were 855 written or verbal exchanges of information provided to the Service by the RCMP—a significant increase over the 615 exchanges in the previous year. The Service, for its part, provided the RCMP with 227 disclosure letters in 2004–2005, and 215 in the previous year. A disclosure letter from CSIS is required to allow the RCMP to use Service information to pursue a criminal investigation.

During 2004–2005, CSIS also provided the RCMP with 24 advisory letters—compared to 15 letters in 2003–2004. The RCMP request advisory letters from the Service to use CSIS information in court proceedings.

The year under review marks the fourth year of operation for the RCMP-led Integrated National Security Enforcement Teams

(INSETs), to which CSIS staff from four regions, as well as CSIS Headquarters, have been seconded. The Service reports that the INSETs have proven to be beneficial in that they have fostered closer cooperation between the Service and the RCMP. Because INSETs are operationally led by the RCMP, SIRC has a very limited capacity to review their activities—and indeed these joint operations once again highlight the limitations of SIRC’s mandate in the increasingly operationally integrated security sector.

This year, two SIRC studies (2004-02 and 2004-07) examined the substance of the information exchanged with the RCMP and the nature of cooperation between the two organizations during the course of its reviews of regional offices and CSIS investigations.

FEDERAL COURT WARRANTS AND WARRANT STATISTICS

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

In 2004–2005, there were 855 written or verbal exchanges of information provided to the Service by the RCMP—a significant increase over the 615 exchanges in the previous year.

Table 6
New and Replaced/Renewed/Supplementary Warrants

	2002–2003	2003–2004	2004–2005
New warrants	52	68	40
Replaced/Renewed/Supplementary	150	130	207
Total	202	198	247¹⁷

Every year, SIRC asks CSIS to provide statistics on the Service’s request for warrants (i.e., the information CSIS provides the Court in seeking a warrant), as well as on warrants granted by the Federal Court. Table 6 compares the number of warrants issued in each of the last three fiscal years.

In 2004–2005 most warrants were approved for one year. A select few were approved for a shorter span at the request of the Service. This was done to allow the expiration of these warrants to coincide with the expiration dates of other warrants on related files.

For three applications, the Court asked the Service for interim reports to provide the Court with up-to-date information on the status of a target, or to justify the continued need for—or usefulness of—the warrants.

In another case, the Court declined to grant one of the powers sought by the Service until the Court had been provided with more compelling evidence of the need for that power.

On several occasions, revisions were made to affidavits in support of applications during the hearings before the Federal Court. In one instance, the Court adjourned the hearing

The use of warrants by CSIS deserves continued scrutiny—a task that SIRC takes very seriously.

so that the Service could make changes. The application was approved after the submission of amended documents.

The Federal Court did not impose any new conditions or revise any existing conditions on warrants during the fiscal year under review. The Service also reported that in 2004–2005, no judicial decisions affected its applications for warrants, the execution of powers contained in warrants, or the warrant process in general.

17. The increase in warrant totals reflects a revised process for calculating statistics and does not represent an increase in the Service’s targeting.

According to the Service, the Federal Court issued nine urgent warrants during 2004–2005, compared to 30 in the previous year.

Also of note, Section 28 of the *CSIS Act* authorizes the Governor-in-Council to make regulations governing: the forms of warrants; the practice and procedure applicable to the hearing of applications; as well as the place where (and the manner in which) hearings may be held. There were no regulations made in 2004–2005.

Section 3

**Want to Know More?
An Overview of SIRC**

Want to Know More? An Overview of SIRC

COMMITTEE MEMBERSHIP

During the 2004–2005 fiscal year, SIRC was chaired by the Honourable Paule Gauthier, P.C., O.C., O.Q., Q.C., who was first appointed Chair on September 30, 1996, and reappointed to a second five-year term in 2000. M^{me} Gauthier's appointment as Chair ended on June 7, 2005. On June 24, 2005, the Honourable Gary Filmon, P.C., O.M., was appointed as SIRC's new Chair, and M^{me} Aldéa Landry, P.C., Q.C. was appointed as the Committee's newest member. Other Members of the Committee are: the Honourable Raymond Speaker, P.C., O.C. (reappointed on September 16, 2004, to a new five-year term); the Honourable Baljit Chadha, P.C.; and the Honourable Roy Romanow, P.C., O.C., Q.C.

