



SECURITY INTELLIGENCE  
REVIEW COMMITTEE

# SIRC Annual Report 2005–2006

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  
[www.sirc-csars.gc.ca](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 2006

Cat. No. PS105-2006

ISBN 0-662-49440-7



SECURITY INTELLIGENCE  
REVIEW COMMITTEE

# **SIRC Annual Report 2005–2006**

**An operational review of the  
Canadian Security Intelligence Service**



Photo: Couvrette/Ottawa

Members of SIRC (from left to right):  
The Honourable Baljit S. Chadha, The Honourable Gary Filmon (Chair), The Honourable  
Raymond Speaker, The Honourable Aldéa Landry, The Honourable Roy Romanow

September 29, 2006

The Honourable Stockwell Day, P.C., M.P.  
Minister of Public Safety  
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 2005–06, for your submission to Parliament.

Yours sincerely,



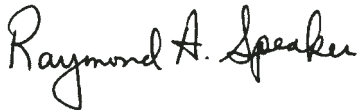
Gary Filmon, P.C., O.M.  
Chair



Baljit S. Chadha, P.C.



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



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



Aldéa Landry, P.C., C.M., Q.C.



## Table of contents

---

<b>Members' Statement</b> .....	v
<b>How this report is organized</b> .....	vii
<b>Section 1: A year in review 2005–06</b> .....	1
<b>A. Reviews of CSIS security intelligence activities</b> .....	3
How SIRC carries out its review function .....	3
SIRC reviews in 2005–06 .....	5
Review of a counter-terrorism investigation (# 2005–01) .....	5
CSIS liaison with foreign agencies: review of a security liaison post (# 2005–02) .....	7
Review of the Integrated Threat Assessment Centre (# 2005–03) . . .	9
Review of a counter-intelligence investigation (# 2005–04) . . . . .	11
Review of foreign arrangements with countries suspected of human rights violations (# 2005–06) .....	12
Review of CSIS's electronic-surveillance and information-gathering techniques (# 2005–07) .....	15
Review of activities and investigations in a CSIS region (# 2005–08) .....	17
<b>B. Investigation of complaints</b> .....	18
How SIRC investigates complaints .....	18
New procedures .....	22
SIRC complaint decisions in 2005–06 .....	22
Report on the investigation into the complaint in the matter of Bhupinder Liddar (Report #1) .....	22
Denial of security clearance (Report #2) .....	23
Alleged discrimination (Report #3) .....	24
Alleged improper response to a complainant's illness (Report #4) .....	25

<b>Section 2: CSIS accountability mechanisms</b> . . . . .	29
<b>A. Reporting requirements</b> . . . . .	31
CSIS Director's Annual Report (2004–05) . . . . .	31
Certificate of the Inspector General (2005) . . . . .	32
Unlawful conduct by CSIS . . . . .	32
Disclosures of information . . . . .	33
<b>B. Section 17 arrangements</b> . . . . .	34
Arrangements with domestic agencies . . . . .	34
Arrangements with foreign agencies . . . . .	35
<b>C. Policy and governance framework</b> . . . . .	36
National Requirements for Security Intelligence . . . . .	36
Ministerial Direction . . . . .	36
Changes in CSIS operational policy . . . . .	37
Governor-in-Council regulations and appointments . . . . .	37
<b>D. CSIS operational activities</b> . . . . .	37
Counter Intelligence Branch . . . . .	38
Counter Proliferation Branch . . . . .	39
Counter Terrorism Branch . . . . .	39
Research, Analysis and Production Branch . . . . .	40
Security Screening Branch . . . . .	41
Foreign Liaison and Visits Branch . . . . .	46
Federal Court warrants and warrant statistics . . . . .	47
Integrated Threat Assessment Centre . . . . .	49
<b>Section 3: Want to know more about SIRC?</b> . . . . .	51
Committee membership . . . . .	53
Staffing and organization . . . . .	54
Budget and expenditures . . . . .	55
Inquiries under the <i>Access to Information</i> and <i>Privacy Acts</i> . . . . .	55
Communications . . . . .	56
Modern comptrollership . . . . .	57
<b>Appendix A: SIRC reviews since 1984</b> . . . . .	59
<b>Appendix B: Recommendations</b> . . . . .	71



# Members' Statement

---

As the 21<sup>st</sup> century unfolds, the spectre of terrorism has become the major preoccupation of police and national security agencies. Even in those countries that have not suffered direct attacks, terrorism has sowed fear and uncertainty. The challenge for Canada is to ensure public safety without compromising the values that are the bedrock of our democratic tradition.

The Security Intelligence Review Committee (SIRC) is one of the organizations responsible for maintaining that balance. It is the only independent, external body equipped with the mandate to review the activities of the Canadian Security Intelligence Service (CSIS), by examining its operations and investigating complaints. For over two decades, SIRC has fulfilled this responsibility, always conscious of CSIS's vital role in safeguarding our society, but alert to the extraordinary powers that it is authorized to employ.

Our annual report summarizes, to the extent that national security permits, SIRC's key accomplishments in 2005–06. This year's report provides highlights of seven reviews as well as four decisions rendered in complaints cases. Among the more noteworthy reviews was an examination of CSIS's relationship with agencies in four countries suspected of human rights violations, plus our first review of the Integrated Threat Assessment Centre, a key component of Canada's National Security Policy. We also examined CSIS's electronic-surveillance and information-gathering techniques, to gain a better understanding of how rapidly evolving technologies are being used by CSIS and exploited by terrorists and foreign intelligence agencies. We made fourteen recommendations as a result of these seven reviews, which are summarized at the end of this report.

In addition to conducting reviews, SIRC is also responsible for investigating complaints against CSIS. In fulfilling this role, we provide an independent recourse mechanism for groups and individuals, with all the powers of a superior court. Over the past two decades, SIRC has issued 125 decisions related to complaints, each of which stands as a testament to our fairness and objectivity. In 2005–06, SIRC dealt with 63 complaints—a significant increase over recent years—and issued four new decisions. Among these is a Section 42 complaint concerning the denial of a security clearance to Mr. Bhupinder Liddar, where SIRC found in favour of the complainant.

Innovative procedures designed to modernize the complaints function are also highlighted in this year's report. In an effort to be more inclusive, we posted an Arabic translation of "How To Make A Complaint" on SIRC's website. In consultation with CSIS, we introduced pre-hearing conferences to resolve preliminary procedural matters and adopted the principle of continuing disclosure, so that new documents can be introduced at any time before a decision is rendered. We are proud of these innovations because they have streamlined our investigation process and over time, will help to ensure that SIRC's recourse mechanism is better understood.

Accountability is the *raison d'être* of review and oversight agencies around the world. That is why we felt it so important to contribute to the work of the O'Connor Commission, which is tasked with making recommendations on an independent, arm's-length review mechanism for the RCMP's national security activities. During the past year, our Chair discussed this subject at a public hearing of the Commission and SIRC staff held wide-ranging discussions with their Commission counterparts. Mr. Justice O'Connor's recommendations will likely focus considerable public attention on the adequacy of Canada's review mechanisms, and we will be very interested to see how the federal government responds.

**A society that bends the rules confirms the worst prejudices and suspicions of its enemies, while individual rights are meaningless without real and lasting human security.**

As stated previously, terrorism poses significant and continuing challenges to Canada and other western democracies. As free societies, we are compelled to use every available resource to counter this deadly threat, while at the same time upholding the principles of accountability, fairness, respect for individual rights and an absolute adherence to the rule of law.

If we can leave our readers with one message, it is this: do not assume that the demands of public safety and our democratic values are in an irreconcilable conflict with each other. In fact, they are complementary. A society that bends the rules confirms the worst prejudices and suspicions of its enemies, while individual rights are meaningless without real and lasting human security. That is why it is so important that police and national security agencies are held accountable for their actions and choices.

For twenty-two years, SIRC has strived to ensure real accountability by upholding Canadians' fundamental rights and freedoms and by insisting that CSIS act lawfully. This is our legacy and our continuing commitment to Parliament and the citizens we serve.

## How this report is organized

The Security Intelligence Review Committee provides assurance to the Parliament of Canada—and through it, to Canadians—that CSIS is acting lawfully 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. The second is to receive and investigate complaints by any person about any action of the Service.

SIRC's 2005–06 annual report is organized to reflect key findings and recommendations arising from its reviews and complaints investigations. Also included is more general background material, collected to inform Committee Members and to assist readers in understanding the broader context in which CSIS's security intelligence work is carried out. The report's three sections are summarized as follows:

### **Section 1: A year in review 2005–06**

This section summarizes seven reviews SIRC conducted during the period covered by this report. It also provides information about complaints received by SIRC.

### **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 contains information provided by CSIS on operational activities, plans and priorities, organized according to the Service's major branches.

### **Section 3: Want to know more about SIRC?**

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



## **Section 1**

---

**A year in review 2005–06**



## A year in review 2005–06

### A. Reviews of CSIS security intelligence activities

#### HOW SIRC CARRIES OUT ITS REVIEW FUNCTION

The Security Intelligence Review Committee is the only independent, external body equipped with the legal mandate and expertise to review the activities of CSIS. SIRC 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, SIRC seeks to ensure that the fundamental rights and freedoms of Canadians are respected.

To fulfill its mandate, SIRC directs staff to undertake a number of reviews each year. These provide a retrospective examination and assessment of specific CSIS investigations and functions. Under the *CSIS Act*, SIRC has virtually unlimited power to review CSIS's performance. 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 SIRC's findings and recommendations. Upon completion, the report is forwarded to the Director of CSIS and the Inspector General of CSIS.

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

#### What's the difference between an oversight and a review agency?

An oversight body looks on a continual basis at what is taking place inside an intelligence service and has the mandate to evaluate current investigations or work in "real time." SIRC is a review body, so unlike an oversight agency, it can make a full assessment of CSIS's past performance without being compromised by any involvement in its day-to-day operational decisions and activities.

SIRC's research program is designed to address a broad range of subjects. In deciding what to review, SIRC considers:

- priorities and concerns identified by Parliament or in the media;
- particular activities that could intrude on individual rights and freedoms;
- the CSIS Director's classified report to the Minister;
- the need to assess regularly each of the Service's branches and regional offices;
- SIRC's statutory authorities as detailed in the *CSIS Act*;
- events with the potential to cause threats to the security of Canada;
- commitments by SIRC to re-examine specific matters;
- issues identified in the course of SIRC's complaints function; and
- new policy directions or initiatives announced by CSIS or the Government of Canada.

This approach allows SIRC to manage the inherent risk of being able to review only a small percentage of CSIS activities in any given year. Each review results in a "snapshot" of the Service's actions in relation to applicable laws, policies and Ministerial Direction. Over the past two decades, SIRC's reviews have provided Parliament and Canadians with a comprehensive picture of the Service's operational activities, and assurance that CSIS is acting lawfully.

SIRC 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, the Inspector General of CSIS, central agencies, as well as the Auditor General, the Information Commissioner, and the Privacy Commissioner of Canada.



