SECURITY INTELLIGENCE
REVIEW COMMITTEE

SIRC Annual Report 2006–2007

An operational review of the Canadian Security Intelligence Service

Canada

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

(613) 990-8441 (voice)
(613) 990-5230 (fax)
www.sirc-csars.gc.ca
Collect calls are accepted between 8:00 AM and 5:00 PM, EST

Cat. No. PS105-2007E-PDF
ISBN 978-0-662-46644-4

SECURITY INTELLIGENCE
REVIEW COMMITTEE

SIRC Annual Report 2006–2007

An operational review of the Canadian Security Intelligence Service

Canada

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 28, 2007

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 2006–07, 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

Members' Statement

This year marks a significant anniversary in Canada's history. A quarter of a century has passed since the signing of the *Canadian Charter of Rights and Freedoms*, a document that guarantees freedom of conscience and religion; freedom of thought, belief, opinion and expression, including freedom of the press; freedom of peaceful assembly; and freedom of association. With the adoption of the *Charter*, these freedoms became constitutionally protected and Canadians gained recourse to the courts if the state infringed upon or denied their *Charter* rights.

There is no question that the bedrock values articulated in that historic constitutional document have helped to define what it means to be Canadian. They have had a profound influence on government, including the work of review agencies such as the Security Intelligence Review Committee (SIRC). These freedoms have been brought into sharp relief in recent years when considered along with the state's obligation to protect the safety of its citizens against a growing terrorist threat.

In carrying out our duties, the Committee has often found itself considering *Charter* issues. For example, as part of our reviews, we regularly examine CSIS's execution of judicially authorized warrant powers to ensure that intrusive investigative techniques comply with the law and the terms of the Court, and therefore do not constitute unreasonable search and seizure.

SIRC recognizes that the conduct of security intelligence agencies can prompt impassioned debate about whether the ends can ever justify the means. We also have first-hand knowledge that there are individuals who will seek to exploit Canada's rights and freedoms in order to harm our country, our citizens and our neighbours and friends around the world.

It is against this backdrop that SIRC's annual report features a summary of a Section 54 report that was submitted to the Minister of Public Safety on August 17, 2007. This type of report is relatively rare: only eight have been prepared in the last ten years. This latest report deals with the case of Mohammed Mansour Jabarah, a Canadian citizen and an admitted al Qaida member, who was convicted of terrorist-related offences in the United States.

In reviewing CSIS's role in this matter, we found that some of its actions violated certain rights as guaranteed under the *Charter*. As a result, we have made several recommendations to the Minister of Public Safety and the CSIS Director.

It is important to understand why SIRC takes issue with some of CSIS's actions and we invite readers to consider our analysis carefully. Mohammed Mansour Jabarah is a Canadian who, no matter how heinous his crimes and no matter how much we deplore them, is entitled to all of the rights and freedoms afforded to any other citizen under our *Charter*. Furthermore, an agent of the state must uphold the *Charter* otherwise Canadian officials would be free to pick and choose to whom certain guaranteed rights and freedoms would apply. Clearly, that would be unacceptable to all Canadians.

"An agent of the state must uphold the *Charter* otherwise Canadian officials would be free to pick and choose to whom certain guaranteed rights and freedoms would apply."

SIRC recognizes that police and security intelligence agencies in the post 9/11 world must deal with daunting challenges, including globalized and technologically sophisticated terrorist groups. We also know that the relative safety that Canadians enjoy is thanks in large part to the efforts of these same agencies on our behalf. But the obligation to ensure public safety ought not to reduce in any way respect for the rule of law.

Mr. Justice Ian Binnie of the Supreme Court of Canada characterized the competing demands of national security and human rights as a "clash of titans." It is true that at times, human rights and national security objectives may appear to clash. But in a healthy democracy where rights and freedoms have constitutional protection, we firmly believe that they can—indeed they must—coexist. That is a principle which all Canadians should uphold and that every citizen has a continuing responsibility to protect.

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. SIRC has two key functions. The first is to conduct in-depth reviews of CSIS activities to ensure that they accord 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 2006–07 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:

Section 1: A year in review 2006–07
This section summarizes nine reviews SIRC completed during the period covered by this report. It also provides information about five complaint reports issued by SIRC.

Section 2: CSIS accountability mechanisms
Featured in this section are descriptions of the policy and governance framework within which CSIS operates. This section also contains information provided by CSIS on operational activities, plans and priorities, organized according to the Service's major branches.

Section 3: About SIRC
This section provides details about the outreach, liaison and administrative activities of SIRC, including its annual budget and expenditures.

Section 1

A year in review 2006–07

A year in review 2006–07

A. Review of CSIS security intelligence activities

HOW SIRC CARRIES OUT ITS REVIEW FUNCTION

The Security Intelligence Review Committee is the only body with the legal mandate and expertise to carry out ongoing, independent review of 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 acting in accordance with the law, policy and Ministerial Direction in the performance of its duties and functions. In doing so, SIRC seeks to ensure that CSIS respects the fundamental rights and freedoms of Canadians.

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 the Committee identifies as having special importance or that the Minister directs 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 and guide 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:

- events with the potential to create threats to the security of Canada;
- particular activities that could intrude on individual rights and freedoms;
- the CSIS Director's annual 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*;
- priorities and concerns identified by Parliament or in the media;
- commitments by SIRC to re-examine specific matters;
- issues identified in the course of SIRC's complaints functions; 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 number of CSIS activities in any given year. Each review results in a "snapshot" of the Service's actions in a particular context. Over more than 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 only 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, the central agencies, the Auditor General, the Information Commissioner and the Privacy Commissioner of Canada.

SIRC REVIEWS IN 2006–07

Review of a security liaison post

Review 2006–01

Background

During the period under review, CSIS maintained a number of Security Liaison Officer (SLO) posts[1] around the world—the number and locations of which are classified, except for those in London, Paris and Washington. These posts work with Citizenship and Immigration Canada to process immigration requests. They also exchange security intelligence information, provide advice to senior staff of the Canadian Mission or Embassy, and liaise with foreign security and intelligence agencies with whom the Service has approved arrangements.

Methodology

SIRC examined how the Service managed its relationships at the post as well as all information exchanges with relevant foreign security and intelligence agencies. SIRC also inquired into the management of CSIS staff at the post, visits to and from the region, and examined the assessments of those agencies with whom the SLO cooperates, a profile of the post itself, and all CSIS studies or reports pertaining to the countries which fall under the post's areas of responsibility. In particular, SIRC evaluated the impact of the immigration security screening workload on other SLO functions.

Findings

SIRC found that the post was managed effectively and that its operations were in accordance with the *CSIS Act*, Ministerial Direction, and operational policy and guidelines. Staff at the post completed and submitted immigration tracking forms on a regular basis, and submitted all required contact and visit forms. The post provided timely and relevant information and advice concerning visits to CSIS Headquarters by foreign representatives. Appropriate approvals were sought and obtained regarding all visits. CSIS's assessments of agencies with which the Service cooperates were, for the most part, completed accurately and submitted in a timely manner, and a new Section 17 arrangement with an organization in the region was established in accordance with Ministerial Direction and operational policy.

[1] SLOs have since been renamed Foreign Officers, as part of a corporate reorganization of CSIS. See Section 2 for details.

All foreign exchanges included the appropriate caveats in accordance with operational policy—specifically, the Service ensured that all information shared with foreign partners was identified as having originated from CSIS, and included restrictions on how it could be used. Finally, SIRC confirmed that the post complied with a CSIS directive not to provide information to or cooperate with a specific foreign intelligence organization during the period under review because of concerns about that agency's reliability.

There were no recommendations arising from this review.

Review of activities and investigations in a CSIS regional office

Review 2006–02

Background

SIRC regularly reviews, on a rotating basis, the activities and investigations of CSIS in each region of Canada. These regional reviews provide insight into how investigations authorized by CSIS Headquarters are implemented in the field. They also help SIRC gain a better understanding of the priorities and challenges of individual regional offices.

This year, SIRC chose to review CSIS's smallest regional office, which, despite its size, has full operational and administrative capabilities.

Methodology

For the period September 1, 2004 to August 31, 2005, SIRC assessed the activities of this regional office with reference to the *CSIS Act*, Ministerial Direction and operational policies. SIRC examined the regional office's:

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

Findings

SIRC found that the operations of the CSIS regional office were in full accord with all applicable laws, directions and policies. CSIS had reasonable grounds to suspect that the targets of authorized investigations in this region posed a threat to the security of Canada, and the intrusiveness of the techniques used was

proportionate to the suspected threat. The information collected by CSIS was strictly necessary to fulfill its mandate. SIRC was pleased to observe that regional staff are responding to emerging threats in a timely and professional manner.

The regional office met all requirements of the Federal Court of Canada in applying for and executing warrant powers in specific investigations. Further, the Service acted appropriately and within the law in its management of human sources. There were a few administrative errors noted in certain human source files, but SIRC considered these minor and they did not affect the Service's investigations.

SIRC found no issues of concern regarding the regional office's cooperation and exchange of information with domestic partners, or with the application of security policies, practices and procedures.

There were no recommendations arising from this review.

Review of a counter-terrorism investigation

Review 2006–03

Background

The focus of this review was a nation-wide CSIS investigation of two Middle East-based organizations listed as terrorist entities under the *Criminal Code of Canada*. The Service's aim was to discover whether there was any formal presence of these terrorist groups in Canada, to identify Canadian-based support networks and to identify persons or groups of persons in Canada who were associated with these Middle Eastern organizations.

Although this was a relatively long-running investigation, there were never more than ten approved targets during the review period of September 1, 2002 to November 30, 2005. By the end of 2005, CSIS had not identified any formal organized presence of these groups in Canada, but the Service had initiated several new investigations of individuals believed to be either linked to, or acting on behalf of the organizations under investigation.

Methodology

This was the first time that SIRC had examined this particular investigation. SIRC analysed documentation pertaining to: the targeting of individuals suspected of engaging in threat-related activities; the management of human sources against authorized targets; and all exchanges of information with domestic and foreign organizations.

Findings

The Service's identification and investigation of targets were found to be in full accord with the *CSIS Act* as well as applicable Ministerial Direction and operational policies. In each investigation, CSIS had reasonable grounds to suspect a threat, and the targeting authorities were proportionate to the seriousness of the threats. CSIS investigators collected only information that was strictly necessary to the investigation.

SIRC noted that the investigation suffered from a lack of resources throughout the review period, and that administrative responsibility for this file shifted repeatedly among CSIS operational desks. This had adverse consequences on the management of information and, to some degree, on the management of human sources. However, generally speaking, SIRC found CSIS to be in compliance with operational policies in the handling of its human sources.

Section 2 of the *CSIS Act* prohibits the investigation of individuals involved in lawful advocacy, protest or dissent (LAPD), unless such activities are carried out in conjunction with threats to the security of Canada. Operational policy therefore requires that investigations which come into contact with LAPD receive special, high-level authorization.