On June 24, 2005, the Honourable Gary Filmon, P.C., O.M., was appointed as SIRC's new Chair, and M^{me} Aldéa Landry, P.C., Q.C. was appointed as the Committee's newest member.

All Members of the Committee are Privy Councillors, who are appointed by the Governor-in-Council after consultation by the Prime Minister with the leaders of the Opposition parties. There were no vacancies on the Committee at the close of this fiscal year.

STAFFING AND ORGANIZATION

The Committee is supported by an Executive Director and a staff of 19, located in Ottawa. The staff comprises: an Associate Executive Director, a Deputy Executive Director, Senior Counsel, Counsel, Senior Paralegal (who also serves as Access to Information and Privacy Officer/Analyst), nine Researchers, a Corporate Services Manager and four administrative staff.

Committee Members provide staff with direction on research and other activities that are identified as a priority for the year. Management of day-to-day operations is delegated to the Executive Director with direction, when necessary, from the Chair as Chief Executive Officer.

RESEARCH AND REVIEW ACTIVITIES

On an annual basis, the Committee identifies specific CSIS investigations and areas of responsibility for detailed review. Unforeseen events or new priorities may result in these reviews being supplemented by additional projects. SIRC analysts undertake the detailed research for each project, with direction from senior management and

regular reporting to the Committee. Given the highly classified and sensitive nature of the materials being reviewed, SIRC staff divide their time between SIRC's premises and a fully equipped office at CSIS Headquarters, set up for the exclusive use of Committee staff.

SECURITY INTELLIGENCE BRIEFINGS

As part of their ongoing information gathering, the Chair of SIRC, Committee Members, and senior staff participate in regular discussions with CSIS executive and staff, and other senior members of 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. Such activities enrich the Committee's knowledge about the range of issues and opinions affecting the security intelligence field. The Committee also visits CSIS regional offices on a rotating basis to examine how Ministerial Direction and CSIS policy affect the day-to-day work of investigators in the field. These trips give Committee Members an opportunity to meet with senior CSIS staff, to receive briefings on local issues, challenges, priorities and perspectives, and to communicate the Committee's focus and concerns. During the 2004–2005 fiscal year, the Committee visited two regional offices.

ADDITIONAL COMMITTEE ACTIVITIES

- On September 8, 2004, SIRC's Executive Director addressed the Interim Committee of Parliamentarians, which was established to consult and make recommendations regarding the proposed statutory Committee of Parliamentarians on National Security.
- The Chair, Committee Members, and Executive Director attended the International Intelligence Review Agencies Conference in Washington, D.C., October 3–5, 2004. The Committee stayed an extra day to meet with representatives from the oversight bodies of the American security and intelligence community.
- On October 6, 2004, the British High Commission visited SIRC's office to introduce the new Chief of the British Security Intelligence Services, who was appointed in August 2004.
- On October 6, 2004, the Associate Executive Director, on behalf of the Executive Director, was a guest lecturer at a Carleton University Canadian Centre of Intelligence and Security Studies seminar on intelligence, statecraft and international affairs. The Associate Executive Director provided students with an overview of SIRC.
- The Executive Director attended the Canadian Centre of Intelligence and Security Studies (CCISS) Conference in Ottawa on April 14–15, 2004, entitled "Conference on the Gouzenko Affair: The Beginnings of Canadian Counter-Espionage and Cold

War Intelligence History.” The Executive Director is a member of the board of advisors for the CCISS.

- The Executive Director and several staff attended a conference of the Canadian Association of Security and Intelligence Studies, held in Ottawa on October 14–17, 2004.
- On November 26, 2004, the Executive Director and Deputy Executive Director met with members of the Netherlands Supervisory Committee on the Intelligence and Security Services.
- On March 21, 2005, the Executive Director gave a presentation to the students of the “National Security and Intelligence in the Modern State” course at Carleton University.
- In Spring 2005, SIRC released *Reflections*—a publication that recounted the watershed events over the Committee’s 20-year history, including the McDonald Commission, the passage of the *CSIS Act*, as well as key reviews and complaint cases that SIRC has undertaken over the past two decades. It also provided detailed information on the inner workings of the Committee—helping to raise public awareness about SIRC’s role and responsibilities.