**SIRC REVIEWS IN 2005–06****Review of a counter-terrorism investigation**

---

**Report # 2005–01**

---

**Background**

This review focused on a CSIS investigation of a terrorist organization suspected of raising funds in Canada for its activities abroad.

**Methodology**

SIRC examined this investigation for the period from January 1, 2004–January 31, 2005. It reviewed hard-copy and electronic documentation pertaining to the following operational activities of the Service:

- the targeting of individuals suspected of engaging in threat-related activities, as well as the targeting-approval process;
- the direction of human sources against authorized targets;
- all exchanges of information with domestic partners; and
- advice to government.

**Findings**

Overall, the Service's activities were 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 targets of the investigation posed a threat to the security of Canada and that the targeting authorities were proportionate to the seriousness of the threats. CSIS investigators collected only information that was strictly necessary to the investigation.

Further, the Service's use of human sources and its exchanges of information with domestic partners complied with the *CSIS Act* and applicable Ministerial Direction. Although there were a few administrative errors in CSIS's management of sources, they did not affect the quality of the investigation, nor did SIRC see them as serious. SIRC also found that all reports CSIS distributed to senior government officials accurately reflected information in its operational reports.

SIRC was concerned about one exchange of information involving a foreign agency and noted a problem that arose as a consequence of a domestic partner's misuse of CSIS information.

SIRC also learned that CSIS's investigation of the terrorist organization brought it into contact with a sensitive Canadian institution.

CSIS has a mandate to investigate threats to the security of Canada, no matter how sensitive the venue in which those threats arise. Nevertheless, certain Ministerial Directions and operational policies require CSIS to take particular care when there is the possibility that its investigative activities will bring it into contact with a sensitive Canadian institution, which includes the academic, media, political, religious and trade union sectors.

In accordance with Section 2 of the *CSIS Act*, when investigating activities that pose a threat to the security of Canada, CSIS is prohibited from investigating those involving lawful advocacy, protest and dissent unless they are carried on in conjunction with threat-related activities. However, there are occasions when it will investigate groups or individuals who simultaneously engage in a legitimate political activity and a threat-related activity; who engage in a threat-related activity under the guise of a legitimate political activity; or who engage in a legitimate political activity that evolves into a threat-related activity.

These policies are more stringent than those governing other aspects of CSIS operations. They require that CSIS balance the use of intrusive investigative techniques against possible damage to civil liberties or to these fundamental societal institutions. This review identified an area where, in SIRC's opinion, operational policy needs to be expanded to cover CSIS's contact with the sector in question.

**SIRC therefore recommended that CSIS extend its sensitive sector policy to require senior-level approval for certain investigative techniques.** It is worth noting that SIRC made a similar recommendation in last year's annual report (see SIRC study # 2004–06).

## CSIS liaison with foreign agencies: review of a security liaison post

---

### Report # 2005–02

---

#### Background

CSIS maintains a number of Security Liaison Officer (SLO) posts outside Canada. With the exception of Washington, London and Paris, the location of these posts is classified. This year, SIRC reviewed one of the busiest of these posts, which receives thousands of messages annually and has numerous exchanges with foreign security and intelligence agencies located in that country.

#### Methodology

SIRC's objective was to determine whether the exchanges of information with the foreign agencies at this post were within the scope of the approved liaison agreements in place. SIRC also assessed whether activities at this post complied with the *CSIS Act*, with Ministerial Direction and with the Service's operational policies and procedures.

SIRC conducted this study by reviewing documents at CSIS Headquarters, as well as through on-site visits to the post. For context, the report also considered trends identified in previous SLO studies and SIRC's ongoing reviews of CSIS's foreign arrangements.

#### Findings

SIRC found that the SLO post in question was managed effectively and that its operations complied with the *CSIS Act*, Ministerial Direction, as well as with CSIS operational policy and guidelines.

#### SLOs:

- carry out regular liaison with foreign security and intelligence agencies;
- provide security screening services in support of Canada's immigration program;
- carry out the exchange of security intelligence information with approved agencies; and
- provide advice to senior staff of the Canadian Mission or Embassy.

SIRC made five recommendations.

First, SIRC reiterated a recommendation from its Section 54 report on Maher Arar—that **CSIS Security Liaison Officers should maintain a written record when requests for information from CSIS Headquarters are transmitted verbally to foreign intelligence agencies.**

The four remaining recommendations concerned issues related to the documentation used by CSIS to manage its foreign relationships.

**SIRC recommended that CSIS update the post profile.**

To ensure that CSIS Headquarters and SLOs are kept apprised of information exchanged with foreign partners, operational policy requires that CSIS employees submit a written report following a contact or visit with a representative of a foreign service. Not only are these reports important for managing CSIS's foreign relationships, they also help to keep the appropriate SLOs informed of discussions with foreign agencies and of information exchanged with their foreign counterparts. During the review period, such reports were not submitted regularly to CSIS Headquarters by the post. **SIRC recommended that CSIS Headquarters remind operational branches and SLOs to submit these reports in a timely fashion.**

**SIRC also recommended that CSIS produce an assessment document concerning a new relationship with a specific foreign agency, especially since CSIS Headquarters made the same request in 2003.**

Finally, with respect to CSIS's documentation of a separate and relatively new foreign arrangement with a particular intelligence agency, SIRC noted a lack of any written documentation regarding possible human-rights concerns cited by organizations such as Amnesty International and Human Rights Watch. As a result, **SIRC recommended CSIS develop an operational policy for documenting its relationships with agencies that are known or reputed to have engaged in human-rights abuse.**

## Review of the Integrated Threat Assessment Centre

---

### Report # 2005–03

---

#### Background

In April 2004, the Government of Canada announced *Securing an Open Society: Canada's National Security Policy*. One outcome was the establishment of the Integrated Threat Assessment Centre (ITAC) in July 2004, to ensure that terrorist threat assessments can be quickly transmitted to those decision-makers who need this information. It officially opened in October 2004.

ITAC allows for increased involvement by municipal and provincial authorities in evaluating and countering threats to Canada's national security. Located at CSIS Headquarters, ITAC is a functional component of the Service. It is governed by the *CSIS Act*, Ministerial Direction, CSIS operational policies, and is subject to review by SIRC.

Many within the security and intelligence community have adopted the term "fusion centres" when referring to the integration of all information relevant to the security and defence of a country.

ITAC brings together analysts, security experts, enforcement and intelligence officials from the Canada Border Services Agency, the Communications Security Establishment, the Department of National Defence, Foreign Affairs Canada, Privy Council Office, the Ministry of Public Safety, Transport Canada, Ontario Provincial Police, Sûreté du Québec, RCMP and CSIS.

The ITAC Director is appointed by the National Security Advisor to the Prime Minister, in consultation with the Director of CSIS. The current ITAC Director, seconded from the RCMP, was appointed in July 2005 for a two-year term. CSIS's role with respect to other ITAC partners is one of first among equals. The Service supplies the Centre's administrative, security and support services and administers its budget.

#### Methodology

This review was a foundation study to be used as a basis for future SIRC reviews. SIRC examined all available documentation concerning the formation and operations of ITAC, as well as its predecessor, the Integrated National Security Assessment Centre (INSAC).

SIRC was provided with all threat assessments produced by INSAC between February 2003 and July 2004, as well as ITAC threat assessments produced between October 2004 and February 2005. Of these, SIRC reviewed a sample of INSAC and ITAC reports to assess whether drafting, review and distribution processes complied with the *CSIS Act*, Ministerial Direction and operational policy.

### Findings

SIRC found that, for the most part, the Service complied with the *Act* as well as Ministerial Direction. However, SIRC also found that the Service had not yet integrated the operations of the Centre into existing operational policies or approved new ITAC-specific policies. **SIRC recommended that CSIS review its policies to determine where ITAC-specific amendments are required to address the role of this organization.**

ITAC produces assessments that warn the government about terrorist threats to Canada and to Canadian interests abroad. The Centre consults with its partners and clients in identifying specific topics, and with an advisory committee to develop its work plan. Each assessment integrates open-source and classified intelligence obtained from various domestic and foreign agencies. Classified information is extracted by ITAC staff on-site from partner agencies' respective electronic networks that hold criminal, intelligence and immigration information. SIRC found that ITAC's electronic capacity gives it unprecedented and far-reaching access to Canadian intelligence sources.

Once completed, ITAC's threat assessments are distributed to agencies and departments at the federal, provincial, territorial and municipal levels of government, as well as to Canadian law enforcement agencies. They are also provided to foreign agencies. SIRC found that most of these exchanges were conducted using approved CSIS cooperation agreements with foreign security and intelligence agencies. However, the Committee noted that CSIS was exchanging information with another foreign fusion centre without a Section 17 arrangement, as required under the *CSIS Act*. **SIRC recommended that CSIS formalize its relationship with this centre and seek an approved foreign arrangement from the Minister of Public Safety.**

ITAC also redistributes within the Canadian government the threat assessments produced by counterparts in the United States, the United Kingdom, Australia and New Zealand. These assessments accounted for almost three-quarters of all reports distributed by ITAC between October 2004 and August 2005. SIRC noted that, as of January 2005, ITAC was in the process of analyzing distribution problems and was studying its network to identify bottlenecks.

## Review of a counter-intelligence investigation

---

### Report # 2005–04

---

#### Background

SIRC examined a long-running counter-intelligence investigation, which was last reviewed in 1996. A foreign intelligence service was suspected of covert espionage and foreign interference in Canada, as defined by Sections 2(a) and 2(b) of the *CSIS Act*.

CSIS sought to identify which sectors or industries (aeronautical, telecommunications, military, scientific or technological) were being targeted by the foreign intelligence service. It also looked into suspected incidents of spying on expatriates who had relocated to Canada.

According to Section 2(a) of the *CSIS Act*, “espionage... that is against Canada or detrimental to the interests of Canada or activities directed toward or in support of such espionage” are threats to the security of Canada.

Section 2(b) defines foreign interference threats as “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.”

#### Methodology

SIRC’s review concentrated on the Service’s management of this investigation between January 2002 and December 2004, plus some material outside of the review period. This included hard-copy and electronic documentation related to targeting decisions and the management of human sources.

#### Findings

Overall, the counter-intelligence investigation complied with the *CSIS Act*, Ministerial Direction and operational policy during the review period.

SIRC concluded that:

- CSIS had reasonable grounds to suspect that this foreign intelligence service or its agents posed a threat to the security of Canada;
- the level and intrusiveness of the investigation were proportionate to that threat; and
- the Service only collected information strictly necessary to fulfill its mandate.

CSIS's investigation was terminated during the review period. SIRC noted that CSIS had thoroughly investigated all suspected espionage and foreign interference activities, and was satisfied that these were either unsupported by corroborative evidence or were isolated incidents. Further, the Service assured SIRC it was prepared to deal on a case-by-case basis with any future threats posed by the foreign intelligence service in question.