SIRC noted one case where policy requirements were not met. The Service was investigating several members of a Canadian-based community centre because it believed these individuals were engaged in threat-related activities unrelated to the centre's LAPD endeavours. SIRC's review confirmed that the Service's investigation was not focussed on these LAPD activities. Nonetheless, operational policy requires senior-level authorization because of the individuals' involvement in LAPD activities. SIRC found that CSIS investigators failed to obtain the appropriate senior-level authorization in this case, and reminded the Service of their obligation to do so.

The Service's exchanges of information with domestic and international partners were appropriate, although a difficult working relationship with one foreign agency did affect CSIS's investigations during the review period. SIRC also saw one case where ineffective coordination between CSIS and the RCMP resulted in CSIS losing track of an individual for several months. The RCMP and CSIS had exchanged information irregularly on this person. As a consequence of the RCMP's decision to downgrade its investigation, CSIS no longer had accurate information regarding the individual's whereabouts. CSIS could not locate the individual in the ensuing five months, until it learned that the individual was no longer in the country, whereupon CSIS terminated its investigation.

Finally, SIRC reviewed a case of a Canadian citizen detained by a foreign country for suspected involvement in terrorist activity. Media reports alleged that the individual had been mistreated while in detention. SIRC concluded that the Service had conducted an effective and appropriate investigation of the terrorism allegations and of the alleged mistreatment of the detainee. It also found that CSIS upheld its responsibility to the Department of Foreign Affairs and International Trade (DFAIT)—the lead agency responsible for this case.

There were no recommendations arising from this review.

Review of a Section 16 activity

Review 2006–04

Background

Under the provisions of Section 16 of the *CSIS Act*, either the Minister of National Defence or the Minister of Foreign Affairs may request in writing the assistance of the Service in collecting foreign intelligence within Canada. Foreign intelligence is defined as information or intelligence relating to the capabilities, intentions or activities of any foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security.

If the Minister of Public Safety agrees with the request, it is passed to the Director of the Service, along with written concurrence and direction. CSIS may retain in its Section 12 database any foreign intelligence it collects only if it aids investigations falling under Section 12 of the *CSIS Act*.

The *Act* specifically prohibits any Section 16 collection being directed at Canadian citizens, landed immigrants or Canadian corporations. In the event that CSIS chooses not to retain Section 16 information for a Section 12 investigation, SIRC's jurisdiction ends once the material has been provided to the requesting minister.

A 1987 Tri-Ministerial Agreement establishes the roles and responsibilities of all parties involved in Section 16 collection. One such party is the Communications Security Establishment (CSE), which provides technical assistance in the collection of foreign intelligence.

Section 16 information which CSE provides to the Service is routinely "minimized" to comply with various directions governing the prohibition against targeting Canadian nationals and Canadian businesses. Thus, the name of a Canadian person or entity, collected incidentally, would be reported to the Service

using language such as "a Canadian person" or "a Canadian company." Under specific circumstances defined in policy, the Service may request identification from CSE if it can demonstrate that the information relates to activities that could constitute a threat to the security of Canada as defined in Section 2 of the *CSIS Act*.

Methodology

SIRC examined CSIS Section 16 collection on a foreign country ("Country A")—assessing that activity against the *CSIS Act*, Ministerial Direction and, in particular, the 1987 Tri-Ministerial Agreement. Specifically, SIRC reviewed the following:

- all Section 16 reporting to and feedback from DFAIT in 2005;
- the application for and use of Section 16 warrant powers and handling of associated documents;
- the management of human sources who provided both threat-related information and foreign intelligence; and
- the authorization for a corresponding investigation of threat-related activities, as well as all exchanges of information with DFAIT based on this threat.

SIRC staff also received a briefing from CSIS and spoke informally to other Service employees.

Findings

CSIS's foreign intelligence collection against Country A met the requirements of the *CSIS Act*, in that it did not involve any targeting of Canadians or Canadian organizations. The application for and use of Section 16 warrant powers, and the management of the human sources reviewed, were also appropriate and in accordance with legal and policy requirements.

The *CSIS Act* restricts Section 16 collection to "within Canada." This means that CSIS cannot task human sources to collect Section 16 information abroad. Although some sources undertook travel abroad, CSIS did not task these human sources to collect Section 16 information while they were outside of Canada. CSIS did, however, have the authority to task these human sources to collect information abroad under a Section 12 investigation of the threat-related activities of Country A. Some of that information proved to be valuable in meeting DFAIT's Section 16 requirements.

There were no recommendations arising from this review.

Review of a counter-terrorism investigation

Review 2006–05

Background

Known for its support of al Qaida, this foreign-based group was among the first to be placed on Canada's List of Terrorist Entities. This was SIRC's first review of a Service investigation into suspected threat-related activity in Canada by this foreign-based group. It afforded SIRC the opportunity to look into a particular investigative technique occasionally employed by CSIS.

Methodology

SIRC reviewed the Service's investigation from January 1, 2003 to December 31, 2005. The objective of this review was to gain an understanding of this investigation and its challenges, and to assess the Service's compliance with the *CSIS Act*, Ministerial Direction and operational policies.

Specifically, SIRC reviewed the:

- investigation and the targeting approvals of suspected group members;
- implementation and execution of Federal Court warrant powers against the principal targets;
- management of human sources, including those under development;
- advice to government and domestic exchanges of information; and
- exchanges of information and cooperation with foreign intelligence agencies.

In addition, SIRC received two briefings—an overview of the Service's investigation, plus a meeting with the lead CSIS investigator to discuss the Service's interaction with the principal targets.

Findings

Overall, SIRC found that the Service complied with the *CSIS Act*, as well as Ministerial Direction and operational policies in its investigation of the targets. The information collected by CSIS did not indicate that the group's members were involved in terrorist activities while in Canada, and CSIS therefore concluded that they were not an active, operational terrorist cell within Canada. SIRC agreed with CSIS's assessment that it had reasonable grounds to suspect that the activities of the principal targets posed a potential threat to the security of Canada.

There were no recommendations arising from this review.

Review of CSIS's collaboration and exchanges of intelligence post-9/11

Review 2006–06

Background

This review was prompted in part by changes in CSIS's relationships with foreign and domestic partners post-9/11. CSIS is exchanging greater amounts of information with its foreign partners, and with a greater number of foreign partners than in the past. Domestically, the RCMP's role in investigating security threats has grown following the passage of the *Anti-Terrorism Act*, which criminalized actions affecting the national security of Canada. As a result, there is increasing pressure on CSIS to provide support for RCMP prosecutions.

Methodology

This review examined CSIS's relationship with one of its foreign partners and with the RCMP. The objective was to assess compliance with the *CSIS Act*, Ministerial Direction, Memoranda of Understanding (MOU) and operational policies, and to review generally CSIS's performance in the context of its relationship with the RCMP.

To that end, SIRC examined all exchanges of information with the RCMP, all files pertaining to the CSIS-RCMP relationship at headquarters and in two regional offices, and all documents pertaining to CSIS's relationship with two Integrated National Security Enforcement Teams for the 2005 calendar year.[2] SIRC also examined CSIS's targeting of two individuals between January 1 and July 31, 2005.

Concerning the foreign agency, SIRC reviewed all exchanges of information between 2001 and 2005, CSIS's 2001 and 2006 assessments of the agency, and all files pertaining to its relationship with the agency for the 2005 calendar year.

[2] More information on the Integrated National Security Enforcement Teams program is available in Section 2 of SIRC's 2002–03 Annual Report.

Findings

CSIS's exchanges of information with the foreign agency were within the scope of the foreign arrangement and complied with the *CSIS Act*, Ministerial Direction and relevant operational policies. SIRC had some concerns about internal mis-communication, as some CSIS officers did not know the status of CSIS's relationship with the foreign agency during the 2002–04 period. This resulted in the SLO receiving incorrect tasking. There was, however, no improper exchange of information.

CSIS's exchanges of information with the RCMP were authorized under the *CSIS Act* and in accordance with Ministerial Direction and relevant operational policies. Looking more generally at the CSIS-RCMP relationship, SIRC noted a spirit of goodwill between the two organizations, as reflected in the new MOU—signed on September 12, 2006—and other initiatives. This new MOU replaces the original one signed in 1990, which had become obsolete.

However, certain challenges remain. SIRC identified two instances that appeared to cause significant friction between CSIS and the RCMP in 2005. The first was an attempted RCMP prosecution using CSIS information. The second concerned the activities of a CSIS human source, which complicated an RCMP investigation for the purposes of criminal prosecution. SIRC notes, however, that there have been positive developments in the CSIS-RCMP relationship in that region since 2005.

SIRC has already noted that the mechanism for exchanging information—in particular, the requirement that the RCMP seek and receive CSIS's explicit permission before using CSIS information in judicial proceedings—was "brought into question"[3] by the 1991 Supreme Court decision, *R. v. Stinchcombe*, requiring the Crown to disclose all relevant information to defence counsel. In 2007, CSIS and the RCMP established a working group to review and improve the process for using security intelligence in criminal prosecutions of national security offences.

There were no recommendations arising from this review.

---

[3] Report 101, CSIS Cooperation with the Royal Canadian Mounted Police, Part 1 as reported in Section 1 of SIRC's 1997–98 Annual Report.

Review of security screening outside of the federal government

Review 2006–07

Section 13 of the *CSIS Act* enables the Service to provide security assessments to federal and provincial governments, as well as police forces and foreign entities. The goal of the Security Screening program is twofold: to prevent a non-Canadian who poses a security concern or risk from entering or receiving status in Canada, and to prevent anyone of security concern from gaining authorized access to sensitive government assets, locations or information.[4]

CSIS security assessments fall into two main program categories:

1. Immigration, whereby the Service provides security assessments to Citizenship and Immigration Canada and the Canada Border Services Agency to support the processing of refugee claims or applications for immigration or citizenship; and
2. Government Security Screening, whereby the Service:
   - provides security assessments to all federal departments and institutions, with the exception of the RCMP;
   - complies with requests from foreign agencies (via arrangements with other countries) concerning Canadians who are candidates for employment in a foreign country and require access to classified material; and
   - provides security assessments for non-clearance related programs such as: nuclear sites, the Parliamentary Precinct, provincial governments, sites of interest in respect to national security (e.g., airports and ports) and other programs.

It should be noted that some programs fall under the Government Security Policy while others, such as the Airport Restricted Access Clearance Program and the Free and Secure Trade program, are performed under different authorities and thresholds.

This review focused on assessments for non-clearance related programs.

[4] For more information on CSIS's Security Screening activities, please see Section 2 of this Annual Report.