BUDGET AND EXPENDITURES

The Committee continues to manage its activities within allocated resource levels. Staff salaries and travel within Canada for Committee hearings, briefings and review activities represent its chief expenditures. In December 2004, Parliament approved Supplementary Estimates, which increased SIRC’s budget by \$344,000 in 2004–2005, as well as in future years. This was based on a 2002 Treasury Board submission in which SIRC presented a business case explaining why additional funding was required to keep abreast of a 30% increase in CSIS’s budget. This new funding was used mainly to hire additional research staff. Table 7 below presents a breakdown of actual and estimated expenditures.

Table 7
SIRC Expenditures

	2004–2005 (Actual \$)	2005–2006 (\$ Estimates)
Personnel	1,766,330	1,777,000
Operating	886,822	1,019,000
Total	2,653,152	2,796,000

INQUIRIES UNDER THE ACCESS TO INFORMATION AND PRIVACY ACTS

The public may make requests to SIRC under both the *Access to Information Act* and the *Privacy Act*. Table 8, *Requests for Release of Information*, outlines the number of requests SIRC has received under these acts for the past three fiscal years.

Access to Information requests for the Committee's studies represent the largest portion of the access requests. The work required to prepare a report for public release need only be done once, but this benefits all subsequent requesters. Consequently, the Committee waives the application fees for all requests for access to its studies.

Table 8
Requests for Release of Information

Year	<i>Access to Information Act</i>	<i>Privacy Act</i>
2002–2003	20	4
2003–2004	31	1
2004–2005	21	3

MODERN COMPTROLLERSHIP

SIRC made significant progress on the implementation of modern comptrollership initiatives during this fiscal year. The organization completed a management action plan, a risk assessment, an audit plan and developed performance indicators. Additional work in support of the implementation of modern comptrollership will continue in the new fiscal year. Given its small staff complement and the absence of dedicated, functional specialists, SIRC often relies on contracted resources to obtain the necessary expertise for this initiative.

Appendix A

Acronyms

Acronyms

CBSA	Canada Border Services Agency
CCRA	Canada Customs and Revenue Agency
CHRA	<i>Canadian Human Rights Act</i>
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
FAC	Foreign Affairs Canada
FES	Front-End Screening
FLV	Foreign Liaison and Visits
HQ	CSIS Headquarters, Ottawa
IG	Inspector General
INSAC	Integrated National Security Assessment Centre
INSETS	Integrated National Security Enforcement Teams

IOC	Information Operations Centre
IRPA	<i>Immigration and Refugee Protection Act</i>
ITAC	Integrated Threat Assessment Centre
LAP	Liaison Awareness Program
OSFI	Office of the Superintendent of Financial Institutions
PSEP	Public Safety and Emergency Preparedness
RAP	Research, Analysis and Production
RCMP	Royal Canadian Mounted Police
RTA	Request for Targeting Authority
SIR	Security Intelligence Report
SIRC	Security Intelligence Review Committee
SLO	Security Liaison Officer
TAU	Threat Assessment Unit
TCA	Transnational criminal activity
TEL	Terrorist Entity Listing
TFA	Terrorist Financing Unit
UNAR	<i>United Nations Afghanistan Regulations</i>
UNSTR	<i>United Nations Suppression of Terrorism Regulations</i>
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 & CSE, Section 40* (TOP SECRET) * (91/92-04)
35. *Victor Ostrovsky* (TOP SECRET) (91/92-05)
36. *Report on Two Iraqis—Ministerial Certificate Case* (SECRET) (91/92-06)
37. *Threat Assessments, Section 40 Study* (SECRET) * (91/92-07)
38. *The Attack on the Iranian Embassy in Ottawa* (TOP SECRET) * (92/93-01)
39. *“STUDYNT” The Second CSIS Internal Security Case* (TOP SECRET) (91/92-15)
40. *Domestic Terrorism Targets—A SIRC Review* (TOP SECRET) * (90/91-13)
41. *CSIS Activities with respect to Citizenship Security Screening* (SECRET) (91/92-12)
42. *The Audit of Section 16 Investigations* (TOP SECRET) (91/92-18)
43. *CSIS Activities during the Gulf War: Community Interviews* (SECRET) (90/91-12)
44. *Review of CSIS Investigation of a Latin American Illegal* (TOP SECRET) * (90/91-10)