Based on the information available for its review, SIRC accepted the Service's evaluation that this foreign intelligence service no longer presented a threat to the security of Canada.

There were no recommendations arising from this review.

---

### **Report # 2005–05**

---

#### **Note:**

SIRC is currently working on review # 2005–05, but it had not been finalized at the time this annual report went to print. A summary of this review will appear in SIRC's 2006–07 annual report.

## **Review of foreign arrangements with countries suspected of human rights violations**

---

### **Report # 2005–06**

---

#### **Background**

The *CSIS Act* authorizes CSIS to enter into arrangements with foreign intelligence agencies for purposes of exchanging information concerning threats to the security of Canada. In cases involving countries that have a questionable commitment to human rights, Ministerial Direction stipulates that arrangements will be considered only if they are required to protect the security of Canada. Once an arrangement is established, CSIS continues to monitor the foreign agency's human rights record through annual assessments.

As provided under Section 38(a)(iii) of the *CSIS Act*, SIRC reviews these arrangements and monitors the information and intelligence that is exchanged. This year, SIRC chose to review CSIS's relationships with agencies from four countries suspected of human rights violations.



## Methodology

This study examined CSIS's foreign arrangements with seven foreign agencies, as well as information exchanged as a result of these arrangements.

For each foreign agency, SIRC examined:

- the rationale for establishing and—if applicable—expanding the arrangement;
- the relationship between CSIS and the agency;
- the nature of the information exchanged;
- special conditions or limitations on the collection or use of information; and
- an assessment of the intelligence disclosed to—and received from—the foreign agency.

The review covered the period January 1, 2002–December 31, 2004. Some information was also requested outside this period.

## Findings

Overall, SIRC found that CSIS's exchanges of information with these agencies were within the scope of the respective foreign arrangements, and that the Service complied with the *CSIS Act*, Ministerial Direction and operational policies.

However, SIRC did note some concerns. First, it found that, even though CSIS was fully compliant in providing certain information to a foreign agency, this could have contributed to that agency's decision to detain a Canadian citizen (who was also a CSIS target) upon arrival in that foreign country.

Second, SIRC was concerned that, even though CSIS was fully compliant in conducting the exchanges in question, information the Service received and used from a foreign agency may have been obtained under duress. SIRC also noted that questions submitted by CSIS to this agency via a third party may have been used in interrogating a Canadian citizen in a manner that violated his human rights. CSIS

had assessed both of these individuals as posing a threat and it obtained the necessary authority to launch investigations. However, it is outside SIRC's capacity to review whether other domestic or foreign agencies, who were also investigating these individuals, may have contributed to these individuals' detention and/or questioning.

SIRC believes that CSIS's policy framework should reflect the challenges of dealing with countries suspected of human rights violations.

Regarding information that could have been obtained through human rights violations, SIRC asked whether CSIS treated it differently than information received by other means. CSIS replied that it takes “no piece of information at face value and must find a way to independently corroborate the information before an assessment as to the reliability of the information is assigned.” CSIS further acknowledged that in most cases, it “will not know whether a piece of information originated from an abuse of human rights, [but] if suspected, the Service has to balance that against the need to secure information to protect Canadians and Canadian interests.”

CSIS noted that employees are expected to scrutinize closely the information received or exchanged with agencies in countries with questionable human rights records, and are encouraged to use due diligence when assessing the information obtained. While the Service indicated that human rights issues are taken into account during the exchange process, there is currently no specific operational policy requiring that it do so.

SIRC recognizes that for CSIS to safeguard Canada’s national security the Service must maintain relationships and exchange information with agencies around the world—some of whom have questionable human rights records. Nevertheless, SIRC believes that CSIS’s policy framework should reflect the challenges of dealing with countries suspected of human rights violations.

**SIRC recommended that CSIS amend its policy governing the disclosure of information to foreign agencies, to include consideration of the human rights record of the country and possible abuses by its security or intelligence agencies.**

As part of its review, SIRC also noted references to secure telephone conversations that took place between a Security Liaison Officer (SLO) stationed abroad and CSIS Headquarters. When SIRC inquired about the content of these conversations, the Service responded that there were no written records of these verbal discussions.

**As a result, SIRC recommended that CSIS Headquarters should maintain a written record of secure telephone conversations with SLOs—specifically conversations that contain operational information—and include this in its reporting.**

SIRC also learned that detailed discussions on the parameters and terms of arrangements are usually held between CSIS and the foreign agencies only after a foreign arrangement has been established. SIRC believes that these issues should be raised earlier in the process of establishing such arrangements.

**SIRC recommended that CSIS review its procedures so that the parameters and methods of exchange—as well as the Service’s expectations—are communicated to the foreign agency prior to entering into new foreign arrangements.**

## Review of CSIS's electronic-surveillance and information-gathering techniques

---

### Report # 2005–07

---

#### Background

When CSIS was created in 1984, there were fewer than ten major telephone companies operating in Canada, and it would be a decade before the Internet would become a household word. Since then, telecommunications services have grown exponentially, as have the online activities of Canadians.

Rapidly evolving technologies have resulted in dramatic changes to the types of techniques that can be used to conduct electronic surveillance. Advances in broadband and wireless communication are increasingly challenging the ability of CSIS and police to lawfully access information needed to ensure public safety. Currently Canadian telephone and Internet service providers are not required to build or maintain intercept capabilities in their networks. As a result, when a new technology is introduced, CSIS and the police often have to research and engineer unique and costly means of gaining lawful access to these networks.

The pace of technological change—and the speed with which terrorists and foreign intelligence agencies are adopting these innovations—means that Canadian law enforcement and security agencies must stay abreast of new developments. So too must SIRC, to continue to perform its review function.

Section 21(3) of the *CSIS Act* permits the Service, with the authorization of a Federal Court judge, to “intercept any communication or obtain any information, record, document or thing.” However, Canada is one of the few G-8 countries that does not have legislation outlining mandatory requirements for companies to provide interception capability. The proposed *Modernization of Investigative Techniques Act* would have addressed this deficiency.

Some groups expressed concern about the impact that this proposed legislation could have had on privacy rights in Canada. SIRC believes that these concerns could be accommodated, however, in a modernized legislative framework, bringing Canada in line with other close

The Government of Canada introduced the *Modernization of Investigative Techniques Act* in November 2005, but the bill only received its first reading before Parliament was dissolved prior to the federal election. Similar legislation has, however, been in place for several years in other countries, including the United States, the United Kingdom and Australia. More information is available at the Public Safety website ([www.psepc-sppcc.gc.ca](http://www.psepc-sppcc.gc.ca)).

allies. It is worth noting that a 2006 public opinion survey suggested that 49 percent of Canadians believe that police and intelligence agencies should have more powers to ensure security, even if it means Canadians have to give up some personal privacy safeguards.<sup>1</sup>

### Methodology

SIRC reviewed two warrant applications approved by the Federal Court in 2004, one for a counter-intelligence investigation and the other for a counter-terrorism investigation. SIRC examined hard-copy and electronic documentation pertaining to each of the warrant applications, as well as the implementation of warrant powers against authorized targets.

### Findings

SIRC found that the Service complied with the *CSIS Act* and all relevant operational policies in its application for, and execution of, warrant powers in support of the counter-intelligence investigation.

Contrary to operational policy, SIRC found that CSIS continued to collect information on a counter-terrorism target for a short period of time after terminating its investigation. CSIS confirmed, however, that it did not process this information and that it subsequently deleted the information. In addition, SIRC was unclear why CSIS believed that warrant powers were necessary to investigate another counter-terrorism target.

SIRC also noted some administrative delays within CSIS in submitting documents related to the implementation of warrant powers against certain counter-terrorism targets. It also found that several other warrant implementation files did not contain all the documents required by operational policy.

SIRC agreed with CSIS that different situations may require different types of documentation and that these requirements may change over time. In the interest of accountability and efficiency, however, **SIRC recommended that CSIS review and revise the warrant policy in question so that it reflects current best practices.** Pursuant to this recommendation, the Service has undertaken to revise its policy in this regard.

---

<sup>1</sup> *Security Monitor (Wave 6)*, Ekos Public Opinion Research, (June 2006), page 16.

## Review of activities and investigations in a CSIS region

---

### Report # 2005–08

---

#### Background

SIRC frequently reviews CSIS's activities in a particular region of Canada. These regional reviews provide insights into how investigations authorized by CSIS Headquarters are implemented in the field, and help SIRC to gain a better understanding of a region's activities, priorities and challenges.

This regional review was timely as it allowed SIRC to examine the first warranted investigation of a new and emerging threat within Canada: homegrown Islamic extremism.

#### Methodology

With respect to the warranted investigation, SIRC assessed the Service's compliance with the *CSIS Act*, Ministerial Direction and relevant operational policy by examining CSIS's:

- acquisition and execution of warrant powers, along with special operations;
- targeting approval process and investigation of targets;
- recruitment, development and tasking of human sources;
- cooperation, liaison and exchanges of information with domestic partners; and
- internal security measures and procedures.

This review covered the period January 1, 2002 to December 31, 2004.

#### Findings

SIRC agrees with the Service's assessment that homegrown Islamic extremism is a serious threat to national security. CSIS's investigations identified several individuals involved in planning terrorist acts, or engaged in fundraising, recruitment and training. SIRC found that the region's description of threat-related activities in its requests for warrants accurately reflected the information held by the Service. Further, the scope of warrant powers requested and subsequently exercised by the Service were appropriate to the threat, and complied with the *CSIS Act*, all Federal Court conditions, as well as the Service's own operational policies.

Although human sources were handled effectively, SIRC observed that there was a lack of coordination regarding joint handling of a source by two regions. SIRC also found that one source was directed against targets within a sensitive institution prior to appropriate approval having been secured, although approval was soon granted thereafter.

SIRC had concerns about the use of a certain interception technique used by the Service and **recommended that CSIS obtain an updated legal opinion governing the use of this particular technique.**

A review of internal security measures, including violations and breaches, is a standard part of every regional review. SIRC found internal security issues were dealt with appropriately in the region, with the exception of a district office, where potential violations were not documented. Although SIRC was assured that other internal safeguards would have prevented any violation, **SIRC recommended that existing operational policy be strictly adhered to by all regions, regardless of location, size or staff complement.**

## B. Investigation of complaints

### How SIRC investigates complaints

In addition to its review function, SIRC is responsible for investigating complaints from the public about CSIS. Almost all complaint cases begin as inquiries to SIRC— either in writing, in person or by phone. SIRC staff respond promptly to such inquiries, usually instructing the prospective complainant about what the *CSIS Act* requires for their concern to become a formal complaint. Once a written complaint is received, SIRC conducts an initial review.

SIRC has all of the powers of a superior court, and has access to all information that might be in the possession of CSIS, except for Cabinet confidences.

Where a complaint does not meet certain statutory requirements, SIRC declines jurisdiction and the complaint is not investigated. If jurisdiction is established, complaints are investigated through a quasi-judicial hearing presided over by one or more Committee members, assisted by staff. In investigating complaints, SIRC has all of the powers of a superior court, and has access to all information that might be in the possession of CSIS, except for Cabinet confidences.