Methodology

SIRC assessed CSIS's compliance with the *CSIS Act*, Ministerial Direction, operational policies, the Government Security Policy and relevant Memoranda of Understanding between the Service and its clients. SIRC conducted an in-depth review of a six-month sample of cases and a detailed analysis of all Information Briefs[5] issued during the review period (there were no denial briefs issued during the review period of April 1, 2004 to March 31, 2006).

Findings

SIRC found considerable variance in the uniformity of Information Briefs, and a lack of consistency in the recording and transcribing of interviews conducted for use within these briefs.[6] SIRC was pleased to note that the Service only conducted screening checks for foreign agencies where an approved arrangement was in place, and that no recommendations were made, as per policy, to foreign entities. Finally, the Service complied with Ministerial Direction in keeping security screening information segregated from the Service's other information holdings because of its sensitivity for the individuals undergoing assessment.

Recommendations

SIRC made two recommendations arising from this review:

- SIRC observed a lack of differentiation in Information Briefs between varying degrees of risk posed by security screening subjects. For example, the Service assessments of a subject's links with individuals known or thought to be threats to national security were supported in some cases by what SIRC considered to be less compelling information than in others. In another example, although some security screening subjects were offered the opportunity to address security issues in an interview with Security Screening Branch, others were not. SIRC found it problematic that no gradation exists within Information Briefs to address varying degrees of risk of screening applicants, and that these briefs were neither uniform nor consistent as required by policy. SIRC consequently recommended that the Service create policy to address this issue.
- SIRC noted that midway through the review period, the Service abandoned the practice of retaining written consent forms for security assessments conducted for a foreign agency, making it impossible to determine that consent had, in fact, been sought and obtained. SIRC recommended that in cases where the Service

---

[5] Information Briefs are issued by CSIS in government screening cases when CSIS uncovers information which may be of concern. They are provided to the requesting agency which then decides whether or not to grant an applicant a security clearance or site access.

[6] The Service has since changed the policy dealing with interviews.

cannot access written consent forms after the fact (i.e., foreign agencies), these forms be obtained for all security assessments.

Review 2006–08

Note:
Review 2006–08 had not been finalized at the time this annual report went to print. A summary of this review will appear in SIRC's 2007–08 annual report.

Review of the CSIS Counter Espionage Investigations desk

Review 2006–09

Background
Since 9/11, western intelligence agencies have increasingly shifted their attention and resources to counter-terrorism investigations. But there remain other security threats that need to be addressed. In 2006, CSIS and other federal authorities were involved in the arrest and deportation of a Russian spy who had been living in Canada for several years under a false identity. The case serves as a reminder that Canada remains a target of foreign espionage.

This was acknowledged by CSIS Director Jim Judd in an October 2006 address to the annual Canadian Association for Security and Intelligence Studies conference. He noted that "foreign espionage is, if anything, growing and in fact becoming even more sophisticated through the application of new technologies."

One of the ways the Service combats this threat is through its Counter Espionage Investigations desk. It was formed in 2002 to compartmentalize sensitive counter-espionage investigations which could lead to the prosecution of individuals who knowingly provide sensitive information or assets to hostile intelligence services or foreign governments in a manner detrimental to Canadian interests.

Methodology

SIRC's review examined the activities carried out by the Counter Espionage Investigations desk to assess compliance with the *CSIS Act*, Ministerial Direction and operational policies. It also explored how the Service investigates and supports the prosecution of counter-espionage offences through information sharing with law enforcement agencies.

SIRC chose two investigations for in-depth review. For each, SIRC examined targeting decisions, investigative activities, operational reporting, as well as cooperation and exchanges of information with domestic and foreign partners. Because of the sensitivity of these cases, SIRC is prevented from offering any further details in this report.

Findings

SIRC found that CSIS complied with the *CSIS Act*, Ministerial Direction and operational policies in carrying out counter-espionage investigations.

In the first investigation, SIRC found that close cooperation between CSIS and its domestic and foreign counterparts allowed a "serious security issue" to be resolved in a timely and efficient manner.

In the second investigation, SIRC found that CSIS's disclosure of information allowed the RCMP to take action against an individual engaged in unlawful activities.

There were no recommendations arising from this review.

B. Section 54 Report

Section 54 of the *CSIS Act* entitles SIRC to provide the Minister of Public Safety with a special report on any matter relating to the performance of CSIS's duties and functions. SIRC determined that the events involving Mohammed Mansour Jabarah, as well as concerns raised by the Canadian Civil Liberties Association, were of sufficient importance to warrant a report of this nature.

In April 2005, the then-Minister of Public Safety wrote to the Canadian Civil Liberties Association to assure them that CSIS's actions in this investigation were "appropriate and in accordance with its mandate." The Committee does not know on what advice the Minister based her response, but SIRC's analysis suggests that Section 12 of the *CSIS Act* would not have authorized all aspects of the investigation. This serves as a reminder of the importance of Ministers receiving accurate and comprehensive advice on such sensitive matters.

Review of the case of Mohammed Mansour Jabarah

Review 2005-05

Background

Mohammed Mansour Jabarah, a Canadian citizen, is an admitted al Qaida member and leader of a terrorist cell that planned to bomb the American and Israeli embassies in Singapore and Manila. If successful, the result could have been catastrophic. However, when the plan was thwarted he fled and was apprehended in Oman in March 2002. On short notice, CSIS officials travelled to Oman and unexpectedly found themselves having to arrange for Jabarah to return to Canada. CSIS paid for his ticket.

This investigation was unusual, if not unique, on several levels. In the post-9/11 environment, Canada was working hard to learn as much as possible about the threat from al Qaida, and to demonstrate its reliability as a close ally of the United States in the fight against terrorism.

Nevertheless, despite Jabarah's admissions, he could not be charged under the *Criminal Code*, since all of his terrorist activities pre-dated Canada's *Anti-Terrorism Act*. CSIS engaged in consultations with Jabarah which led him to sign an agreement to facilitate his entry into the U.S. In May 2002, he was transported there with the assistance of CSIS and subsequently pleaded guilty to a number of terrorism-related offences. At the time SIRC's review was finalized, Jabarah had still not been sentenced and he remains incarcerated.

SIRC decided to name this individual in its Annual Report, given that so much information about this case is already in the public domain. On August 14, 2007, the Privacy Commissioner was informed of SIRC's decision. This was done under paragraph 8(2)(m) of the *Privacy Act* which permits the disclosure of personal information when "the public interest in the disclosure clearly outweighs any invasion of privacy."

Methodology

SIRC reviewed this investigation against CSIS operational policy and procedures, Ministerial Direction and applicable Canadian law, including the *CSIS Act* and the *Charter of Rights and Freedoms*. SIRC was also mindful of two facts: that Jabarah is a Canadian citizen, and that Canadian officials must act in accordance with the law.

SIRC examined classified, electronic and hard copy documentation concerning: CSIS's role during Jabarah's time in Oman and during his accompanied travel from Oman to Canada; after his return to Canada; and his transfer to American custody. The Committee also reviewed unclassified, open source material (a book, letters, media reports, etc.). In addition, SIRC received a general briefing from CSIS and an extensive briefing from the investigators assigned to this case. SIRC also obtained legal advice from the Honourable Gérard LaForest, C.C., Q.C., a former member of the Supreme Court of Canada who is a recognized expert on the *Charter*.

Because of the nature and gravity of the issues raised by its review, the Committee decided to submit its findings and recommendations directly to the Minister of Public Safety, under Section 54 of the *CSIS Act*.

Findings

This review highlights a much wider debate occurring in most western democracies. In a November 2004 speech, Mr. Justice Ian Binnie of the Supreme Court of Canada characterized the competing demands of national security and human rights as a "clash of titans."

In reviewing this case, SIRC acknowledges that the context for these events, soon after 9/11, was such that the protection of Canada and cooperation with Canada's close allies were priorities across the security and intelligence community. SIRC was also told that CSIS believed that Jabarah had consented freely and voluntarily to cooperate with CSIS and to relinquish his liberty to a foreign jurisdiction.

Nevertheless, the Committee approached this study with the knowledge that Section 32 of the *Charter* applies to the actions of CSIS. Ministerial Direction further reinforces the requirement for CSIS to comply with the *Charter*. Because of events that occurred while Jabarah was in Canada and because CSIS helped to arrange his transportation to the U.S. on a Canadian government-owned aircraft, SIRC sought assurance that CSIS had exercised due diligence to ensure its actions were in accordance with Canadian law.

SIRC's review raised questions regarding CSIS's contention that Jabarah's decisions were made freely and voluntarily. SIRC concurs with LaForest that several of the circumstances surrounding this case would lead a court to scrutinize meticulously the actions of CSIS officials to determine whether Jabarah's decisions were completely voluntary. His decisions—made without the benefit of any independent legal advice—resulted in Jabarah's self-incrimination and surrender to U.S. authorities. SIRC believes a court would also have considered other factors, including: his age; his emotional state; whether his fear of the alternatives influenced his return to Canada from Oman; the length of time he spent in the company of CSIS officials while in Canada; and the circumstances surrounding his decision to surrender himself to a foreign jurisdiction.

SIRC was told by a CSIS investigator that Jabarah was not "read his rights" because CSIS is not a police service. This response—subsequently confirmed in writing by the Service—demonstrates a misunderstanding of the application of the *Charter* to government representatives carrying out their official duties.

Jabarah could not be prosecuted for any crime in Canada, since his terrorist activities pre-dated Canada's *Anti-Terrorism Act*. Neither CSIS nor the police had any right to detain him. Based on these and other circumstances, the Committee concluded that Jabarah was "arbitrarily detained" by CSIS in violation of Section 9 of the *Charter*. Because he was detained, his right to silence as protected by Sections 7 and 11(c) was violated, as was his right to counsel under Section 10. Furthermore, his right to remain in Canada as protected by Section 6 of the *Charter* (mobility rights) was breached.

Another Canadian agency informed CSIS that Jabarah could not be criminally charged, since the acts which he committed did not take place in Canada and were not crimes in Canada at that time. However, CSIS knew that Jabarah could be prosecuted in the U.S. During its review, SIRC became aware of actions undertaken by CSIS (which remain classified) that materially assisted U.S. law enforcement officials. For that reason, SIRC believes that CSIS could not be independent with respect to any consultations that it carried out with Jabarah. Moreover, these actions led SIRC to conclude that CSIS strayed from its security intelligence mandate into the area of law enforcement.

Finally, SIRC found that it was missing some documentation relevant to its review. SIRC saw references to meetings for which minutes were not kept, to interdepartmental consultations for which there were no written records, and to operational email messages that had been deleted. SIRC was concerned by these gaps in the written record. It was especially troubled that an investigation of such importance and sensitivity—which had a direct impact on the indictment and prosecution of a Canadian by U.S. authorities—could be conducted by CSIS without requesting any formal legal advice from the Department of Justice.