45. *CSIS Activities in regard to the Destruction of Air India Flight 182 on June 23, 1985—A SIRC Review* (TOP SECRET) * (91/92-14)
46. *Prairie Region—Report on Targeting Authorizations (Chapter 1)* (TOP SECRET) * (90/91-11)
47. *The Assault on Dr. Hassan Al-Turabi* (SECRET) (92/93-07)
48. *Domestic Exchanges of Information (A SIRC Review—1991/92)* (SECRET) (91/92-16)
49. *Prairie Region Audit* (TOP SECRET) (90/91-11)
50. *Sheik Rahman's Alleged Visit to Ottawa* (SECRET) (CT 93-06)
51. *Regional Audit* (TOP SECRET)
52. *A SIRC Review of CSIS SLO Posts (London & Paris)* (SECRET) (91/92-11)
53. *The Asian Homeland Conflict* (SECRET) (CT 93-03)
54. *Intelligence-Source Confidentiality* (TOP SECRET) (CI 93-03)
55. *Domestic Investigations (1)* (SECRET) (CT 93-02)
56. *Domestic Investigations (2)* (TOP SECRET) (CT 93-04)
57. *Middle East Movements* (SECRET) (CT 93-01)
58. *A Review of CSIS SLO Posts (1992-93)* (SECRET) (CT 93-05)
59. *Review of Traditional CI Threats* (TOP SECRET) (CI 93-01)
60. *Protecting Science, Technology and Economic Interests* (SECRET) (CI 93-04)
61. *Domestic Exchanges of Information* (SECRET) (CI 93-05)
62. *Foreign Intelligence Service for Canada* (SECRET) (CI 93-06)
63. *The Audit of Section 16 Investigations and Foreign Intelligence Reports* (TOP SECRET) (CI 93-11)

64. *Sources in Government* (TOP SECRET) (CI 93-09)
65. *Regional Audit* (TOP SECRET) (CI 93-02)
66. *The Proliferation Threat* (SECRET) (CT 93-07)
67. *The Heritage Front Affair. Report to the Solicitor General of Canada* (SECRET) * (CT 94-02)
68. *A Review of CSIS' SLO Posts (1993–94)* (SECRET) (CT 93-09)
69. *Domestic Exchanges of Information (A SIRC Review 1993–94)* (SECRET) (CI 93-08)
70. *The Proliferation Threat—Case Examination* (SECRET) (CT 94-04)
71. *Community Interviews* (SECRET) (CT 93-11)
72. *An Ongoing Counter-Intelligence Investigation* (TOP SECRET) * (CI 93-07)
73. *Potential for Political Violence in a Region* (SECRET) (CT 93-10)
74. *A SIRC Review of CSIS SLO Posts (1994–95)* (SECRET) (CT 95-01)
75. *Regional Audit* (TOP SECRET) (CI 93-10)
76. *Terrorism and a Foreign Government* (TOP SECRET) (CT 94-03)
77. *Visit of Boutros Boutros-Ghali to Canada* (SECRET) (CI 94-04)
78. *Review of Certain Foreign Intelligence Services* (TOP SECRET) (CI 94-02)
79. *The Audit of Section 16 Investigations and Foreign Intelligence Reports* (TOP SECRET) (CI 94-01)
80. *Domestic Exchanges of Information (A SIRC Review 1994–95)* (SECRET) (CI 94-03)
81. *Alleged Interference in a Trial* (SECRET) (CT 95-04)
82. *CSIS and a “Walk-In”* (TOP SECRET) (CI 95-04)

83. *A Review of a CSIS Investigation Relating to a Foreign State* (TOP SECRET) (CI 95-02)
84. *The Audit of Section 16 Investigations and Foreign Intelligence Reports* (TOP SECRET) (CI 95-05)
85. *Regional Audit* (TOP SECRET) (CT 95-02)
86. *A Review of Investigations of Emerging Threats* (TOP SECRET) (CI 95-03)
87. *Domestic Exchanges of Information* (SECRET) (CI 95-01)
88. *Homeland Conflict* (TOP SECRET) (CT 96-01)
89. *Regional Audit* (TOP SECRET) (CI 96-01)
90. *The Management of Human Sources* (TOP SECRET) (CI 96-03)
91. *Economic Espionage I* (SECRET) (CI 96-02)
92. *Economic Espionage II* (TOP SECRET) (CI 96-02)
93. *Audit of Section 16 Investigations and Foreign Intelligence Reports 1996–97* (TOP SECRET) (CI 96-04)
94. *Urban Political Violence* (SECRET) (SIRC 1997-01)
95. *Domestic Exchanges of Information (1996–97)* (SECRET) (SIRC 1997-02)
96. *Foreign Conflict—Part I* (SECRET) (SIRC 1997-03)
97. *Regional Audit* (TOP SECRET) (SIRC 1997-04)
98. *CSIS Liaison with Foreign Agencies* (TOP SECRET) (SIRC 1997-05)
99. *Spy Case* (TOP SECRET) (SIRC 1998-02)
100. *Domestic Investigations (3)* (TOP SECRET) (SIRC 1998-03)
101. *CSIS Cooperation with the RCMP—Part I* (SECRET) * (SIRC 1998-04)