A complainant has the right to be represented by counsel and to make representations at the hearing. Pre-hearings may be conducted to establish and agree on procedures with the complainant and/or the complainant's counsel. SIRC's Senior Counsel provides legal advice on procedural and substantive matters, and will also cross-examine Service witnesses when, for national security reasons, evidence must be heard without the complainant being present.

At the completion of a hearing, SIRC prepares a report with findings, including any recommendations SIRC considers appropriate. This report is sent to both the Minister of Public Safety and the Director of CSIS. Any information with national security implications is removed from the version of the report that goes to the complainant. Summaries of these reports, edited to protect national security and the privacy of complainants, are also included in SIRC's annual report to Parliament.

## Types of complaints

Four kinds of matters may be investigated by SIRC:

- 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 allegations made to it; and
- Minister's reports in regards to the *Citizenship Act*.

The types of complaints that SIRC investigates are described in the *CSIS Act* and take several forms. Under Section 41 of the *Act*, SIRC can investigate “any act or thing” done by the Service. Under Section 42, it can hear complaints about denials of security clearances to federal government employees and contractors (*see “Determining jurisdiction of a complaint under Section 41 and 42”*). Section 42 does not permit SIRC to accept jurisdiction to hear complaints concerning less intrusive background screening or reliability checks, which are generally conducted simply to determine the trustworthiness or suitability of a potential federal employee. These complaints are addressed through an organization's designated grievance procedure.

Under the *CSIS Act*, individuals who have been denied a security clearance must be informed of this action by the Deputy Head of the organization. These individuals have the right to make a complaint to SIRC, and where appropriate, it will investigate and report its findings and any recommendations to the Minister, the Director of CSIS and the Deputy Head. SIRC also provides the complainant with a report of its findings, taking into consideration the obligation to protect classified information.

Should the Canadian Human Rights Commission receive a written notice from a Minister of the Crown about a complaint that relates to the security of Canada, the Commission may refer the matter to SIRC. Upon receipt of such a referral, SIRC carries out an investigation and reports its findings to the Commission, the respondent and the complainant. SIRC also has the authority to conduct investigations into matters referred to SIRC pursuant to the *Citizenship Act*.

### Determining jurisdiction of a complaint under Section 41

Under Section 41 of the *CSIS Act*, SIRC shall 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 in writing to the Director of CSIS and not have received a response within a reasonable period of time (approximately 30 days), or the complainant must be dissatisfied with the response; and
2. SIRC must be satisfied that the complaint is not trivial, frivolous, vexatious or made in bad faith.

Under Section 41(2) of the *Act*, SIRC cannot investigate a complaint that can otherwise be addressed under existing grievance procedures of the *CSIS Act* or the *Public Service Labour Relations Act* (formerly known as the *Public Service Staff Relations Act*).



## Determining jurisdiction of a complaint under Section 42

With respect to decisions by federal deputy heads to deny security clearances, Section 42 of the *CSIS Act* says SIRC 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 may extend this period if valid reasons are presented.

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 SIRC's jurisdiction or investigated and resolved without a hearing (i.e., administrative review).

**Table 1**  
**Resolution of complaints\***

	2003–04	2004–05	2005–06
Carried over	17	16	18
New	30	30	45
<b>Total</b>	<b>47</b>	<b>46</b>	<b>63</b>
Closed	31	28	39
Carried forward to subsequent year	16	18	24
Reports issued	1	3	4

\* This reflects all complaints received by SIRC. Not all complaints resulted in an investigation. Some were redirected to another government institution, or were determined to be outside SIRC's jurisdiction. Others were withdrawn by the complainants.

### **New procedures**

During 2005–06, SIRC developed in consultation with CSIS new practices to streamline the complaints investigation process and ensure procedural fairness.

First, revisions were made to the way in which documents are disclosed to SIRC by the Service. It is important to note that SIRC's access to information in this area is limited only by Subsection 39(3) of the *CSIS Act*, which states that CSIS may withhold Cabinet confidences from SIRC. New procedures have been adopted based on the principle of continuing disclosure, as provided for in Subsection 226(1) of the *Federal Court Rules*, as well as in Subsection 6(5) of the *Canadian Human Rights Tribunal's Rules*. It allows SIRC to be notified by CSIS in a timely manner when the Service becomes aware of documents relating to a complaint that have not previously been made available to SIRC.

Another innovation is the “pre-hearing conference.” Introduced in January 2006, this conference is conducted by a presiding Member of SIRC with all parties in attendance to resolve preliminary procedural matters (e.g., allegations to be investigated, the identity and number of witnesses to be called). Provided that no issues of national security are raised, the conference can be conducted by telephone and a transcript is later provided to the parties.

As of March 31, 2006, four pre-hearing conferences had been held by SIRC.

### **SIRC complaint decisions in 2005–06**

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

## **Report on the investigation into the complaint in the matter of Bhupinder Liddar**

### **REPORT #1**

A complaint was filed with SIRC under Section 42 of the *CSIS Act* after the complainant, Mr. Bhupinder Liddar, was denied a security clearance, based on a recommendation (referred to as a “denial brief”) by CSIS.

After reviewing the complaint, SIRC found there was no reasonable basis for that recommendation, and that it was inaccurate and misleading for several reasons.

First, SIRC concluded that the denial brief contained an unfair and prejudicially inaccurate account of the information that the Service had in its possession when it began the security clearance investigation. Next, SIRC concluded that the brief was based on a field investigation conducted by an inexperienced CSIS investigator, who arrived at unfounded conclusions.

SIRC found that there was no reliable evidence to support a conclusion that the complainant might engage in activities that would constitute a threat to the security of Canada, or that the complainant might disclose classified information in an unauthorized way.

SIRC recommended that:

- **The Deputy Head of the relevant federal department/agency grant the complainant the requested security clearance; and**
- **CSIS institute procedures to ensure that accurate notes are taken, or that a recording is made, of security screening interviews. These should be kept for five years after an interview, or for even longer periods should an interviewee challenge the outcome of a security screening investigation.**

In response to this latter recommendation, CSIS informed SIRC in December 2005 that it had revised its practices concerning note-taking and consensual recording of interviews. Investigators are now required to make an offer to record an interview of a subject when conducted for government security screening. The Service will continue its requirement to prepare an accurate, complete report of the proceedings, regardless of whether the subject consents to the interview being recorded.

## Denial of security clearance

### REPORT #2

SIRC reported a second decision that was also pursuant to Section 42 of the *CSIS Act* concerning the denial of a security clearance.

SIRC found that the decision to deny the security clearance was made on incomplete and at times incorrect information. Some corroborated information that was favourable to the complainant was not included in the denial brief. Moreover, SIRC found that concerns identified by the employing department about the complainant's loyalty and reliability were not supported by the evidence presented during the complaints hearing.

SIRC also found that there was a lack of procedural fairness in this case by the employing department, since the complainant was not able to respond to the allegations prior to the decision to deny the security clearance. The complainant was not made aware by the employing department of the reasons for the denial, including the security concerns identified by CSIS.

SIRC recommended that:

- **the complainant be granted the requested security clearance;**
- **CSIS should verify or corroborate security clearance information provided by an applicant or by sources when it can be done easily;**
- **the employing department/agency should clarify its procedures so that an individual in these circumstances is provided with information concerning any adverse findings by CSIS. This should be done in a manner that respects national security, but provides the individual with an opportunity to know the reasons for a denial of security clearance;**
- **both CSIS and the employing department/agency give consideration to recent remarks by the Privacy Commissioner—that as law enforcement and national security agencies collect more information from more sources, there is a greater chance that information of questionable accuracy could influence decisions or be taken out of context<sup>2</sup>;**
- **the Minister responsible for the employing department/agency write to and inform the complainant’s former Member of Parliament that—contrary to earlier information—there was no evidence that the complainant’s character or past association would affect the individual’s suitability to be granted a security clearance at any level; and**
- **the employing department/agency take measures to ensure the quality and the accuracy of information that is transcribed from hand-written personal history forms.**

## Alleged discrimination

### REPORT #3

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

---

<sup>2</sup> See Office of the Privacy Commissioner, *Annual Report to Parliament (2004): Report on the Personal Information Protection and Electronic Documents Act*, (page 15).

The complainant—a former CSIS employee—was suffering from an illness that meets the definition of disability as provided under the *CHRA*. It was alleged that the Service had failed to accommodate the complainant's disability, and instead allegedly took advantage of that disability to obtain statements and cause termination of employment. It was further alleged that CSIS had refused the complainant's request for an extension of the 25-day limit for appealing or grieving a dismissal.

SIRC found that the complainant, when working for CSIS, was suffering from a disability consistent with Section 7 of the *CHRA*. SIRC also concluded that there was evidence the Service either knew or ought to have known that the complainant was suffering from a disability.

SIRC determined that the complainant was treated in an adverse manner by CSIS because CSIS relied on statements previously made by the complainant as the grounds for the termination of employment. Therefore, SIRC agreed that the complainant presented a legitimate case of discrimination on a ground prohibited by the *CHRA*. The Committee maintained that CSIS should have accommodated the complainant by requesting a health review, and should have provided the complainant with an opportunity to respond to allegations prior to termination of employment.

SIRC recommended that:

- **CSIS's human resources policies on Health Review be amended to require supervisors and other staff to inform their managers or the manager of an employee in question when they have reason to believe that an employee is in need of medical assistance;**
- **the Service allow the complainant to submit a grievance; and**
- **should the Canadian Human Rights Commission investigate the complainant's allegations, the CHRC should not publicly release any information identified in SIRC's report that is subject to national security considerations.**

## **Alleged improper response to a complainant's illness**

### **REPORT #4**

SIRC 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 complainant—a former CSIS employee—alleged that CSIS had:

- pressured the complainant to remain in the workplace and to confess to actions that this individual did not commit;
- breached the Employees Assistance Program’s (EAP) code of confidentiality; and
- failed to assist the complainant when in need of medical treatment.

SIRC found that the cumulative effect of the stress and exhaustion, combined with the uncertainty of the outcome of the disciplinary process, induced the complainant to remain in the workplace, and to make incriminating statements in circumstances that rendered the statements unreliable. SIRC further maintained that CSIS failed to both assess the reliability of the complainant’s confession and provide the complainant with an opportunity to respond to a new alleged infraction prior to termination of employment.

SIRC found that a reasonable person would interpret the actions of CSIS’s Chief of Health Services—who was responsible for the EAP—as “counselling” with respect to the complainant. As a result, SIRC found that the code of confidentiality was breached when the Chief of Health Services brought an investigator to take a statement from the complainant.