Recommendations

SIRC made six recommendations stemming from this review:

- The 1987 Memorandum of Understanding (MOU) between CSIS and the Department of Foreign Affairs and International Trade (DFAIT) be updated to designate Foreign Affairs as the lead agency in cases involving Canadian citizens detained abroad. The MOU should also reflect the protocol recommended by Mr. Justice O'Connor, namely, "timely and open consultation among Canadian agencies" involved with Canadians detained abroad, "a coherent and unified approach" led by DFAIT and "accountability for the course of action adopted" in such cases.

- CSIS amend its policies so that emails are automatically retained unless there is a conscious decision to delete them.
- The Service clearly communicate to its employees what would constitute "recorded information," as distinct from "transitory records," and should therefore be filed and retained under applicable federal legislation.
- Whenever possible, CSIS keep written records of its interdepartmental consultations, including but not limited to its formal and informal consultations with DFAIT and the Department of Justice.
- CSIS ensure that the storage, retention and retrieval of all operational information under its control, including email messages, is in accordance with applicable federal legislation, including the *CSIS*, *Privacy*, *Access to Information* and *Library and Archives of Canada Acts*.
- CSIS request and obtain written advice from the Department of Justice in operations where an individual is questioned in circumstances which may give rise to a detention, in order to ensure that the individual's *Charter* rights are respected, and in all occasions when it is unclear whether the Service's activity falls within its statutory mandate under Section 12 of the *CSIS Act*.

Conclusion

Jabarah is a terrorist but also a Canadian citizen, and no matter how despicable his actions, the *Charter* conferred on him certain fundamental rights. SIRC's mission is to protect Canadians' rights by ensuring that CSIS acts within the law. Therefore, the Service must comply with the *Charter* in carrying out its investigations as mandated by the *CSIS Act*, no matter what unexpected circumstances may arise.

C. Investigation of complaints

HOW SIRC INVESTIGATES COMPLAINTS

In addition to its review function, SIRC is responsible for investigating complaints 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 a concern to become a formal complaint.

Once a written complaint is received, SIRC conducts an initial review. 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 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.

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 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 *CSIS 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. Section 42 does not permit SIRC to accept jurisdiction to hear complaints concerning less intrusive background screening or reliability checks, which are conducted simply to determine the trustworthiness or suitability of a potential federal employee. These complaints are addressed through an organization's designated grievance procedure.

Pursuant to Section 42 of 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, the Deputy Head concerned and the complainant.

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 Director of CSIS, the Minister of Public Safety, the Minister of the department concerned and the complainant. SIRC also has the authority to conduct investigations into matters referred to SIRC pursuant to the *Citizenship Act.*

When SIRC's investigation of a complaint made under Section 41 is concluded, it provides the Director of CSIS, the Minister of Public Safety and the complainant with a report of its findings and recommendations.[7] Summaries of these reports, edited to protect national security and the privacy of complainants, are also included in SIRC's annual report to Parliament.

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).

---

[7] The complainant receives a declassified version of the report.

Table 1
Resolution of complaints

	2004–2005	2005–2006	2006–2007
Carried over	16	18	24
New	30	45	37
Total	**46**	**63**	**61**
Closed	28	39	41
Carried forward to subsequent year	18	24	20
Reports issued	3	4	5

How SIRC determines 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.

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*.

…under Section 42

With respect to 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.

These types of complaints must be filed within 30 days of the denial of the security clearance. SIRC may extend this period if valid reasons are presented.

D. SIRC complaint decisions 2006–07

The following are summaries of the five reports issued by SIRC during the period under review, in response to complaints filed.

Alleged discrimination in an immigration process

Report 2006–01

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)*. The complainant in the case alleged discrimination in contravention of the *CHRA* after being denied a "security clearance".[8] Since this security assessment was required for the complainant's immigration process, the allegation was that the complainant was prevented from becoming a Canadian citizen because of the denial of the clearance.

The complaint specifically alleged: a delay by CSIS in processing the complainant's security assessment which formed the basis of the advice to the Minister of Citizenship and Immigration provided under Section 14 of the *CSIS Act*; accusations made against the complainant by CSIS during an interview with the complainant; and poor treatment by the Service during an administered polygraph examination.

SIRC concluded there was no evidence to support the allegations concerning the Service's delay in processing the security assessment, or in the manner in which the citizenship interview and polygraph examination were conducted. SIRC found that the Service did not proceed with its investigation with intent to treat the complainant adversely because of his national or ethnic origin. Rather the Service investigated security concerns associated with the complainant's application for Canadian citizenship.

Recommendation

- SIRC recommended that the Canadian Human Rights Commission not investigate this complaint.

[8] The original complaint used the term "security clearance." It should be noted that CSIS provides security *assessments* which form the basis of a clearance issued by the Minister of Citizenship and Immigration. CSIS itself does not issue clearances in these cases. For more information on the security screening process, see Section 2 of this Annual Report.

Alleged actions by CSIS during a citizenship interview

Report 2006–02

SIRC reported a decision concerning a complaint pursuant to Section 41 of the *CSIS Act* dealing with the alleged actions of CSIS during a citizenship interview.

SIRC found that CSIS failed to provide the complainant with proper notice before it conducted the citizenship interview. SIRC found that although CSIS's report to Citizenship and Immigration Canada contained some errors, the report adequately reflected the content of the complainant's citizenship interview.

Recommendation

- SIRC recommended that CSIS implement a procedure to verify that individuals about to be interviewed by CSIS for citizenship or immigration interviews be given adequate written notice by Citizenship and Immigration Canada that CSIS intends to interview them.[9]

Revocation of a security clearance

Report 2006–03

SIRC reported a decision on a complaint pursuant to Section 42 of the *CSIS Act*, concerning the revocation of a security clearance of a CSIS employee, which ultimately led to the employee's dismissal.

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

SIRC concluded there were reasonable grounds to believe the complainant:

- May have knowingly associated with individuals considered to be a security threat;
- Failed to report to CSIS self-admitted suspicions about those individuals' activities; and

[9] SIRC has since been informed by CSIS that CIC is now notifying immigration interviewees about whether or not their interview will be conducted by the Service.

- May have disclosed classified information, which was a breach of security.

SIRC concluded the Director had reasonable grounds to revoke the complainant's security clearance.

Recommendations

SIRC recommended that CSIS:

- Create and implement a policy requiring that its employees be informed of their right to legal representation and be given an opportunity to consult with a legal representative before and while an interview is conducted for the purposes of either a breach of security or a breach of conduct investigation;
- Create a roster of lawyers from the private sector who have a Top Secret clearance whom CSIS employees may retain;
- Create and implement a policy by which its investigators must declare a conflict of interest when an individual seeks their opinion about the retention of legal counsel;
- Create and implement a policy requiring that its employees input relevant information in a timely manner;
- Amend its policy dealing with the destruction of investigative materials—including audio cassettes and notes—concerning a breach of security investigation or a disciplinary investigation;
- Remind its employees that SIRC has the statutory right to access all information under the control of CSIS—except for matters of Cabinet confidence—including audio cassettes, handwritten notes and email messages, and that care should be taken to not destroy information that could have an impact on SIRC's ability to exercise its right to access such information; and
- Place greater emphasis on employees' obligations with respect to the protection of classified information in its orientation course and other security briefings.

Alleged false statements

Report 2006–04

SIRC reported a decision on a complaint made pursuant to Section 41 of the *CSIS Act* by Human Concern International (HCI), alleging that the Service made a false statement to the Federal Court of Canada, via the Minister of Public Safety and the Minister of Citizenship and Immigration. It was further alleged that a document filed by both Ministers was based on CSIS information that the Service knew—or ought to have known—would impugn the character, reputation and

standing of the complainant. Furthermore, HCI maintained that not being party to the court proceedings meant there was no formal opportunity to challenge a statement by the Service that was later published in two Canadian newspapers.

Upon receipt of this complaint, SIRC encouraged the two parties to seek an alternative resolution of this dispute. When these discussions failed, SIRC undertook its own investigation. It found that the Service had made an unsubstantiated allegation about the complainant in its advice to the Ministers of Public Safety and Citizenship and Immigration which was in turn presented to the Federal Court. As well, SIRC found that CSIS knew that reliance would be placed on its advice by both the Ministers of Public Safety and Citizenship and Immigration, as well as the Federal Court. For this reason, and since HCI was not given an opportunity to respond to the impugned statement, CSIS should have taken care to avoid making an unsubstantiated statement which could lead to injury or loss of support and funding.

Recommendations

SIRC recommended that:

- CSIS formally retract this particular statement and that it do so by informing the Minister of Citizenship and Immigration, the Minister of Public Safety, the Federal Court of Canada and the publishers of two newspapers; and
- CSIS apologize to HCI for having made an unsubstantiated statement.

Alleged delay in processing a citizenship application

Report 2006–05

SIRC reported on another complaint made pursuant to Section 41 of the *CSIS Act*, which alleged that CSIS deliberately and improperly caused a delay in the processing of the complainant's citizenship application. The complainant, a permanent resident of Canada, applied for Canadian citizenship and was the subject of a security screening interview conducted by the Service, as requested by Citizenship and Immigration Canada (CIC).[10]

[10] Section 14 of the *CSIS Act* allows the Service to advise any Minister of the Crown on matters relating to the security of Canada, or provide any Minister of the Crown with information relating to security matters or criminal activities.

In this case, CSIS explained to SIRC that the investigator's delay in filing the report of the interview with the complainant had occurred partly due to workload issues in the aftermath of 9/11.

SIRC's authority under Section 41 of the *CSIS Act* does not extend to investigating CIC. Therefore, it was unable to determine CIC's role in any delay in the processing of the complainant's citizenship application. Regarding the Service's role, SIRC found that the Service:

- delayed in scheduling the interview between the complainant and the screening investigator;
- delayed in completing and filing the interview report; and
- contributed to additional delays by recommending that CIC consult with another federal agency.

SIRC determined, however, that these delays—although regrettable—were unforeseeable and found the complainant's allegations were unsupported.

Section 2

CSIS accountability mechanisms

CSIS accountability mechanisms

A. Reporting requirements

CSIS DIRECTOR'S ANNUAL REPORT (2005–06)

Each year, the Director of CSIS must submit a classified report to the Minister of Public Safety, detailing the Service's priorities and operational activities. The *CSIS Act* also requires that the Inspector General of CSIS examine this report and submit a certificate to the Minister, which attests to the extent to which 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*.

According to the Director's Annual Report, the central priorities of the Service are the assurance of public safety and safeguarding of key critical infrastructure. The Director noted that he supports appropriate lawful access legislation to enhance CSIS's ability to meet these priorities. He believes such legislation would enhance intelligence-gathering capabilities and facilitate CSIS's access to modern telecommunications networks.