102. *Source Review* (TOP SECRET) (SIRC 1998-05)
103. *Interagency Cooperation Case* (TOP SECRET) (SIRC 1998-06)
104. *A Case of Historical Interest* (TOP SECRET) (SIRC 1998-08)
105. *CSIS Role in Immigration Security Screening* (SECRET) (CT 95-06)
106. *Foreign Conflict—Part II* (TOP SECRET) (SIRC 1997-03)
107. *Review of Transnational Crime* (SECRET) (SIRC 1998-01)
108. *CSIS Cooperation with the RCMP—Part II* (SECRET) * (SIRC 1998-04)
109. *Audit of Section 16 Investigations & Foreign Intelligence 1997–98*
(TOP SECRET) (SIRC 1998-07)
110. *Review of Intelligence Production* (SECRET) (SIRC 1998-09)
111. *Regional Audit* (TOP SECRET) (SIRC 1998-10)
112. *CSIS Liaison with Foreign Agencies* (TOP SECRET) (SIRC 1998-11)
113. *Allegations by a Former CSIS Employee* (TOP SECRET) * (SIRC 1998-12)
114. *CSIS Investigations on University Campuses* (SECRET) (SIRC 1998-14)
115. *Review of Foreign Intelligence Activities in Canada* (TOP SECRET)
(SIRC 1998-15)
116. *Files* (TOP SECRET) (SIRC 1998-16)
117. *Audit of Section 16 Investigations & Foreign Intelligence* (TOP SECRET)
(SIRC 1999-01)
118. *A Long-Running Counter-Intelligence Investigation* (TOP SECRET)
(SIRC 1999-02)
119. *Domestic Exchanges of Information* (TOP SECRET) (SIRC 1999-03)
120. *Proliferation* (TOP SECRET) (SIRC 1999-04)

121. *SIRC's Comments on the Draft Legislation Currently Before Parliament—Bill C-31* (PROTECTED) * (SIRC 1999-05)
122. *Domestic Targets* (TOP SECRET) (SIRC 1999-06)
123. *Terrorist Fundraising* (TOP SECRET) (SIRC 1999-07)
124. *Regional Audit* (TOP SECRET) (SIRC 1999-08)
125. *Foreign State Activities* (TOP SECRET) (SIRC 1999-09)
126. *Project Sidewinder* (TOP SECRET) * (SIRC 1999-10)
127. *Security Breach* (TOP SECRET) (SIRC 1999-11)
128. *Domestic Exchanges of Information 1999–2000* (TOP SECRET) (SIRC 2000-01)
129. *Audit of Section 16 Investigations and Foreign Intelligence Reports 1999–2000* (TOP SECRET) (SIRC 2000-02)
130. *CSIS Liaison with Foreign Agencies* (TOP SECRET) (SIRC 2000-03)
131. *Regional Audit* (TOP SECRET) (SIRC 2000-04)
132. *Warrant Review* (TOP SECRET) (SIRC 2000-05)
133. *Review of CSIS Briefs to Citizenship and Immigration Canada 1999–2000* (TOP SECRET) (SIRC 2001-02)
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)
 151. *CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post*
(TOP SECRET) (SIRC 2004-01)
 152. *Review of CSIS's Investigation of Transnational Criminal Activity*
(TOP SECRET) (SIRC 2004-02)
 153. *Review of the Terrorist Entity Listing Process* (SECRET) (SIRC 2004-03)
 154. *Review of Activities and Investigations in a CSIS Regional Office*
(TOP SECRET) (SIRC 2004-04)