SIRC recommended that the Service:

- **add a note to the complainant’s personnel file, advising that certain statements by the complainant were obtained under circumstances such that the remarks should be considered unreliable;**
- **ensure that it follows the Breach of Conduct and Discipline Policy prior to discipline being imposed on an employee;**
- **create a policy to require that all pertinent information having an impact on the reliability of statements (e.g., competency of the person to make a free and voluntary statement) be included in all internal security investigation files;**
- **remind its employees that all their written records may be subject to the *Access to Information Act*, the *Privacy Act*, as well as to operational policy, and that these should only be disposed of in accordance with the Service’s disposal-of-records policies;**
- **create a policy to require that a written record be kept of an assessment by senior management regarding the reliability and relevance of oral and written statements before deciding how to conclude an internal security investigation;**

- post a notice at the offices of Health Services and on any website pertaining to the Service's EAP that any communication other than with a counsellor, as defined by the EAP policy, will not be subject to any code of confidentiality. Staff working for the EAP must declare to participants seeking assistance under the EAP that only communications with a counsellor will be subject to the code of confidentiality;
- amend its EAP policy to require that reasonable steps be taken to ensure any required consent provided by an employee is given freely and voluntarily, and that a record of those steps should be kept on the employee's file; and
- amend CSIS's human resources policies to require that supervisors and other staff inform their managers or the manager of an employee in question when they have reason to believe that an employee is in need of medical assistance.





## **Section 2**

---

### **CSIS accountability mechanisms**



## CSIS accountability mechanisms

### A. Reporting requirements

#### **CSIS DIRECTOR'S ANNUAL REPORT (2004–05)**

Every year, the Director of CSIS must submit a Top Secret report to the Minister of Public Safety, describing in detail the Service's priorities and operational activities. The *CSIS Act* requires that the Inspector General of CSIS examine this report and submit a certificate to the Minister, attesting to the extent to which he or she is satisfied with its contents. Finally, the Minister sends a copy of both documents to SIRC for its review, as required by Section 38(a) of the *CSIS Act*.

The 2004–05 Director's report stated that in supporting the Service's highest priority—public safety—CSIS is working to prevent a terrorist attack from either occurring or originating in Canada. The Director noted that this is having an impact on the agency's resources, and discussed the strategies being used to combat this challenge.

Attention was also drawn to a new dimension of the threat posed by Islamic extremism. While the threat from al-Qaida remains strongest overseas, a terrorist attack on Canadian soil is now considered probable. For the first time, CSIS also warned about the relatively new threat posed by homegrown converts.

The Director's report also noted that the Service continues to investigate attempts by foreign countries to conduct espionage and interfere with expatriate communities in Canada.

The report highlighted efforts by CSIS to strengthen its cooperation with domestic partners. The Service also reported having excellent relations with its key foreign partners, and that it had assisted foreign intelligence services in newly democratized states by providing training on the principles and techniques of intelligence collection.

The report included details about the Service's human sources and security screening programs, as well as a description of its compliance with Ministerial Direction and National Requirements from the Minister of Public Safety.

Readers should note that CSIS posts public, unclassified reports on its website ([www.csis-scrs.gc.ca](http://www.csis-scrs.gc.ca)).

**CERTIFICATE OF THE INSPECTOR GENERAL (2005)**

The position of Inspector General (IG) was established in 1984 under the *CSIS Act*. The IG functions as the “eyes and ears” of the Minister of Public Safety, reviewing the Service’s operations and providing assurance that CSIS is complying with the *CSIS Act*, Ministerial Direction and operational policy.

Every year, the IG submits a certificate to the Minister stating the extent to which he or she is satisfied with the CSIS Director’s Annual Report. The certificate informs the Minister of any instances of CSIS failing to comply with either the *Act* or Ministerial Direction, or an unreasonable or unnecessary exercise of powers.

In the latest certificate, the IG noted that the Director of CSIS had reported three incidents of non-compliance with operational policy for 2004–05. The IG looked into these incidents and found that appropriate action had been taken in each case. The IG also identified two additional cases of non-compliance. However, she indicated that the only corrective action required was “a greater degree of diligence in respecting the reporting requirements.”

The IG also expressed concern about several inaccuracies she identified in the Director’s report. Two concerned statistical errors but others were, in her view, more substantive. According to the certificate, the Service has acknowledged the inaccuracies and has advised the IG that corrective steps would be taken.

The IG concluded that there had been substantial improvements in the response time of the Service in assisting her office staff with their work. “The concerns raised above,” she added, “are not intended in any way to detract from the devotion or dedication of the Service or its employees to serve Canada and to counter threats to the security of the state.”

For more information, please refer to the Inspector General’s home page on the Public Safety website ([www.psepc-sppcc.gc.ca](http://www.psepc-sppcc.gc.ca)).

**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 his or her comments to the Attorney General of Canada and to SIRC.

In 2005–06, there were no activities requiring such a report.

## DISCLOSURES OF INFORMATION

Section 19 of the *CSIS Act* prohibits information obtained by the Service in the course of its investigation from being disclosed except in specific circumstances. Of note, Section 19(2)(d) gives the Minister of Public Safety the power to override any invasion-of-privacy concerns, authorizing the Service to disclose information deemed to be in the national or public interest. When such information is released, the Director of CSIS must submit a report to SIRC. In the past, there have been only two disclosures under this section of the *Act*. In 2005–06, CSIS reported to SIRC that there were no such disclosures of information.

The Service can also disclose information in written or verbal form to any law enforcement body or federal government entity, such as the Department of National Defence and Foreign Affairs Canada. When CSIS permits the use of its information by the RCMP for use in judicial proceedings, it must do so in writing.

A disclosure letter from CSIS permits the RCMP to use the Service's information to pursue a criminal investigation. Should the RCMP wish to use this information in a court of law, they must obtain an advisory letter from the Service granting them permission to do so.

The following table summarizes the Service's Section 19 disclosures by branch.

<b>Branch</b>	<b>Law enforcement (a)</b>	<b>Foreign Affairs Canada (b)</b>	<b>Department of National Defence (c)</b>	<b>Public interest (d)</b>
Counter Terrorism	293	0	4	0
Counter Intelligence	19	0	0	0
Counter Proliferation	23	1,340	2,353	0
<b>Totals</b>	<b>335</b>	<b>1,340</b>	<b>2,357</b>	<b>0</b>

(a) Disclosed under Section 19(2)(a)

(b) Disclosed under Section 19(2)(b)

(c) Disclosed under Section 19(2)(c)

(d) Disclosed under Section 19(2)(d)

## Conditions for disclosure of information by CSIS

Under Section 19(2) of the *CSIS Act*, there are four situations in which the Service may disclose information obtained in the performance of its duties and functions. These are defined 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 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.

## B. Section 17 arrangements

### ARRANGEMENTS WITH DOMESTIC AGENCIES

In carrying out its duties and functions, CSIS often collaborates with federal departments and agencies, provincial governments and law enforcement agencies. Since 9/11, more groups have become involved in national security, including police and non-governmental partners (especially concerning critical infrastructure). This creates a challenge for the Service, as it must cultivate and maintain healthy relationships with both new and existing partners to ensure that information is exchanged efficiently and that joint operations are conducted effectively.

From sharing information to conducting joint operations, domestic arrangements can take many forms. As of March 31, 2006, CSIS had 29 Memoranda of Understanding in place with domestic partners so that information could be exchanged. Of these, 17 were with federal departments or agencies, and 10 were with provincial and municipal entities (e.g., governments, agencies, police). Also of note, the arrangement with the National Security Advisor, established in 2004–05, was renewed for one more year.

Under Section 17(1) of the *CSIS Act*, the Service may, with the approval of the Minister of Public Safety, enter into an arrangement or otherwise cooperate with domestic agencies for the purpose of performing its duties and functions. Section 38(a)(iii) of the same Act authorizes SIRC to review all domestic arrangements.

### ARRANGEMENTS WITH FOREIGN AGENCIES

Section 17(1) of the *CSIS Act* states that the Service can enter into arrangements with foreign agencies to exchange information concerning threats to the security of Canada. New foreign arrangements require the approval of the Minister of Public Safety, in consultation with the Minister of Foreign Affairs. Even without such an arrangement, CSIS can still accept unsolicited information from an agency or organization of a foreign country.

The Service can also expand the scope of existing active arrangements, defining the subject matter and the extent of authorized exchanges. In the case of enhanced arrangements, the Director of CSIS is granted more discretion and has the authority to approve the expansion of activities without obtaining Ministerial approval, but subject to any Ministerial caveats or instructions that may have been imposed when the initial arrangement received approval.

SIRC reviews all new, enhanced or renewed foreign arrangements, as provided under Section 38(a)(iii) of the *CSIS Act*. To do so, it examines whether:

- CSIS's foreign arrangements were in compliance with the conditions set out in the *CSIS Act*, Ministerial Direction and operational policy;
- approvals from the Minister of Public Safety and the Director of CSIS were in place when the Service began exchanging information;
- the human rights record of the foreign agency's host country—including open-source reporting from human rights agencies—was considered; and
- the most recent agency assessment met CSIS guidelines.

In 2005–06, SIRC chose to review thirteen foreign arrangements with agencies in nine countries.

SIRC found that all foreign arrangements were in accordance with the *CSIS Act*, Ministerial Direction and operational policy.

SIRC also found that the Service had informed itself of the human rights situation in all the countries and agencies in question. Moreover, the Service had proceeded cautiously with exchanges of information involving countries with questionable human rights records, although SIRC will continue to monitor one particular arrangement.

Although two assessments were not submitted on an annual basis as required, SIRC noted an improvement concerning the annual submission of agency assessments and that, overall, these met the Service's guidelines.

## C. Policy and governance framework

### **NATIONAL REQUIREMENTS FOR SECURITY INTELLIGENCE**

Subsection 6(2) of the *CSIS Act* states that the Minister of Public Safety may issue written directions to the Director of CSIS. The document, entitled "National Requirements for Security Intelligence," outlines where the Service should focus its investigative efforts, and provides general direction to CSIS in its collection, analysis and advisory responsibilities. It is based on a Memorandum to Cabinet, prepared annually by CSIS for the Minister of Public Safety to present to his or her Cabinet colleagues.

In 2005–06, a Memorandum was reviewed and approved by Cabinet, but no National Requirements were issued. The Service informed SIRC that, in the absence of specific Ministerial Direction, it relied on the priorities approved by Cabinet, which would normally have served as the basis for the annual National Requirements.

### **MINISTERIAL DIRECTION**

Under Subsection 6(2) of the *CSIS Act*, the Minister of Public Safety may issue directions governing CSIS's activities and investigations.

No new directions were issued in the year under review.

This outcome is consistent with what SIRC had predicted in its 2000–01 annual report.<sup>3</sup> At that time, it foresaw that Ministerial Direction would likely not be

---

<sup>3</sup> *SIRC Annual Report 2000–01*, page 8.



updated regularly in the future. SIRC expected that increased emphasis on the Service's own operational policies would serve as the source for special instructions and guidelines for implementation.