The investigation of terrorism and terrorist threats to Canada and Canadian interests abroad remain the Service's highest operational priority, in particular the numerous threats posed by Islamist extremism. The Director emphasized that the threat from al Qaida was most acute overseas, and that many of the Service's targets (including some Canadian citizens) are involved in international terrorist groups whose activities directly threaten Canadian interests internationally.

The Service continued to expand its role in supporting Canadian forces abroad. In 2005–06, this included support for Canadian forces in Afghanistan, involvement in the mission to recover Canadian hostages in Iraq and assistance in the evacuation of Canadian citizens from Lebanon. The Director publicly acknowledged these activities in October 2006.

In addition, the Director reported that CSIS had ongoing investigations into many domestic terrorist-related activities, including the threat of serious violence related to Native extremism, militant Quebec nationalism and white supremacist and environmental movements. For the second year, the Director emphasized the threat posed by al Qaida-inspired, homegrown extremists within Canada such as the ongoing criminal proceedings against fifteen individuals living in Toronto.

The Director's report also noted that the Service continued to investigate attempts by foreign countries to conduct espionage, access proprietary technologies and proliferate weapons of mass destruction. Three countries were considered priorities in 2005–06, but many other countries were engaged in similar activities.

The security screening statistics reported by the Director have already been reported in SIRC's 2005–06 annual report. The Director noted that CSIS expanded its security screening responsibilities by signing agreements with two provinces and assumed new obligations under a 2005 tripartite agreement, the Security and Prosperity Partnership of North America.

The Director noted that CSIS expanded its cooperative network with domestic partners by adding two new Memoranda of Understanding in 2005–06. He also reported that CSIS maintains excellent relations with its key foreign partners. Emphasis was also placed on how the Service exercises due diligence concerning the human rights records of partner countries or agencies, and that it continues to provide training to new intelligence services on the principles of intelligence collection in democracies.

Readers should note that CSIS posts public, unclassified reports on its website (**www.csis-scrs.gc.ca**).

CERTIFICATE OF THE INSPECTOR GENERAL OF CSIS (2006)

The position of Inspector General (IG) was established in 1984 under the *CSIS Act*. The IG carries out internal reviews of CSIS on behalf 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 also 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 its powers.

The IG reported being satisfied with the 2005–06 CSIS Director's Annual Report, but noted there were some discrepancies between the statistics reported and the facts provided to the IG. The IG found that the Service had not acted beyond its statutory authority and that it exercised its duties and functions effectively and professionally.

The IG reported that for 2005–06, there was an increase in the number of incidents of non-compliance with operational policy. The IG defines non-compliance as any action that is not in adherence with rules, procedures, principles and guidelines set out in operational policy. She does not differentiate the relative importance of any instance of non-compliance.

Among the concerns brought forward by the IG was that CSIS's 2005 annual direction statement was based on national security intelligence requirements issued to CSIS by an ad-hoc Cabinet Committee. According to the IG, the national requirements become a Cabinet Confidence and therefore limit the IG's right of access to all CSIS information.

The IG found several cases where information was mishandled, including cases where her staff found discrepancies and inaccuracies in CSIS files, as well as instances where CSIS was unable to locate or retrieve documentation requested.

The IG identified several gaps in current CSIS policy. She noted that the policy framework did not reflect the current procedures for the approval of information exchanges with partner agencies. The IG observed that there is a growing disconnect between policy and practice with respect to the execution of warrant powers.

Section 16 of the *CSIS Act* requires the Service to limit the collection of foreign intelligence to within Canada, while security intelligence collected under Section 12 may be obtained within Canada and abroad.[11] In her 2006 certificate, the IG noted considerable overlap between the Service's Section 12 and Section 16 investigations, leading her to conclude that in some cases, the effect of the geographical restriction of Section 16 is meaningless.

Finally the IG concluded that she observed a gap in operational policies governing certain CSIS operations overseas.

For more information, please refer to the Inspector General's home page on the Public Safety website (**publicsafety.gc.ca**).

[11] See SIRC review 2006-04 for details on a Section 16 activity.

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 or functions. The Minister, in turn, must send the report with his or her comments to the Attorney General of Canada and to SIRC. In 2006–07, no CSIS employees acted unlawfully, and no such reports were issued.

DISCLOSURES OF INFORMATION

Section 19 of the *CSIS Act* prohibits information obtained by the Service in the course of its investigations from being disclosed except in the following specific circumstances:

1. 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;
2. information related to the conduct of Canada's external relations may be disclosed to the Minister of Foreign Affairs;
3. information related to the defence of Canada may be disclosed to the Minister of National Defence; and
4. 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.

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. This is an exceedingly rare occurrence—there have been only two disclosures under this Section of the *Act*.

The Service may also disclose information verbally or in writing 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 in judicial proceedings, it must do so in writing.

The Service provided over 130 disclosure letters during fiscal year 2006–07.

B. Foreign and domestic arrangements

Sections 13 and 17 of the *CSIS Act* allow CSIS to enter into arrangements with foreign and domestic organizations or agencies in order to perform its duties and functions. SIRC receives copies of these arrangements as they are initiated, and examines a selection of them every year.

ARRANGEMENTS WITH DOMESTIC AGENCIES

CSIS often collaborates with federal departments and agencies, provincial governments and law enforcement agencies. Since 9/11, more groups have been involved in national security, including police forces and other government partners. 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.

Although many domestic arrangements take the form of a Memorandum of Understanding (MOU), CSIS may collaborate with any domestic agency whether or not an MOU is in place. As of March 31, 2007, CSIS had 35 MOUs with domestic partners: 19 with federal departments or agencies and 16 with provincial and municipal entities.

In September 2006, the Service updated its MOU with the RCMP. The updated MOU reflects new mechanisms of cooperation and consultation between the two organizations. The MOU also outlines the implementation of a national counter-terrorism strategy to facilitate CSIS-RCMP cooperation and coordination. It establishes counter-terrorism threat overview and investigative priorities common to both organizations, as well as developing joint training programs.

ARRANGEMENTS WITH FOREIGN AGENCIES

As of March 31, 2007, CSIS had 271 foreign arrangements with agencies in 147 countries. 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 Minister approved seven new arrangements in 2006–07, and expanded six existing ones.

On occasion, the Service must alter foreign arrangements—to accommodate a change in the foreign partner[12], to reactivate a dormant relationship, or to place an arrangement into dormancy. Eight arrangements were altered during the year under review. Another eight were restricted.

The Director of CSIS has the discretion to approve the expansion or alteration of a foreign arrangement without Ministerial approval. These remain subject to any Ministerial caveats or instructions that may have been imposed when the initial arrangement was approved.

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

- CSIS foreign arrangements were in accordance 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 was considered; and
- the most recent arrangement profile met CSIS guidelines.

In 2006–07, SIRC reviewed 19 foreign arrangements with agencies in 14 countries. SIRC found that all foreign arrangements were in accordance with the *CSIS Act*, Ministerial Direction and operational policies.

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.

SIRC also observed an improvement in the timely submission of arrangement profiles. All of the profiles reviewed by SIRC reflected the current security, human rights and political environment of the countries and agencies in question.

[12] These changes can include merging of two agencies into one, or a change in agency name.

C. Policy and governance

NATIONAL REQUIREMENTS FOR SECURITY INTELLIGENCE

The Minister of Public Safety issues National Requirements for Security Intelligence, which contain general direction from government regarding where CSIS should focus its investigative efforts, as well as guidance on the Service's collection, analysis and advisory responsibilities.

The 2006–08 National Requirements direct the Service to continue to maintain a flexible capability to meet Canada's evolving security intelligence needs by relying on risk management. The Minister notes that today's threat environment is increasingly international and transnational in nature, with many offshore threats to Canada's security requiring foreign investigations. CSIS is therefore directed to continue to investigate threats to Canada's security both within Canada and abroad.

For 2006–08, the Minister has directed CSIS to pursue the following security intelligence priorities:

- Safeguarding against—and advising the government of—the possibility of a terrorist attack occurring in or originating from Canada, or affecting Canadian citizens or assets abroad;
- Continuing to conduct research and analysis in support of the listing of terrorist entities under the *Criminal Code of Canada* and combating terrorist financing;
- Supporting the Government of Canada's efforts in Afghanistan;
- Working closely with other government departments to combat transnational criminal activity;
- Investigating threats to Canada's national security arising from activities of countries that engage in espionage;
- Continuing to identify and investigate countries and groups that have or may attempt to acquire weapons of mass destruction, and advising the government of the threats posed by these activities;
- Supporting the collection of foreign intelligence in Canada to assist the Minister of Foreign Affairs and/or the Minister of National Defence pursuant to Section 16 of the *CSIS Act*;
- Delivering security screening programs to federal departments, agencies and other clients;
- Providing the Government of Canada with intelligence assessments and ensuring that CSIS keeps itself informed of political, social and economic environments from which threats to the security of Canada may emerge; and

- Ensuring CSIS's technical equipment and information systems meet the requirements of its investigations.

MINISTERIAL DIRECTION

Under Section 6(2) of the *CSIS Act*, the Minister of Public Safety may issue written directions governing CSIS's activities and investigations. The last time the Minister issued such direction was in 2001, when a compendium was provided to SIRC. In June 2007, however, SIRC received the latest *National Requirements for Security Intelligence* for 2006–08 (no direction was issued for 2005–06).

CHANGES IN CSIS OPERATIONAL POLICY

CSIS administrative, security, human resources and operational policies embody rules and procedures that govern the range of activities undertaken by the Service. Administrative, security and human resources policies are all internal corporate policies. Operational policies, which describe how CSIS employees should perform their duties, are updated regularly in accordance with government policy, legislative and other changes. They are reviewed by SIRC to ensure that they conform to the *CSIS Act* and Ministerial Direction.

In 2006–07, CSIS revised and/or published over 120 policies. Some revisions were administrative in nature. The remainder were of an operational nature and pertained to, among other things, warrant acquisition and approvals for Section 12 and 16 investigations. Although no new policies were developed as a result of CSIS's organizational realignment, 14 corporate and 77 operational policies were amended (see **CSIS operational activities**).

One of the policy projects the Service undertook in 2006–07 was the Director's "Delegation of Responsibility" project—a review of all operational policies to determine where executive and management responsibilities must be delegated. CSIS informed SIRC that this project is ongoing and that it would share the results upon its completion.