155. *Review of a Counter-Terrorism Investigation* (TOP SECRET) (SIRC 2004-05)
156. *Review of a Counter-Intelligence Investigation* (TOP SECRET)
(SIRC 2004-06)
157. *Review of CSIS's Information Operations Centre* (TOP SECRET)
(SIRC 2004-07)
158. *Review of CSIS's Exchanges of Information with Close Allies* (TOP SECRET)
(SIRC 2004-08)
159. *Review of a Counter-Proliferation Investigation* (TOP SECRET)
(SIRC 2004-09)
160. *Terrorist Financing Activities in Canada* (TOP SECRET) (SIRC 2004-10)
161. *Section 54 Report to the Minister of Public Safety and Emergency Preparedness*
(TOP SECRET) *

Appendix C

Key Findings and Recommendations

Key Findings and Recommendations

REVIEW OF THE TERRORIST ENTITY LISTING PROCESS

In 2004–2005, SIRC conducted its first review of a CSIS function engendered by Canada's new *Anti-Terrorism Act*, specifically the Service's role in the Terrorist Entity Listing (TEL) process. The TEL process is mandated under Section 83.05 of the *Criminal Code*, as amended by the *Anti-Terrorism Act*. CSIS's role in the TEL process is the creation of Security Intelligence Reports (or SIRs), considered by the Minister of Public Safety and Emergency Preparedness in her recommendation to the Governor-in-Council concerning whether or not an entity should be listed.

The Committee contends that the listing process may require CSIS to collect, retain, and analyze information that does not fall within the definition of “threats to the security of Canada” as defined in the *CSIS Act*. Overall, in the Committee's review of the Service's role in the TEL process, SIRC found that the Service's collection of information for the listing process was undertaken in accordance with Ministerial Direction—once this direction was provided—and according to relevant operational policies. Nevertheless, SIRC concluded that the process required the Service to collect some information that does not fall under the authority set out in the *CSIS Act*, in regard to “threats to the security of Canada.”

The Committee was unable to have access to the SIRs during its review of the Service's role in the TEL process, owing to Cabinet confidence. While SIRC was able to perform a reasonably comprehensive review of CSIS's role in this process, its efforts nevertheless fell short of a complete assessment.

REVIEW OF CSIS'S INVESTIGATION OF TRANSNATIONAL CRIMINAL ACTIVITY

This review assessed CSIS's investigation of transnational criminal activities (TCA) and focussed on the Canadian-based activities of several foreign-based, transnational organized crime groups. The investigations sampled for this review were national in scope and subject to Level II and Level III targeting investigations into suspected threat-related activities as described in Section 2(b) of the *CSIS Act*.

SIRC concluded that CSIS had reason to believe that the activities of the four individual targets were foreign-directed or undertaken on behalf of foreign interests, and generally represented a threat as defined in Section 2(b) of the *CSIS Act*. In addition, SIRC

found that the Service complied fully with Ministerial Direction and operational policy in applying for targeting authorization. It also applied a level of intrusiveness proportionate to the suspected threats.

There were no recommendations arising from this review.

REVIEW OF A COUNTER-TERRORISM INVESTIGATION

This study outlined the results of SIRC's examination of a CSIS counter-terrorism investigation that had not been the focus of a comprehensive SIRC review in over a decade, yet has remained a high priority of the Counter Terrorism Branch. This investigation was the subject of a Level III targeting authority for suspected threat-related activities as described in Section 2(c) of the *CSIS Act*.

The Committee selected for in-depth review one issue-based target, one targeted organization, six individual targets, one warrant and six human-source operations. SIRC assessed the Service's compliance with the *CSIS Act*, Ministerial Direction and operational policy by examining key operational activities. SIRC found that, based on the information in the Service's possession, CSIS had reasonable grounds to suspect that the authorized targets of investigation posed a threat to the security of Canada. The level and intrusiveness of the Service's investigation were proportionate to the suspected threat.

There were no recommendations arising from this study.

REVIEW OF ACTIVITIES AND INVESTIGATIONS IN A CSIS REGIONAL OFFICE

SIRC endeavours each year to undertake a comprehensive review of CSIS's activities in a particular region. This type of review looks at the targeting of individuals, implementation of warrant powers, use of human sources, as well as cooperation and exchanges of information with Canadian and foreign partners. SIRC also reviewed CSIS's internal security measures for the region, as well as any security violations and breaches between April 1, 2000–March 31, 2003.

Overall, the region's investigative activities during the review period complied with the *CSIS Act*, Ministerial Direction and operational policy. SIRC found that CSIS had reasonable grounds to suspect the authorized targets of investigation posed a threat to the security of Canada, and that the intrusiveness of the techniques used were proportionate to the suspected threat these targets posed.