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

CSIS operational policy embodies the rules which govern the range of activities that CSIS undertakes in doing its work. Operational policy is updated regularly in accordance with legislative and other changes. These updates are reviewed by SIRC to ensure that they conform to the *CSIS Act*, Ministerial Direction and existing operational policies.

In 2005–06, CSIS was preparing for a significant reorganization of its operations, implemented in May 2006. According to the Service, an evolving threat environment required that CSIS make these changes to increase operational capability, consolidate and enhance analysis functions and enhance corporate support.<sup>4</sup>

CSIS revised almost 50 policies in 2005–06, of which 40 were changes reflecting the government department name change from Solicitor General to Public Safety and Emergency Preparedness Canada. Other significant influences on policy included the Service's role in assisting Canadian military operations (for which CSIS is developing a new policy), as well as the expansion of intelligence collection by CSIS overseas.

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

Section 8(4) of the *CSIS Act* states that 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.

The Governor-in-Council did not issue any regulations in 2005–06.

## **D. CSIS operational activities**

The following section describes CSIS operational activities, and provides an overview of the priorities and achievements of each operational branch during 2005–06. This information provides a useful background that helps SIRC carry out its own work. It should be noted that many of the organizational units discussed below have changed as a result of the May 2006 reorganization.

---

<sup>4</sup> CSIS press release, May 1, 2006.

### COUNTER INTELLIGENCE BRANCH

The Counter Intelligence Branch focuses its operations on the hostile activities of foreign intelligence services known to be operating within Canada. The branch investigates threats to national security, including espionage and foreign-influenced activities (e.g., attempts to monitor, influence or coerce émigré communities in Canada). The branch is also responsible for investigating threats to Canadian economic security, specifically economic espionage, the clandestine acquisition of technologies and transnational criminal activity. For an example of a SIRC study in this area, see *Review of a counter-intelligence investigation (#2005–04)* in this annual report.

In 2005–06, the Service reported to SIRC that espionage activities in Canada are becoming steadily more complex and sophisticated. This is particularly true of cyber-based and other electronically-based attacks on Canadian targets. The branch reported that several successful operations were undertaken against the espionage activities of a number of foreign states.

CSIS also noted that this branch had received an increasing number of requests from other Canadian government departments to contribute its assessment and analysis on a range of issues. For example, the branch examined over 80,000 visa applications during the period under review, and successfully detected a number of known or suspected intelligence officers seeking entrance into Canada.

**Table 3**  
**Authorized targets (2005–06)**

Branch	Individuals	Organizations	Issues/events	Totals
Counter Intelligence	152	36	4	<b>192</b>
Counter Proliferation	55	6	6	<b>67</b>
Counter Terrorism	274	31	30	<b>335</b>
<b>Totals</b>	<b>481</b>	<b>73</b>	<b>40</b>	<b>594</b>

### **COUNTER PROLIFERATION BRANCH**

The Counter Proliferation Branch investigates activities related to the proliferation of weapons of mass destruction (WMD) through the development and procurement programs of foreign states of concern or terrorist organizations. The branch keeps a close watch on rogue states or groups who sponsor or commit acts of terrorism, as well as the activities of foreign intelligence services. The branch also examines the threat of chemical, biological, radiological and nuclear terrorism.

The branch reported a number of successes in its investigations, allowing the Service to play an important role in sharing intelligence with its foreign partners. It also expanded its intelligence collection activities on state-sponsored terrorism and participated in Canadian government efforts to identify covert attempts to transfer funds to international terrorist organizations.

The Counter Proliferation Branch also has units that assist other CSIS operations. These include the Threat Assessment Unit (TAU), which produces threat assessment reports on a wide range of topics, and the Immigration Assessment Unit, which liaises with the Canada Border Services Agency. TAU's assessments serve as an early warning mechanism to the government about threats to Canada and to Canadian interests abroad. In 2005–06, it produced 360 threat assessments—compared to 450 in the previous year.

### **COUNTER TERRORISM BRANCH**

The role of the Counter Terrorism Branch is to advise the Government of Canada on threats of serious violence that could affect the safety and security of Canadians and Canada's allies.

For the fifth year in a row, Islamic extremism—particularly al-Qaida-inspired or related—remains the main concern of this branch. Moreover, the Service believes that the threat posed by these terrorist groups has increased in 2005–06. A priority of the branch is the interdiction and removal of such radicals from Canada.

The Service initiated several new investigations of alleged foreign extremists or terrorist groups that may have infiltrated into Canada. The Service also identified several previously unknown domestic extremists involved in threat-related activities. In cooperation with other domestic agencies, the branch prevented a suspected foreign extremist from entering Canada, and disrupted a Canadian-based terrorist cell.

Many of the Counter Terrorism Branch's operations are conducted in cooperation with the RCMP. The Service advises the government on threats to Canada's national security and the RCMP investigates criminal activity that poses a similar threat. Under the *Anti-Terrorism Act* (2001), the role of the RCMP in combating international terrorism was enhanced, resulting in closer ties with CSIS in matters of national security. This has resulted in successful, collaborative intelligence gathering and technical operations.

CSIS reported to SIRC that while there remains some duplication of investigations, efforts are being made within each organization to address this matter. Also, as noted in previous annual reports, CSIS continues to participate in four of the RCMP's Integrated National Security Enforcement Teams (INSETS), located in several regions across Canada. Now in its fifth year of operation, this program is projected to expand to a fifth region in 2006.

The participating CSIS regions report positive working relationships with the teams. Close cooperation and regular communication have limited potential overlap between the mandates of both organizations.

### RESEARCH, ANALYSIS AND PRODUCTION BRANCH

The Research, Analysis and Production Branch produces security intelligence assessments to support the Service's operations and the Canadian government's decision-making in relation to threats to national security. It develops strategic and operational analyses of current threats and emerging issues. The *Intelligence Briefs*, *CSIS Reports* and *CSIS Studies* are the key documents prepared by this branch. CSIS produced 41 of these reports in 2005–06 and distributed them throughout the security intelligence community and to other clients.

For more information on the Terrorist Entity list, see the Public Safety website at [www.psepc-sppcc.gc.ca](http://www.psepc-sppcc.gc.ca). Readers should also refer to SIRC's study # 2004–03, summarized in SIRC's Annual Report for 2004–05.

As SIRC reported in its 2004–05 annual report, CSIS has a role in the Terrorist Entity Listing process, including developing Security Intelligence Reports (SIRs) that describe the grounds for listing an entity. These reports help the Minister of Public Safety decide whether to recommend to the Governor-in-Council to add a particular entity to the Terrorist Entity list.

In 2005–06, the branch produced nine SIRs. It also began its second two-year review of existing SIRs in the same period, to determine whether it is reasonable to maintain or to de-list an entity.

Finally, the branch supports CSIS's consultations with Foreign Affairs Canada on listing the names of persons or groups under Schedule 1 of the *United Nations Suppression of Terrorism Regulations* (UNSTR).

### SECURITY SCREENING BRANCH

One of the largest branches of CSIS, Security Screening has two program streams, government screening and immigration screening.

**Government screening**—CSIS performs security clearance investigations for all government employees<sup>5</sup> whose duties require access to classified assets or information. In each investigation, the Service provides requesting departments or agencies with a security assessment, which is an appraisal of an individual's reliability as it relates to loyalty to Canada. The largest clients of this service are Public Works and Government Services Canada (PWGSC) and the Department of National Defence (DND)—accounting for over 25 percent and 20 percent respectively of all requests in 2005–06.

As indicated in Table 4 below, CSIS received 42,100 requests for new or updated security clearances and provided 37,800 security assessments in 2005–06. Although the volume of requests increased by about 15 percent from the previous fiscal year, the number of security assessments issued by CSIS remained roughly the same, indicating that not all requests could be completed within the period under review.

**Table 4**  
**Government screening\***

	2003–04	2004–05	2005–06
Requests from DND	9,900	9,100	9,200
Requests from other departments or agencies	27,600	27,400	32,900
<b>Total</b>	<b>37,500</b>	<b>36, 500</b>	<b>42,100</b>
Assessments issued to DND	10,100	9,000	8,900
Assessments issued to other departments or agencies	27,600	27,600	28,900
<b>Total</b>	<b>37,700</b>	<b>36, 600</b>	<b>37,800</b>

\* Figures have been rounded to the nearest 100.

<sup>5</sup> Although CSIS will provide security assessments to the RCMP based on information contained in its records, it does not conduct such investigations on behalf of Canada's national police force. The RCMP conducts these investigations on its own behalf.

To track its efficiency in responding to security screening requests, CSIS calculates its turnaround times using a median number of days.<sup>6</sup> As indicated in Table 5, the median turnaround times generally decreased in 2005–06 from the previous fiscal year. There was a significant decrease in the time taken to prepare security assessments for DND at all levels.

**Table 5**  
**Median turnaround (in days)**

		2003–04	2004–05	2005–06
DND	Level I (Confidential)	20	49	24
	Level II (Secret)	18	63	19
	Level III (Top Secret)	96	70	39
Non-DND	Level I (Confidential)	7	12	15
	Level II (Secret)	11	14	13
	Level III (Top Secret)	82	69	60

The Service does not issue denials of security clearance. Rather, it advises the requesting department or agency of information that would affect CSIS's ability to recommend clearance. On rare occasions, CSIS will recommend to a requesting agency that a clearance be denied. However, it is the responsibility of the requesting agency to accept or reject this recommendation. In 2005–06, the Service issued 19 information briefs reporting information of an adverse nature, and issued one denial brief.

CSIS also provides site-access screening. Unlike a government security clearance, a site-access clearance only gives an individual access to certain secure areas within installations or provides accreditation for a special event. In 2005–06, CSIS received over 60,000 requests for this type of screening, and provided four information briefs to requesting agencies.

<sup>6</sup> CSIS reports its turnaround statistics using median numbers rather than averages because this mitigates the impact of unusually short or lengthy processing times, and better represents the typical amount of time to process an assessment.

**Table 6**  
**Site-access screening programs\***

	2003–04	2004–05	2005–06
Parliamentary precinct	1,400	1,100	1,000
Airport restricted-access area	28,800	31,100	37,600
Nuclear facilities	5,700	6,800	10,600
Free and Secure Trade (FAST)	N/A	21,500**	3,100
Special events accreditation	0	1,800	5,600
Other government departments	1,400	2,300	2,400
<b>Total</b>	<b>37,300</b>	<b>64,600</b>	<b>60,300</b>

\* Figures have been rounded to the nearest 100.

\*\* Refers to a one-time request to review previously granted passes, due to elevated security concerns related to the U.S. presidential elections.

### CSIS advice on security screening can take one of five forms:

1. **Notices of assessment** are issued in those government and immigration screening cases when CSIS finds no adverse information on an applicant.
2. **Incidental letters** are issued to Citizenship and Immigration Canada (CIC) and to the Canada Border Services Agency (CBSA) when the Service has information about an applicant who is or has been involved in non-security related activities described under the *Immigration and Refugee Protection Act* (IRPA).
3. **Information briefs** are issued in government screening cases when CSIS has information that could have an impact on the requesting agency's decision to grant an applicant a security clearance or site access. It is also provided in immigration screening cases when the Service has information that an applicant is or was involved in activities that do not necessarily warrant inadmissibility for entry into Canada.
4. **Inadmissibility briefs** are issued to CIC/CBSA when an applicant is deemed to be inadmissible to Canada under the security provisions of the IRPA.
5. **Denial briefs** are issued when the Service recommends to a requesting agency that a security clearance or site access be denied to an individual.