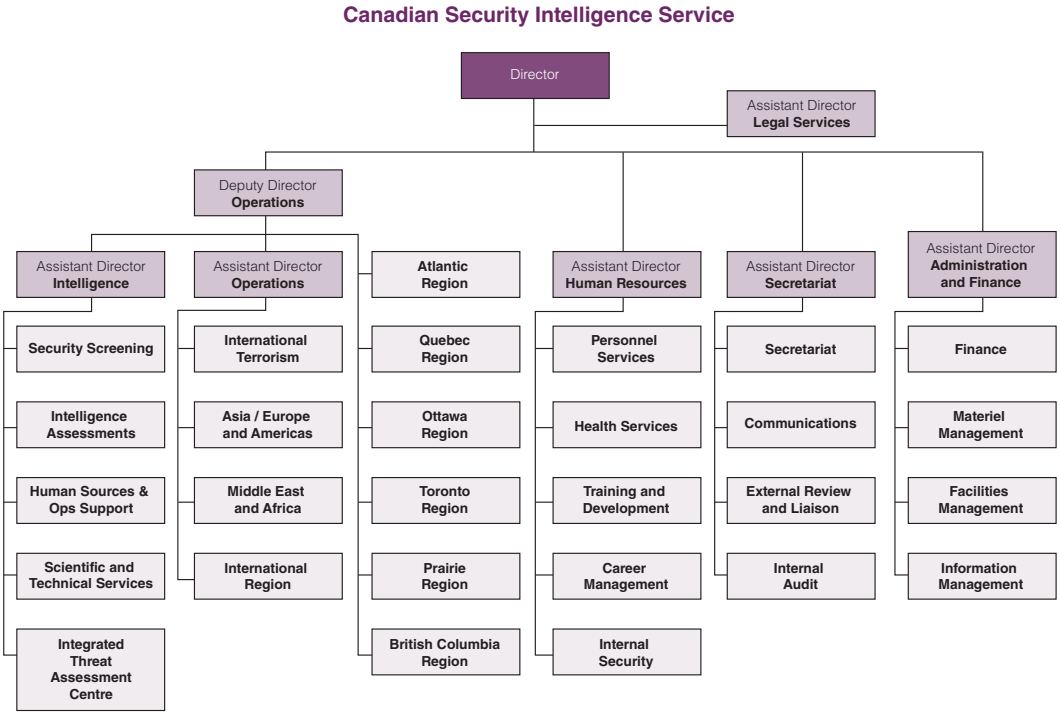
GOVERNOR-IN-COUNCIL REGULATIONS AND APPOINTMENTS

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 2006–07.

D. CSIS operational activities

In May 2006, CSIS implemented a new operational structure. According to the Service, this realignment of resources was designed to ensure that CSIS could increase its operational capacity, consolidate and enhance analysis and production facilities and improve corporate support. The Deputy Director Operations, who reports to CSIS's Director, is now responsible for three groups:



1. **Intelligence**, consisting of five branches: Security Screening; Intelligence Assessments; Human Sources and Operations Support; Scientific and Technical Services; and the Integrated Threat Assessment Centre;
2. **Operations**, consisting of three branches and one region: International Terrorism; Middle East and Africa; Asia, Europe and Americas; and International Region; and
3. **Six regions.**

The functions of these groups are highlighted below.

1. Intelligence

SECURITY SCREENING BRANCH

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

Government screening performs security clearance investigations for all government employees[13] whose duties require them to access classified assets or information. The results of these investigations are security assessments—an appraisal of an individual's reliability as it relates to loyalty to Canada—which are provided to the requesting department or agency. Traditionally, the largest clients of this service have been Public Works and Government Services Canada and the Department of National Defence (DND)—accounting for over 28 percent and 26 percent respectively of all requests in 2006–07.

As indicated in Table 2, in 2006–07, CSIS received 51,200 requests for new or updated security clearances and provided 55,000 security assessments to federal departments. The volume of requests increased by approximately 22 percent from the previous fiscal year, and the number of security assessments issued by CSIS increased by 46 percent compared with previous years.

[13] CSIS does not conduct security clearance investigations on behalf of Canada's national police force. The RCMP conducts these investigations on its own behalf.

Table 2
CSIS government security screening*

	2004-05	2005-06	2006-07
Requests from DND	9,100	9,200	13,100
Requests from other departments or agencies	27,400	32,900	38,100
Total	**36,500**	**42,100**	**51,200**
Assessments issued to DND	9,000	8,900	13,100
Assessments issued to other departments or agencies[14]	27,600	28,900	41,800
Total	**36,600**	**37,800**	**55,000**

* Figures have been rounded to the nearest 100.

To track its efficiency in responding to security screening requests, CSIS calculates its turnaround times using a median number of days. As indicated in Table 3, the median turnaround times increased over the previous year's levels in all but one case. The time it took to process a Level I clearance more than doubled for departments other than DND.

Table 3
Median turnaround time (in calendar days)

		2004–05	2005–06	2006–07
DND	Level I (Confidential)	49	24	40
	Level II (Secret)	63	19	40
	Level III (Top Secret)	70	39	82
Non-DND	Level I (Confidential)	12	15	32
	Level II (Secret)	14	13	21
	Level III (Top Secret)	69	60	47

[14] This number includes assessments performed for provincial governments and for access to nuclear facilities.

The Service does not decide who receives a security clearance. Rather, it advises the requesting department or agency of information that could have an impact on their decision to grant a 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 2006–07, the Service issued 14 information briefs reporting information of an adverse nature. No denial briefs were issued.

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 buildings or provides accreditation for a special event. In 2006–07, CSIS received over 83,900 requests for this type of screening, and provided three information briefs to requesting agencies. The increase in requests for access to nuclear facilities, which rose by roughly 69 percent, is a result of a five-year renewal cycle for pre-existing clearances.

There were no special events for which the Service provided assessments. All other site-access requests remained close to levels of previous years.

Table 4
Site-access screening*

	2004–05	2005–06	2006–07
Parliamentary precinct	1,100	1,000	1,100
Airport restricted-access area	31,100	37,600	39,300
Nuclear facilities	6,800	10,600	17,900
Canada Border Services Agency (CBSA) / Free and Secure Trade (FAST)[15]	21,500	3,100	23,100
Special events accreditation	1,800	5,600	0
Other government departments	2,300	2,400	2,500
Total	**64,600**	**60,300**	**83,900**

* Figures have been rounded to the nearest 100.

[15] The FAST program came into effect in 2004–05. The data for 2006–07 represents screening requests for both FAST and CBSA, which CSIS is now calculating together.

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 requires the Security Screening Branch to conduct investigations and to provide 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 Section 34(1) of the *Immigration and Refugee Protection Act.*

In 2006–07, the branch received 92,300 requests under various immigration screening programs (see Table 5). The number of requests received within and from outside Canada and the number of refugee determination and front-end screening requests were almost the same as the previous year.

Table 5
Immigration security screening

	Requests*			Briefs		
	2004–05	2005–06	2006–07	2004–05	2005–06	2006–07
Within and outside Canada[16]	56,100	63,200	62,800	88	133	201
Front-end Screening[17]	22,900	17,100	17,900	184	89	143
Refugee determination[18]	14,200	11,700	11,600	110	127	153
Subtotal	**93,200**	**92,000**	**92,300**	**382**	**349**	**497**
Citizenship applications	161,200	308,000	227,300	124	120	155
Total	**254,400**	**400,000**	**319,600**	**506**	**469**	**652**

* Figures have been rounded to the nearest 100.

CSIS finds no adverse information in the vast majority of its screening investigations of refugee claimants or immigration/citizenship candidates. In 2006–07 the Service issued 157 information briefs, 44 inadmissibility briefs and 2 incidental letters related to immigration cases.

As has been the case in recent years, the Service's turnaround times for providing information or inadmissibility briefs were generally quite lengthy. Information briefs related to immigration cases took a median of 460 calendar days for an application filed in Canada, 620 days for those filed from the United States and 161 days for those filed abroad. Information briefs related to permanent resident applicants who are refugees in Canada had a median turnaround time of 442 days, and those for files subject to the Front-End Screening program had a turnaround time of 365 days. For inadmissibility briefs, SIRC noted similar median times.

[16] This includes permanent residents from within and outside Canada (excluding the Refugee Determination Program), permanent residents from within the United States and applicants from overseas.

[17] Individuals who arrive at the Canadian border or other ports of entry claming refugee status.

[18] Refugees, as defined by *IRPA*, who apply from within Canada for permanent resident status.

Table 6 provides a three-year highlight of the Service's median turnaround time in providing notices of assessment.

Table 6
Median turnaround time (in days) for notices of assessment

	2004–05	2005–06	2006–07
Citizenship	1	1	1
Immigration (Canada)[19]	44	70	78
Immigration (USA)[20]	150	62	29
Overseas immigration	7	16	14
Refugee determination	56	96	98
Front-end screening	27	23	19

Other screening activities

In 2006–07, the Security Screening Branch vetted 114,500 visa applications of foreign nationals. The Branch also continued to provide screening for various site-access programs. For more information on this branch's security screening activities, refer to SIRC Review 2006–07 in this year's annual report.

New programs

The Security Screening Branch was involved in three new programs:

- **The Marine Facilities Restricted Area Access Control Program**—designed to provide security assessments to ensure security of Canada's ports;
- **The Trusted Traveller Program**—a pre-clearance program for travellers who travel frequently to the United States. This program is currently under development and there is no date set for its implementation; and
- **Passenger Protect**—the Branch worked with other government departments in the development of airline passenger screening programs, in particular the domestic "no fly" program, which became operational on June 18, 2007.

---

[19] This includes certain classes of individuals who apply for permanent resident status within Canada.

[20] This includes persons who have been legally admitted to Canada for at least one year, and who may submit their application to Citizenship and Immigration offices in the United States.

INTELLIGENCE ASSESSMENTS BRANCH

The Intelligence Assessments Branch (formerly Research, Analysis and Production) consolidates the key analytical function of the Service and centralizes its main intelligence reporting mechanisms. It develops strategic and operational analyses of current threats and emerging issues, and produces Intelligence Briefs, Threat and Risk Assessments, Studies and Pathfinders.

This branch also has a role in the Terrorist Entity Listing process. Every two years, the Minister of Public Safety is obliged, under the *Criminal Code*, to review the Terrorist Entity Listing to determine whether there are reasonable grounds to add or remove entities from the list. The Minister bases this assessment on Security Intelligence Reports prepared by CSIS. In 2006–07, the Branch developed two such reports. The Minister's review of the listing was completed and approved by the Governor-in-Council on November 9, 2006.

HUMAN SOURCES AND OPERATIONS SUPPORT BRANCH

This branch provides a range of support and coordination services including risk management for operational activities across the Service. It is the policy centre in a number of areas including operational security, multilingual services and management of human sources. It also houses the Threat Management Centre, which provides 24/7 support to operational staff in headquarters, regional offices and foreign offices, and coordinates the Service's participation in major events such as the upcoming 2010 Winter Olympic Games in Vancouver.

SCIENTIFIC AND TECHNICAL SERVICES BRANCH

This branch develops and deploys technical tools and mechanisms to support the operations and investigations of CSIS's other branches.