During the review, SIRC's attention was drawn to the involvement of certain targets in a local organization—one that had multiple functions. Based on this, the Committee

found that the organization had a dual function. SIRC believes operational policy governing investigations that have an impact on, or appear to have an impact on one function should apply to this organization. CSIS disagreed with this finding.

The Committee recommended that CSIS define a term in its operational policy.

REVIEW OF A COUNTER-PROLIFERATION INVESTIGATION

This study examined the Service's investigation of the threat to Canadian security posed by activities related to the proliferation of weapons of mass destruction by persons or organizations linked to a certain country.

SIRC found that the Service complied fully with Ministerial Direction and operational policy with respect to applications for targeting authorization and approvals for each of the investigations reviewed by SIRC. The Committee concluded that the Service 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 investigation was proportionate to the suspected threat. CSIS collected only information strictly necessary to fulfill its mandate.

SIRC endorsed the Service's approach of engaging relevant private-sector entities, undertaken via the Liaison Awareness Program (LAP). The Service met all of the requirements of the *CSIS Act* and operational policy with respect to warrant acquisition. SIRC concluded that one CSIS regional office did not comply fully with policy requirements concerning the timely provision of verbal and written tasking to the employee responsible for monitoring intercepted communications. CSIS adhered to policy requirements and Ministerial Direction in the management of the human-source operations reviewed. Overall, the Service's cooperation and exchanges of information with domestic and foreign partners complied with operational policy.

There were no recommendations arising from this review.

REVIEW OF CSIS'S INFORMATION OPERATIONS CENTRE

SIRC undertook its first-ever review of CSIS's investigation of threats against Canada's critical information infrastructure. It did so with two objectives. First, SIRC reviewed the role of the Information Operations Centre (IOC) in investigating threats against Canada's critical information infrastructure. Second, the Committee reviewed the IOC's operations, examining one counter-intelligence investigation of an information operation for compliance with the *CSIS Act*, Ministerial Direction and Service operational policies.

Notwithstanding two concerns identified below, SIRC found that in carrying out its duties and functions, the Service complied with the *CSIS Act*, Ministerial Direction and CSIS operational policies. SIRC's first concern was that operational policy keep pace with the matter reviewed.

SIRC recommends that the Service review operational policy to ensure that it clearly incorporates certain matters in relation to Section 12 targeting.

The Committee's second concern was related to administrative errors.

SIRC recommends that the Service review operational policy to ensure that if it is necessary to cross-reference operational database reports recorded under one file number with reports recorded under another file number, this should be noted in the "Investigator's Comments" section of the reports.

REVIEW OF CSIS'S EXCHANGES OF INFORMATION WITH CLOSE ALLIES

The case of Mr. Arar focussed public attention on the use of information that may have been collected in Canada and then shared with Canada's foreign partners. The Committee decided to undertake its first in-depth examination of CSIS's exchanges of information with close allied partners. Drawing on one of the Service's counter-terrorism investigations, SIRC chose to review CSIS's information exchanges with four allied agencies as the focus of the detailed review.

In the context of the investigation that was reviewed, SIRC found that the Service's exchanges of information with allied agencies were in accordance with respective foreign arrangements and complied with the *CSIS Act*, Ministerial Direction and operational policy. The Committee also found that the Service exercised due diligence in exchanging information about targets of investigation.

While the Service obtained appropriate approval prior to disclosing information to selected allied agencies, SIRC found that operational policy should accurately reflect which managerial level is accountable for information exchanged with foreign agencies.

SIRC recommended that CSIS amend operational policy to indicate clearly the managerial level accountable for disclosures to foreign agencies.

In this study, SIRC also examined how human rights were addressed within the context of foreign arrangements. When CSIS initiates the process to enter into a new arrangement with a foreign agency, it informs Foreign Affairs Canada and the Minister of Public Safety and Emergency Preparedness that it will “closely scrutinize the content of the information provided to, or received from, a foreign agency in order to ensure that none of the information sent to, or received from, that agency is used in the commission of, or was obtained as a result of, acts that could be regarded as human rights violations.” However, the Committee concluded that CSIS was not in a position to provide such an absolute assurance.