**Immigration screening**—CSIS’s Security Screening Branch also conducts investigations and provides advice to Citizenship and Immigration Canada as well as the Canada Border Services Agency to support the processing of refugee claims or applications for immigration or citizenship. The Service’s authority in this regard is provided under Sections 14 and 15 of the *CSIS Act*.

In 2005–06, the branch received approximately 92,000 requests under various immigration screening programs (see Table 7)—slightly fewer than in previous years. There was a significant drop—almost 20 percent—in the number of refugee determination screening requests, compared to the previous year. Meanwhile, the number of citizenship requests almost doubled. Also of note, there was an increase—about 13 percent—in the number of immigration screening requests.

**Table 7**  
**Types of immigration screening requests**

	Requests*			Briefs		
	2003–04	2004–05	2005–06	2003–04	2004–05	2005–06
Within and outside Canada	57,300	56,100	63,200	106	88	133
Front End Screening**	22,700	22,900	17,100	92	184	89
Refugee determination***	16,500	14,200	11,700	122	110	127
<b>Subtotal</b>	<b>96,500</b>	<b>93,200</b>	<b>92,000</b>	<b>320</b>	<b>382</b>	<b>349</b>
Citizenship applications	203,400	161,200	308,000	150	124	120
<b>Total</b>	<b>299,900</b>	<b>254,400</b>	<b>400,000</b>	<b>470</b>	<b>506</b>	<b>469</b>

\* Figures have been rounded to the nearest 100.

\*\* Represents those individuals who arrive at the Canadian border claiming refugee status.

\*\*\* Represents those refugees (as defined by IRPA) who apply from within Canada for permanent resident status.

The above table shows that CSIS finds no adverse information in the vast majority of its screening investigations of refugee claimants or immigration/citizenship candidates—one in every 250 immigrant applications or refugee claims screened, and one in every 2,500 citizenship applications screened. In 2005–06, of the total briefs regarding immigration screening (349), CSIS issued 232 information briefs and 117 inadmissibility briefs. There were also 12 incidental letters.



SIRC noted that generally the Service's turnaround times for the provision of information or inadmissibility briefs are quite lengthy. For information briefs related to immigration cases, it takes between 12 to 18 months to complete, depending on where the application was filed. In refugee cases, the median turnaround time was ten months for files subject to the Front End Screening program. For inadmissibility briefs, SIRC noted similar median times. For immigration files, the turnaround times ranged from a year to 18 months, while refugee files ranged from eight to 11 months.

Table 8 provides a three-year highlight of the Service's median turnaround time in providing notices of assessment.

	2003–04	2004–05	2005–06
Citizenship	1	1	1
Immigration requests from within Canada	46	44	70
Immigration requests from overseas	5	7	16
Immigration requests from the U.S.	152	150	62
Refugee determination	53	56	96
Front End Screening program	32	27	23
Visa vetting	12	13	11

**Other screening activities**—In 2005–06, the Security Screening Branch vetted over 36,000 visa applications of foreign nationals. It also started participating in the Free and Secure Trade (FAST) program and conducted over 3,000 security assessments of truck drivers who applied for a FAST border pass under this program. Consult the Canada Border Services Agency website at [www.cbsa-asfc.gc.ca/import/fast/menu-e.html](http://www.cbsa-asfc.gc.ca/import/fast/menu-e.html) for more information on this program.

**Other programs**—The Front End Screening (FES) and the Electronic Data Exchange (EDE) programs were introduced in 2001 to facilitate Canada's immigration and refugee screening processes. The FES program checks all refugee applications against CSIS records to identify potential security risks as early as possible in the refugee determination process. Further information on the FES program can be found in SIRC study # 2003–01, which was summarized in SIRC's 2003–04 annual report.

The EDE is an electronic network for filing screening applications that serve to accelerate processing times. Over 50 government clients use this service, such that almost all screening requests for refugee claimants or immigration/citizenship candidates are filed electronically. As in previous years, CSIS reported to SIRC that it is continuing to expand EDE access to additional clients, including six new government clients and two new immigration posts in the fiscal year.

### **FOREIGN LIAISON AND VISITS BRANCH**

The Foreign Liaison and Visits (FLV) Branch manages the Service's liaison with foreign agencies and coordinates visits to CSIS Headquarters and CSIS regional offices by foreign representatives. FLV is also responsible for coordinating all Section 17(1) arrangements with foreign security intelligence or law enforcement agencies, as well as the operation of security liaison posts abroad.

At the end of the 2005–06 fiscal year, CSIS had a total of 265 foreign arrangements with 144 countries. During that period, CSIS received Ministerial approval to establish six new arrangements, modify or enhance four others, and to suspend three arrangements.

Of the 265 foreign arrangements, 217 were active, 39 were dormant (i.e., no liaison contact for a period of at least one year), and nine were suspended or restricted (including the three mentioned in the previous paragraph). Any foreign arrangement classified as “dormant” or “restricted” remains as such until an update assessment of the relationship is completed.

The FLV Branch is also responsible for security liaison posts. The Service relies on these posts to liaise with foreign security and intelligence agencies. Security liaison officers are also called upon to assess the effectiveness of individual Section 17 foreign arrangements and submit annual assessments on each foreign agency in terms of their reliability as a partner, and their human rights record. For more information, see *CSIS liaison with foreign agencies: review of a security liaison post (# 2005–02)* in this annual report.

As in past years, SLO posts abroad faced increasing workloads related to immigration screening requirements. As a result, CSIS Headquarters provided temporary assistance and relief to certain SLO posts to assist with screening backlogs.

## FEDERAL COURT WARRANTS AND WARRANT STATISTICS

Warrants are one of the most powerful and intrusive tools available. They provide CSIS with Federal Court authorization to use investigative techniques that would otherwise be illegal, such as monitoring of telephone communications. For this reason, the use of warrants by CSIS deserves continued scrutiny—a task that SIRC takes very seriously.

Each year, SIRC collects statistics on the Service's warrant applications and on warrants granted by the Federal Court. Though SIRC does not have the resources to examine all warrants granted to the Service by the Federal Court, it will look at a certain number of warrants as part of its annual reviews.

When SIRC examines a warrant, it looks into all aspects of the warrant process, starting with the development of the warrant application. SIRC verifies whether:

- CSIS's justification for requesting warrant powers was reasonable;
- CSIS complied with the applicable legal and policy requirements in applying for warrant powers; and
- the warrant application accurately reflected the information held by CSIS.

SIRC also looks at the actual warrant approved by the Federal Court and what happens after that approval (i.e., how the warrant powers were used by CSIS).

Warrant application refers to the process by which CSIS submits warrant requests for consideration by the Service's Warrant Review Committee, the Minister of Public Safety and the Federal Court.

Warrants are documents issued by a Federal Court judge under Section 21(3), 22 or 23 of the *CSIS Act*, authorizing the Service to implement specific powers against particular individuals.

**Table 9**  
**Warrant statistics**

	2003–04	2004–05	2005–06
New	68	40	24
Replaced or renewed	130	207	203
<b>Total</b>	<b>198</b>	<b>247</b>	<b>227</b>

During the period under review, 24 new warrants were approved by the Federal Court. It also approved the renewal or replacement of 203 warrants. Included among the 227 warrants were 31 urgent warrants approved in 2005–06: more than three times the number approved in the previous year. In 2005–06, there were 248 expired or terminated warrants, compared to 220 in the previous fiscal year.

The Service also reported judicial decisions in 2005–06 that affected its applications for warrants, the execution of powers contained in warrants, or the warrant process generally. In two cases, the Court did not approve warrant powers. In the first instance, the judge decided that although the activities of the individual clearly constituted a threat to the security of Canada, the granting of warrant powers was premature. In the second instance, the judge refused the application on factual grounds. On other applications, the Federal Court requested additional information and clarification before approving the warrants. It also requested that the Service submit interim reports on the execution of certain warrant powers to ensure they were used for the purposes intended.

During 2005–06, the Federal Court dismissed an application for warrants. The decision was based on the fact that the Service had not provided full, fair and accurate disclosure of all material facts in the affidavit. The Court's decision was without prejudice to the right of the Service to bring forward a new application in relation to the same targets.

The Service subsequently provided the Court with a full explanation of the circumstances in question, and at that time, also informed the Minister of Public Safety, SIRC and the Office of the Inspector General. As a precautionary measure, the Director imposed a moratorium on the filing of warrant applications with the Federal Court until he was satisfied, on a case by case basis, that the Service's disclosure obligations had been addressed.

The Director has instigated a full review of the warrant process under the leadership of the Service's General Counsel. This request stemmed from his concerns about efficacy, timeliness and accountability of the current procedures, as the warrant application process has become increasingly complex and cumbersome over recent years. The implementation of the recommendations of the warrant review, which is scheduled for Fall 2006, is subject to consultation with the Department of Justice and the Department of Public Safety.

Moreover, since the dismissal of the warrant application, CSIS's Director and General Counsel have appeared before a Federal Court panel to discuss the case and the process for preparing and submitting warrant applications.

Also of note, although Section 28 of the *CSIS Act* authorizes the Governor-in-Council to make regulations governing the forms of warrants, practices and procedures applicable to the application hearings, as well as the location and manner in which hearings may be held, there were no such regulations made during this or any previous review period.

### **INTEGRATED THREAT ASSESSMENT CENTRE**

For details on the Centre's mandate and how it operates, see *Review of the Integrated Threat Assessment Centre (# 2005-03)* in this annual report. During 2005-06, ITAC issued 98 threat assessments and redistributed 382 others that were produced by the fusion centres of allied intelligence agencies. ITAC was also responsible for advising the National Security Advisor to the Prime Minister concerning several special threat assessments.

The majority of ITAC staff are seconded from partner agencies for a period of two years. Secondees are subject to the *CSIS Act* in the same fashion as CSIS employees. Despite being operational for two years, ITAC was not fully staffed at the end of the period under review.



## **Section 3**

---

**Want to know more about SIRC?**





## Want to know more about SIRC?

### COMMITTEE MEMBERSHIP

SIRC is chaired by the Honourable Gary Filmon, P.C., O.M., who was appointed on June 24, 2005. The other Members are the Honourable Raymond Speaker, P.C., O.C., the Honourable Baljit S. Chadha, P.C., the Honourable Roy Romanow, P.C., O.C., Q.C., and the Honourable Aldéa Landry, P.C., C.M., Q.C.

All Members of SIRC are Privy Councillors, who are appointed by the Governor-in-Council after consultation by the Prime Minister with the leaders of the Opposition parties.