INTEGRATED THREAT ASSESSMENT CENTRE

The Integrated Threat Assessment Centre (ITAC) produces assessments that warn the government about terrorist threats to Canada and to Canadian interests abroad. Once completed, ITAC's threat assessments are distributed to domestic and foreign partners. Additionally, ITAC acts as a distribution hub for threat assessments produced by counterparts in the United States, the United Kingdom, Australia and New Zealand.[21]

---

[21] For more information about ITAC, refer to Section 1 of SIRC's 2005–06 Annual Report.

During the period under review, ITAC issued 83 threat assessments and redistributed 1,150 others produced by allied fusion centres. ITAC also began publishing *Media Watch* advisories at the beginning of the fiscal year, which are published each business day for distribution to clients. Further, ITAC provided 90 threat assessment briefings to its domestic clients. Presentations were provided to several government departments, including the Canada Revenue Agency and the Canada Border Services Agency. Also of note, ITAC produced one threat assessment at the request of the National Security Advisor.

In its previous annual report, SIRC observed that ITAC was not fully staffed but ITAC reported that as of March 31, 2007, the Centre was fully staffed.

2. Operations

Since the May 2006 realignment, each operational branch is responsible for investigating all threats emanating from within their respective geographic areas, with the exception of the International Terrorism Branch, which focuses exclusively on al Qaida and al Qaida- inspired groups regardless of geographic boundaries.

INTERNATIONAL TERRORISM BRANCH

This branch conducts investigations globally and within Canada, focusing on Islamist extremists engaged in a variety of terrorist-related activities which pose a direct threat to Canadians and Canadian interests. Notable among this branch's areas of interest is the radicalization of Islamists within Canada.

MIDDLE EAST AND AFRICA BRANCH

The Middle East and Africa Branch concentrates its investigative effort on threats that emanate from, or have as their major focus in, Middle East and African countries. This includes issues of terrorism, foreign-influenced activities, the proliferation of weapons of mass destruction and espionage.

ASIA, EUROPE AND AMERICAS BRANCH

This branch investigates threats emanating from its vast area of geographic responsibility, namely espionage, terrorism (including domestic extremism) transnational criminal activity and foreign-influenced activities.

INTERNATIONAL REGION

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

As part of CSIS's realignment, a new category of position, Foreign Officers (FO), was created. FO is the Service's generic term for any CSIS employee working at a post or mission abroad. FOs can include the formerly named Security Liaison Officers, the administrative assistants who support them, temporary duty officers who are working in a post, technical officers assigned to a post, and foreign secondment officers. FOs duties include:

- Management and collection of information on threats to the security of Canada;
- Management and collection of immigration security assessments;
- Liaison with foreign governments or institutions; and
- Collaborating and sharing information with staff at Canada's missions abroad.

The Service relies on these foreign posts to assist in liaising with foreign security and intelligence agencies, as well as to coordinate visits to CSIS Headquarters and regional offices by foreign representatives. SIRC's most recent examination of one of these foreign posts is summarized in SIRC Review 2006–01 in this year's annual report.

FEDERAL COURT WARRANTS AND WARRANT STATISTICS

Warrants are one of the most powerful and intrusive tools available to the Service. They provide CSIS with Federal Court authorization to use investigative techniques that would otherwise be illegal, such as the monitoring of telephone communications. For this reason, the use of warrants by CSIS is an important aspect of SIRC's reviews.

Each year, SIRC collects statistics on the Service's warrant applications and on warrants granted by the Federal Court under Sections 12 and 16 of the *CSIS Act*. SIRC does not have the resources to examine all warrants granted to the Service. It does, however, look at a certain number of warrants as part of its annual review activity.

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:

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

SIRC also looks at the actual warrant approved by the Federal Court and the Service's execution of warrant powers (i.e., how the warrant powers were used by CSIS).

Table 7
Warrant Statistics

	2004–05	2005–06	2006–07
New warrants	40	24	42
Replaced or renewed	207	203	134
Total	**247**	**227**	**176***

* Included in this number were 25 urgent warrants.

In 2006–07, the Federal Court approved 42 new warrants—almost twice as many as the previous year. However, the Federal Court approved the renewal or replacement of only 134 warrants—a sharp drop from 203 reported in the previous year. Forty-two warrants were either terminated or expired without being renewed during the same period. No warrant applications were denied and all warrant powers requested by the Service were granted by the Federal Court.

In SIRC's 2005–06 annual report, SIRC reported on CSIS's review of the warrant process, which stemmed from a moratorium imposed by the Director after a warrant application was rejected by the Federal Court.[22] During this moratorium—in effect from June 22, 2005 to June 28, 2006—there were 38 warrants approved on an exceptional basis by the Director and the Service's General Counsel. As a result of a year-long assessment of the warrant process, CSIS reported to SIRC that it is finalizing a streamlined approach to warrant review which is expected to be in effect by late 2007.

In preparing this report, SIRC asked the Service if the Federal Court had asked for any warrant applications to be modified before they were approved. Three instances were reported.

[22] For more information on the moratorium, see "Federal Court Warrant and Warrant Statistics" in Section 2 of SIRC's 2005–06 Annual Report.

Section 3

About SIRC

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 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, direct staff to undertake reviews, prepare complaint reports in consultation with staff, visit CSIS regional offices, appear before Parliament and exercise other duties associated with their responsibilities.

SIRC meetings and briefings 2006–07

April 5, 2006: The Chair spoke to the Associates of the I.H. Asper School of Business at the University of Manitoba in Winnipeg.

May 1, 2006: The Associate Executive Director and the Senior Counsel met with a delegation from the Czech Parliament.

May 12, 2006: The Chair and Executive Director delivered a presentation to Federal Court Judges regarding SIRC's warrant reviews.

June 8, 2006: The Associate Executive Director and Senior Researchers attended the third Review Agencies Forum hosted by the Inspector General of CSIS. In attendance were officials from the Commissioner of the Communications Security Establishment, the Inspector General of CSIS, and the Commission for Public Complaints Against the RCMP.

September 19, 2006: The Executive Director, the Associate Executive Director and the Senior Counsel met with Sir Peter Gibson, UK Intelligence Services Commissioner, his assistant David Massam and a representative from the UK High Commission.

September 22, 2006: The Chair spoke to the Global Business Forum in Banff, Alberta.

September 26, 2006: The Executive Director, the Associate Executive Director and the Senior Counsel met with a Norwegian Parliamentary Committee.

Continued on the next page

SIRC meetings and briefings 2006–07
(continued)

October 2–4, 2006: The Chair, one Committee Member and the Executive Director attended the International Intelligence Review Agencies Conference in Cape Town, South Africa. The Chair also participated in a panel discussion.

October 10, 2006: The Executive Director spoke at a Carleton University seminar on Intelligence, Statecraft and International Affairs.

October 26–28, 2006: The Executive Director and several staff attended the annual conference of the Canadian Association of Security and Intelligence Studies, held in Ottawa.

November 1, 2006: The Chair, the Members of the Committee, the Executive Director, the Associate Executive Director and the Senior Counsel appeared before the Standing Committee on Public Safety and National Security of the House of Commons.

November 17, 2006: The Executive Director spoke at a Carleton University seminar entitled National Security and Intelligence in the Modern State.

December 10, 2006: The Chair appeared on CTV's *Question Period.*

January 31, 2007: The Associate Executive Director, Senior Counsel and Senior Researchers attended the fourth Review Agencies Forum, hosted by the Commission for Public Complaints Against the RCMP.

STAFFING AND ORGANIZATION

SIRC is supported by an Executive Director, Susan Pollak, and an authorized staff complement of 20, located in Ottawa. The staff comprises: an Associate Executive Director, Senior Counsel, a Senior Advisor, a Corporate Services Manager, Counsel, a Senior Paralegal (who also serves as Access to Information and Privacy Officer/Analyst), plus researchers and administrative staff.

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

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, and other experts.

SIRC also visits CSIS regional offices on a rotating basis to examine 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 2006–07, SIRC visited two regional offices.

BUDGET AND EXPENDITURES

SIRC continues to manage its activities within allocated resource levels. Staff salaries and travel within Canada for Committee meetings, hearings, briefings and review activities represent SIRC's chief expenditures. Table 8 below presents a breakdown of actual and estimated expenditures.

Table 8
SIRC expenditures 2006–07

	2006–07 (Actual)	2006–07 (Estimates)
Personnel	$1,817,160	$1,777,000
Goods and Services	$809,674	$1,019,000
Total	**$2,626,834**	**$2,796,000**

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

The public may make requests to SIRC under both the *Access to Information Act* and the *Privacy Act*. Table 9 outlines the number of requests SIRC has received under these Acts for the past three fiscal years.

Requests for SIRC's reviews represent the largest portion of these requests. SIRC waives the application fees for all such requests.

Table 9
Requests for release of information

	2004–05	2005–06	2006–07
Access to Information Act	21	17	12
Privacy Act	3	5	2

COMMUNICATIONS

Although SIRC's annual report is the main communications vehicle for informing Parliament and Canadians about its work, it has also 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.

On occasion, the Committee is invited to attend and speak at conferences. In September 2006, the Chair delivered a speech to the Global Business Forum in Banff, Alberta, concerning "Global Threats to National Security." In it, he examined the impact of the current threat environment on Canada's economic security and well-being, described CSIS's role in combating such threats and explained SIRC's review functions.

In October 2006, the Chair delivered a speech on "Country Experiences: Oversight Mechanisms, Challenges and Opportunities" at the International Intelligence Review Agencies Conference, held in Cape Town, South Africa. This biannual conference brings together review agencies similar to SIRC to discuss issues of common concern. The Executive Director and another Member of the Committee were also in attendance.

SIRC's website represents another important communications vehicle. It is continually updated with information relevant to the security and intelligence community. All of SIRC's annual reports since its creation are available, plus copies of speeches, backgrounders and other publications, as well as information on the roles and responsibilities of SIRC.

As principal spokesperson, SIRC's Chair has met with journalists to discuss SIRC's work and appeared on CTV's *Question Period*. He also wrote an op-ed piece, which was published in the *Calgary Herald*.

MANAGEMENT ACCOUNTABILITY

SIRC continues to make progress in this area, although as a very small federal agency without dedicated staff responsible for financial and human resource management, SIRC must increasingly rely on external contractors, diverting resources from its core functions.

In 2006–07, SIRC developed a financial management framework to improve the allocation and monitoring of expenditures. The latter aspect has been delayed, however, by technical problems related to software transition, preventing SIRC from realizing the full benefits of a modernized and automated monitoring of its expenditures.

In June 2006, SIRC received the results of an independent, external audit, which was a condition of receiving additional funding approved by Parliament in 2004. This audit found that "SIRC's internal processes are reasonably well-controlled, thus enabling SIRC to properly manage the expenditure of public funds with prudence and probity." Coincidentally, the Treasury Board Secretariat initiated

another audit of hospitality and travel expenses of small federal agencies and included SIRC in its ambit. The results of this second audit are expected to be published by the Treasury Board Secretariat in the coming year.