SIRC recommended that CSIS revise the content of the letters to Foreign Affairs Canada and the Minister of Public Safety and Emergency Preparedness to avoid leaving any impression that it can guarantee that information sent to, or received from, a foreign agency was not used in the commission of, nor was obtained as a result of, acts that could be regarded as human rights violations.

REVIEW OF A COUNTER-INTELLIGENCE INVESTIGATION

SIRC examined this counter-intelligence investigation for the period January 1, 2003, to December 31, 2003. The objective was to assess the Service’s compliance with the *CSIS Act*, Ministerial Direction and all relevant operational policies.

Overall, the counter-intelligence investigation was in compliance with the *CSIS Act*, Ministerial Direction and operational policy during the review period. SIRC found that CSIS had reasonable grounds to suspect that the authorized targets of investigation posed a threat to the security of Canada. Moreover, the Committee found that the intrusiveness of the techniques used were proportionate to the suspected threat that these targets posed. CSIS investigators only collected information that was strictly necessary for the investigation. They also acted appropriately and within the law in their use of human sources.

Throughout the review, SIRC paid particular attention to CSIS’s investigation of interference activities. SIRC found that CSIS’s operational policies covering these types of situations were incomplete. Because of this, the Committee recommended that:

CSIS review and amend, where appropriate, its operational policies relating to specific institutions to ensure that they cover all aspects of a given process.

TERRORIST FINANCING ACTIVITIES IN CANADA

The objective of this study was to examine CSIS's investigation of terrorist financing activities in Canada for in-depth review. SIRC selected one issue-based target, and five specific targets. In each case, the Committee assessed the Service's compliance with the *CSIS Act*, Ministerial Direction and operational policy.

The Committee concluded that the Service had reasonable grounds to suspect that the activities of targeted individuals and groups posed a threat to the security of Canada. The level and intrusiveness of the Service's investigation were proportionate to the suspected threat, and CSIS collected only that information necessary to fulfill its mandate. The Service's activities complied with the *CSIS Act*, Ministerial Direction and operational policy.

SIRC was satisfied with the degree and nature of the Service's cooperation with domestic and foreign partners.

It is possible that the Service may be required to collect and analyze information regarding an entity that meets the definition of a *listed person or group* under the *United Nations Suppression of Terrorism Regulations* (UNSTR), but does not represent a *threat to the security of Canada* under Section 12 of the *CSIS Act*. Further, SIRC noted that the UNSTR does not specifically direct the Service to participate in the listing process, nor has the Minister of Public Safety and Emergency Preparedness provided CSIS with specific direction to that effect.

There were no recommendations arising from this study.

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

SIRC sought to determine whether exchanges of information from this post with foreign agencies were within the scope of the government-approved liaison agreements in place. The Committee also assessed the operations at the security liaison post in relation to the *CSIS Act*, Ministerial Direction, and the Service's operational policies and procedures.

For context, SIRC also reviewed this post's operations, and evaluated them against issues raised in SIRC's ongoing statutory reviews of CSIS's Foreign Arrangements. Moreover, the report considered trends identified in SIRC's SLO studies over the previous five years.

SIRC was concerned by the lack of updated CSIS documents to assess the liaison relationships at the post. While there are written guidelines for the creation, submission and updating of these documents, there are no formal CSIS policies governing this activity. The Committee made the following recommendation:

The Committee recommended that the Service create policies for the preparation, updating and annual submission of CSIS documents used to assess the scope of exchanges with foreign agencies.

REVIEW OF FOREIGN ARRANGEMENTS

Under Section 17(1) of the *CSIS Act*, the Service may enter into an arrangement with the government of a foreign state, or an international organization of states (or an institution thereof), for the purpose of performing its duties and functions. Section 38(a)(iii) of the *CSIS Act* directs SIRC to review all such arrangements. During 2004–2005, SIRC undertook its first comprehensive review of the expansion process. An enhancement or expansion occurs when the Service changes an existing arrangement. This defines the subject matter and extent of authorized exchanges.

SIRC found that CSIS complied with the conditions set out in Ministerial Direction and operational policy regarding the expansion of the ten existing foreign arrangements. With respect to expansion approvals, SIRC noted that the Service has no operational policy on what type of information must be contained in the request submitted to the Director. The Committee also noted that the assessment of agencies with whom the Service has arrangements were not always submitted on a yearly basis as required in the Foreign Liaison Post Procedures Manual.

There were no recommendations arising from this review.