SIRC provides assurance to Parliament—and through it, to Canadians—that CSIS complies with legislation, policy and Ministerial Direction in the performance of its duties and functions. SIRC seeks to ensure that the Service does not undermine the fundamental rights and freedoms of Canadians. It is the only independent, external body equipped with the legal mandate and expertise to review the activities of CSIS. Moreover, SIRC is a cornerstone of Canada's democratic tradition as it ensures the accountability of one of the government's most powerful organizations.

In addition to attending monthly committee meetings, members preside over complaints hearings, prepare reviews and complaint reports in consultation with SIRC staff, visit CSIS regional offices, appear before Parliament and exercise other duties associated with their responsibilities.

### SIRC meetings and briefings 2005–06

**April 18, 2005:** SIRC's Executive Director addressed the Special Senate Committee reviewing the *Anti-Terrorism Act*.

**May 11, 2005:** SIRC staff participated in the first Review Agencies Forum, attended by representatives of the Office of the Commissioner of the Communications Security Establishment (CSE) and the Inspector General of CSIS.

**May 17, 2005:** SIRC's Executive Director and senior staff met with officials from the United Kingdom's Intelligence and Security Committee.

**May 18–19, 2005:** SIRC co-hosted the International Symposium on Review and Oversight, together with its partner, the Canadian Centre of Intelligence and Security Studies of Carleton University.

**May 20, 2005:** The Executive Director and senior staff met with officials of the Dutch Supervisory Committee for Intelligence and Security Services.

**May 31, 2005:** SIRC met with the Independent Advisor to the Minister of Public Safety, regarding Air India.

**June 7, 2005:** The Executive Director and senior staff met with their counterparts from the O'Connor Commission concerning its policy review.

**June 8, 2005:** The Associate Executive Director and Senior Counsel addressed the Special House Committee reviewing the *Anti-Terrorism Act*.

**August 22, 2005:** The Executive Director and senior staff met with their counterparts from the O'Connor Commission concerning its policy review.

*Continued on the next page*

### SIRC meetings and briefings 2005–06

*(continued)*

**October 6, 2005:** The Executive Director attended a Queen's University-Government of Canada policy seminar in Kingston on Canada-U.S. relations regarding the security environment.

**October 11, 2005:** The Executive Director was a guest lecturer at Carleton University's Canadian Centre of Intelligence and Security Studies graduate seminar on intelligence, statecraft and international affairs.

**October 20–22, 2005:** The Executive Director and staff attended the annual conference of the Canadian Association of Security and Intelligence Studies in Montreal.

**November 17, 2005:** SIRC's Chair and Executive Director appeared at a public hearing of the O'Connor Commission, concerning its policy review.

**November 18, 2005:** The Executive Director was a guest lecturer at a Carleton University political science course entitled "Oversight and Access."

**December 2, 2005:** The Associate Executive Director made a presentation to an international seminar in Brasilia, Brazil, on intelligence and the democratic state.

**December 12, 2005:** The Executive Director and senior staff met with their counterparts from the O'Connor Commission concerning its policy review.

**January 24, 2006:** SIRC hosted the second Review Agencies Forum, attended by representatives of the Office of the Commissioner of the CSE, the Inspector General of CSIS, and the Commission for Public Complaints Against the RCMP.

*Continued on the next page*

### STAFFING AND ORGANIZATION

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

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.

As part of their ongoing work, 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 SIRC's knowledge about issues and opinions affecting the security intelligence field.

SIRC 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 be briefed by regional CSIS staff on local issues, challenges and priorities. It is also an opportunity to communicate SIRC's focus and concerns.

During the 2005–06 fiscal year, SIRC visited two regional offices. Over the last five years, SIRC has visited all six CSIS regional offices. In addition, SIRC staff received specialized training in a regional office concerning investigative techniques used by the Service. See *SIRC meetings and briefings 2005–06* for a summary of additional activities undertaken by SIRC during this period.

### BUDGET AND EXPENDITURES

SIRC 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. Table 10 below presents a breakdown of actual and estimated expenditures.

### 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 11 outlines the number of requests SIRC has received under these acts for the past three fiscal years.

### SIRC meetings and briefings 2005–06

(continued)

**March 3, 2006:** The Executive Director of SIRC and members of the Canadian Centre of Intelligence and Security Studies (Council of Advisors and Executive Committee) attended an international conference, entitled “Critical Energy Infrastructure Protection Policy: Assessing Threats, Vulnerabilities and Responses.”

**March 15, 2006:** The Executive Director was the guest lecturer at a Dalhousie University graduate seminar in Halifax, entitled “Parliamentary Oversight of the Canadian Security Intelligence Service.”

**March 21, 2006:** The Executive Director and senior staff met with the United Kingdom’s Joint Parliamentary Committee on Human Rights.

**Table 10**  
**SIRC expenditures 2005–06**

	2005–06 (Actual)	2005–06 (Estimates)
Personnel	\$1,796,000	\$1,777,000
Goods and services	\$941,702	\$1,019,000
<b>Total</b>	<b>\$2,737,702</b>	<b>\$2,796,000</b>

Access to Information requests for SIRC's studies represent the largest portion of access requests. SIRC waives the application fees for all such requests.

**Table 11**  
**Requests for release of information**

	2003-04	2004-05	2005-06
<i>Access to Information Act</i>	31	21	17
<i>Privacy Act</i>	1	3	5

### COMMUNICATIONS

To commemorate its 20<sup>th</sup> anniversary, SIRC co-hosted a major international symposium with the Canadian Centre of Intelligence and Security Studies of Carleton University. Held in May 2005, the theme of this two-day event was "Making National Security Accountable: International Perspectives on Intelligence Review and Oversight," which was explored in panel discussions and keynote speeches. The symposium attracted over 200 registered delegates and featured a range of experts from both Canada and abroad.

Although SIRC's annual report is the main communications vehicle for informing Parliament and Canadians about its work, it has implemented a modest communications program. SIRC has also undertaken some public opinion research, which shows that Canadians' awareness of review bodies remains very low, although perceptions of their independence and objectivity remain positive.

SIRC's website is continually updated with information relevant to the security and intelligence community. Since the website was first launched, traffic has

increased significantly, with the number of “total successful requests” more than doubling, to 539,789 in April 2006, from 201,267 a year ago.

**SIRC posted an Arabic translation of “How to Make a Complaint” on its website in January 2006.**

In an effort to be inclusive and to ensure that its recourse mechanism is well-understood, SIRC posted an Arabic translation of “How to Make a Complaint” on its website in January 2006. In addition, CSIS’s home page now features a direct hyperlink to SIRC’s website. As principal spokesperson, the Chair has met with some journalists to discuss SIRC’s work, and is scheduled to deliver several speeches in the upcoming year.

### **MODERN COMPTROLLERSHIP**

In 2005–06, SIRC contracted for an independent audit of its policy framework to confirm that its policies and procedures were consistent with Treasury Board requirements. It also aimed to identify gaps or omissions requiring attention. Moreover, SIRC developed competency profiles for all its staff and completed position descriptions for its researchers and counsel.

In the coming year, SIRC will be implementing an improved financial management framework, which will introduce further rigor to the way resources are allocated and expenditures are monitored. The Report on Plans and Priorities is the foundation on which budgets for SIRC’s program activities and priorities are established.

Also of note, SIRC contracted for an independent financial audit, which will examine how SIRC has used additional resources that were approved earlier by Parliament. This audit was completed in June 2006.



## **Appendix A**

---

### **SIRC reviews since 1984**





## SIRC reviews since 1984

**Note: Reviews flagged with an “\*\*” are Section 54 reports, which are special documents SIRC prepares for the Minister of Public Safety.**

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 Ostrowsky* (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 Investigation of Threats against Canada's Critical Information Infrastructure* (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)\*
162. *Review of a counter-terrorism investigation* (TOP SECRET) (SIRC 2005–01)
163. *CSIS liaison with foreign agencies: review of a security liaison post* (TOP SECRET) (SIRC 2005–02)
164. *Review of the Integrated Threat Assessment Centre* (TOP SECRET) (SIRC 2005–03)
165. *Review of a counter-intelligence investigation* (TOP SECRET) (SIRC 2005–04)
166. SIRC is currently working on this review, but it had not been finalized at the time this annual report went to print (SIRC 2005–05)
167. *Review of foreign arrangements with countries suspected of human rights violations* (TOP SECRET) (SIRC 2005–06)
168. *Review of CSIS's electronic-surveillance and information-gathering techniques* (TOP SECRET) (SIRC 2005–07)
169. *Review of activities and investigations in a CSIS region* (TOP SECRET) (SIRC 2005–08)

## **Appendix B**

---

### **Recommendations**



## Recommendations

During 2005–06, SIRC made 14 recommendations stemming from the reviews it conducted. These recommendations are summarized below.

Review	SIRC recommended that...
# 2005-01	<ul style="list-style-type: none"> <li>• CSIS extend its sensitive sector policy to require senior-level approval for certain investigative techniques.</li> </ul>
# 2005-02	<ul style="list-style-type: none"> <li>• CSIS Security Liaison Officers should maintain a written record when requests for information from CSIS Headquarters are transmitted verbally to foreign intelligence agencies.</li> <li>• CSIS update the post profile.</li> <li>• CSIS Headquarters remind operational branches and SLOs to submit reports [of discussions with foreign partners] in a timely fashion.</li> <li>• CSIS produce an assessment document concerning a new relationship with a specific foreign agency, especially since CSIS Headquarters made the same request in 2003.</li> <li>• CSIS develop an operational policy for documenting its relationships with agencies that are known or reputed to have engaged in human-rights abuse.</li> </ul>
# 2005-03	<ul style="list-style-type: none"> <li>• CSIS review its policies to determine where ITAC-specific amendments are required to address the role of this organization.</li> <li>• CSIS formalize its relationship with [another foreign fusion centre] and seek an approved foreign arrangement from the Minister of Public Safety.</li> </ul>

Review	SIRC recommended that...
# 2005-06	<ul style="list-style-type: none"> <li>• CSIS amend its policy governing the disclosure of information to foreign agencies, to include consideration of the human rights record of the country and possible abuses by its security or intelligence agencies.</li> <li>• CSIS Headquarters should maintain a written record of secure telephone conversations with SLOs—specifically conversations that contain operational information—and include this in its reporting.</li> <li>• CSIS review its procedures so that the parameters and methods of exchange—as well as the Service’s expectations—are communicated to the foreign agency prior to entering into new foreign arrangements.</li> </ul>
# 2005-07	<ul style="list-style-type: none"> <li>• CSIS review and revise the warrant policy in question so that it reflects current best practices.</li> </ul>
# 2005-08	<ul style="list-style-type: none"> <li>• CSIS obtain an updated legal opinion governing the use of [a certain interception] technique.</li> <li>• Existing operational policy [concerning internal security measures] be strictly adhered to by all regions, regardless of location, size or staff complement.</li> </ul>