Following the successful development of a Management Action Plan and Risk Assessment in 2004–05, SIRC participated in an online reporting exercise under the government-wide Management Accountability Framework. The results of this exercise will be published by the Treasury Board Secretariat.

Also, SIRC completed a threat and risk assessment by an accredited security officer from the Privy Council Office to ensure compliance with the Management of Information Technology Security initiative. SIRC has also enhanced physical security by upgrading its alarm system and further shielding its hearing room.

Appendix A

SIRC reviews since 1984

SIRC reviews since 1984

This listing is also available on the SIRC website at www.sirc-csars.gc.ca. Section 54 reports—flagged with an *—are special reports the Committee makes to 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 and CSE*, Section 40 (TOP SECRET) (91/92-04) *

35. *Victor Ostrovsky* (TOP SECRET) (91/92-05)

36. *Report on Two Iraqis—Ministerial Certificate Case* (SECRET) (91/92-06)

37. *Threat Assessments, Section 40 Study* (SECRET) (91/92-07) *

38. *The Attack on the Iranian Embassy in Ottawa* (TOP SECRET) (92/93-01) *

39. *"STUDYNT" The Second CSIS Internal Security Case* (TOP SECRET) (91/92-15)

40. *Domestic Terrorism Targets—A SIRC Review* (TOP SECRET) (90/91-13) *

41. *CSIS Activities with respect to Citizenship Security Screening* (SECRET) (91/92-12)

42. *The Audit of Section 16 Investigations* (TOP SECRET) (91/92-18)

43. *CSIS Activities during the Gulf War: Community Interviews* (SECRET) (90/91-12)

44. *Review of CSIS Investigation of a Latin American Illegal* (TOP SECRET) (90/91-10) *

45. *CSIS Activities in regard to the Destruction of Air India Flight 182 on June 23, 1985*—A SIRC Review (TOP SECRET) (91/92-14) *

46. *Prairie Region—Report on Targeting Authorizations* (Chapter 1) (TOP SECRET) (90/91-11) *

47. *The Assault on Dr. Hassan Al-Turabi* (SECRET) (92/93-07)

48. *Domestic Exchanges of Information* (A SIRC Review—1991/92) (SECRET) (91/92-16)

49. *Prairie Region Audit* (TOP SECRET) (90/91-11)

50. *Sheik Rahman's Alleged Visit to Ottawa* (SECRET) (CT 93-06)

51. *Regional Audit* (TOP SECRET) (September 1993)

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 and Foreign Intelligence 1997–98* (TOP SECRET) (SIRC 1998-07)

110. *Review of Intelligence Production* (SECRET) (SIRC 1998-09)

111. *Regional Audit* (TOP SECRET) (SIRC 1998-10)

112. *CSIS Liaison with Foreign Agencies* (TOP SECRET) (SIRC 1998-11)

113. *Allegations by a Former CSIS Employee* (TOP SECRET) (SIRC 1998-12) *

114. *CSIS Investigations on University Campuses* (SECRET) (SIRC 1998-14)

115. *Review of Foreign Intelligence Activities in Canada* (TOP SECRET) (SIRC 1998-15)

116. *Files* (TOP SECRET) (SIRC 1998-16)

117. *Audit of Section 16 Investigations and Foreign Intelligence* (TOP SECRET) (SIRC 1999-01)

118. *A Long-Running Counter Intelligence Investigation* (TOP SECRET) (SIRC 1999-02)

119. *Domestic Exchanges of Information* (TOP SECRET) (SIRC 1999-03)

120. *Proliferation* (TOP SECRET) (SIRC 1999-04)

121. *SIRC's Comments on the Draft Legislation Currently Before Parliament—Bill C-31* (PROTECTED) (SIRC 1999-05) *

122. *Domestic Targets* (TOP SECRET) (SIRC 1999-06)

123. *Terrorist Fundraising* (TOP SECRET) (SIRC 1999-07)

124. *Regional Audit* (TOP SECRET) (SIRC 1999-08)

125. *Foreign State Activities* (TOP SECRET) (SIRC 1999-09)

126. *Project Sidewinder* (TOP SECRET) (SIRC 1999-10) *

127. *Security Breach* (TOP SECRET) (SIRC 1999-11)

128. *Domestic Exchanges of Information 1999–2000* (TOP SECRET) (SIRC 2000-01)

129. *Audit of Section 16 Investigations and Foreign Intelligence Reports 1999–2000* (TOP SECRET) (SIRC 2000-02)

130. *CSIS Liaison with Foreign Agencies* (TOP SECRET) (SIRC 2000-03)

131. *Regional Audit* (TOP SECRET) (SIRC 2000-04)

132. *Warrant Review* (TOP SECRET) (SIRC 2000-05)

133. *Review of CSIS Briefs to Citizenship and Immigration Canada 1999–2000* (TOP SECRET) (SIRC 2001-02)

134. *CSIS Investigation of Sunni Islamic Extremism* (TOP SECRET) (SIRC 2002-01)

135. *Source Recruitment* (TOP SECRET) (SIRC 2001-01)

136. *Collection of Foreign Intelligence* (TOP SECRET) (SIRC 2001-05)

137. *Domestic Extremism* (TOP SECRET) (SIRC 2001-03)

138. *CSIS Liaison with Foreign Agencies: Audit of an SLO Post* (TOP SECRET) (SIRC 2001-04)

139. *Warrant Review* (TOP SECRET) (SIRC 2001-06)

140. *Special Report following allegations pertaining to an individual* (TOP SECRET) *

141. *Audit of Section 16 and Foreign Intelligence Reports* (TOP SECRET) (SIRC 2002-02)

142. *Review of the Ahmed Ressam Investigation* (TOP SECRET) (SIRC 2002-03)

143. *Lawful Advocacy, Protest and Dissent Versus Serious Violence Associated with the Anti-Globalization Movement* (TOP SECRET) (SIRC 2002-04)

144. *Regional Audit* (TOP SECRET) (SIRC 2002-05)

145. *Special Report (2002-2003) following allegations pertaining to an individual* (TOP SECRET) *

146. *Front End Screening Program* (TOP SECRET) (SIRC 2003-01)

147. *CSIS Section 12 Operational Activity Outside Canada* (TOP SECRET) (SIRC 2003-02)

148. *Review of a Counter-Intelligence Investigation* (TOP SECRET) (SIRC 2003-03)

149. *Review of a Counter-Proliferation Investigation* (TOP SECRET) (SIRC 2003-04)

150. *CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post* (TOP SECRET) (SIRC 2003-05)

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. *Section 54 Report to the Minister of Public Safety: Review of the case of Mohammed Mansour Jabarah* (TOP SECRET) (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)

170. *Review of a Security Liaison Post* (TOP SECRET) (SIRC 2006-01)

171. *Review of Activities and Investigations in a CSIS Regional Office* (TOP SECRET) (SIRC 2006-02)

172. *Review of a Counter-Terrorism Investigation* (TOP SECRET) (SIRC 2006-03)

173. *Review of a Section 16 activity* (TOP SECRET) (SIRC 2006-04)

174. *Review of a Counter-Terrorism Investigation* (TOP SECRET) (SIRC 2006-05)

175. *Review of CSIS's collaboration and exchanges of intelligence post-9/11* (TOP SECRET) (SIRC 2006-06)

176. *Review of Security Screening outside of the Federal Government* (TOP SECRET) (SIRC 2006-07)

177. Review 2006-08 had not been finalized at the time this annual report went to print. A summary of this review will appear in SIRC's 2007–08 annual report.

178. *Review of the CSIS Counter Espionage Investigations Desk* (TOP SECRET) (SIRC 2006-09)

Appendix B

Recommendations

Recommendations

During 2006–07, SIRC made 19 recommendations, 8 stemming from reviews it conducted and 11 from complaints investigations. These are summarized below.

	SIRC recommended that…
Review 2005-05	• The 1987 Memorandum of Understanding between CSIS and the Department of Foreign Affairs and International Trade be updated to designate Foreign Affairs as the lead agency in cases involving Canadian citizens detained abroad. • CSIS amend its policies so that emails are automatically retained unless there is a conscious decision to delete them. • CSIS clearly communicate to its employees what would constitute "recorded information," as distinct from "transitory records," and should therefore be filed and retained under applicable federal legislation. • Whenever possible, CSIS keep written records of its interdepartmental consultations, including but not limited to its formal and informal consultations with the Departments of Foreign Affairs and Justice. • CSIS ensure that the storage, retention and retrieval of all operational information under its control, including email messages, is in accordance with applicable federal legislation, including the *CSIS, Privacy*, *Access to Information* and *Library and Archives of Canada Acts*. • CSIS request and obtain written advice from the Department of Justice in operations where an individual is questioned in circumstances which may give rise to a detention, in order to ensure that the individual's *Charter* rights are respected, and in all occasions when it is unclear whether the Service's activity falls within its statutory mandate under Section 12 of the *CSIS Act*.
Review 2006-07	• CSIS create policy to address the varying degrees of risk of screening applicants, and to ensure that these briefs are uniform and consistent. • CSIS obtain written consent forms for security assessments in cases where the Service cannot access them after the fact (i.e., foreign agencies).

	SIRC recommended that…
Report 2006-01	• The Canadian Human Rights Commission not investigate this complaint.
Report 2006-02	• CSIS implement a procedure to verify that individuals about to be interviewed by CSIS for citizenship or immigration interviews be given adequate written notice by Citizenship and Immigration Canada that CSIS intends to interview them.
Report 2006-03	• CSIS create and implement a policy requiring that its employees be informed of their right to legal representation and be given an opportunity to consult with a legal representative before and while an interview is conducted for the purposes of either a breach of security or a breach of conduct investigation. • CSIS create a roster of lawyers from the private sector who have a Top Secret clearance whom CSIS employees may retain. • CSIS create and implement a policy by which its investigators must declare a conflict of interest when an individual seeks their opinion about the retention of legal counsel. • CSIS create and implement a policy requiring that its employees input relevant information in a timely manner. • CSIS amend its policy dealing with the destruction of investigative materials—including audio-cassettes and notes—concerning a breach of security investigation or a disciplinary investigation. • CSIS remind its employees that SIRC has the statutory right to access all information under the control of CSIS—except for matters of Cabinet confidence—including audio cassettes, handwritten notes and email messages, and that care should be taken to not destroy information that could have an impact on SIRC's ability to exercise its right to access such information. • CSIS place greater emphasis on employees' obligations with respect to the protection of classified information in its orientation course and other security briefings.
Report 2006-04	• CSIS formally retract a statement and that it do so by informing the Minister of Citizenship and Immigration, the Minister of Public Safety, the Federal Court of Canada and the publishers of two newspapers. • CSIS apologize to Human Concern International for having made an unsubstantiated statement.