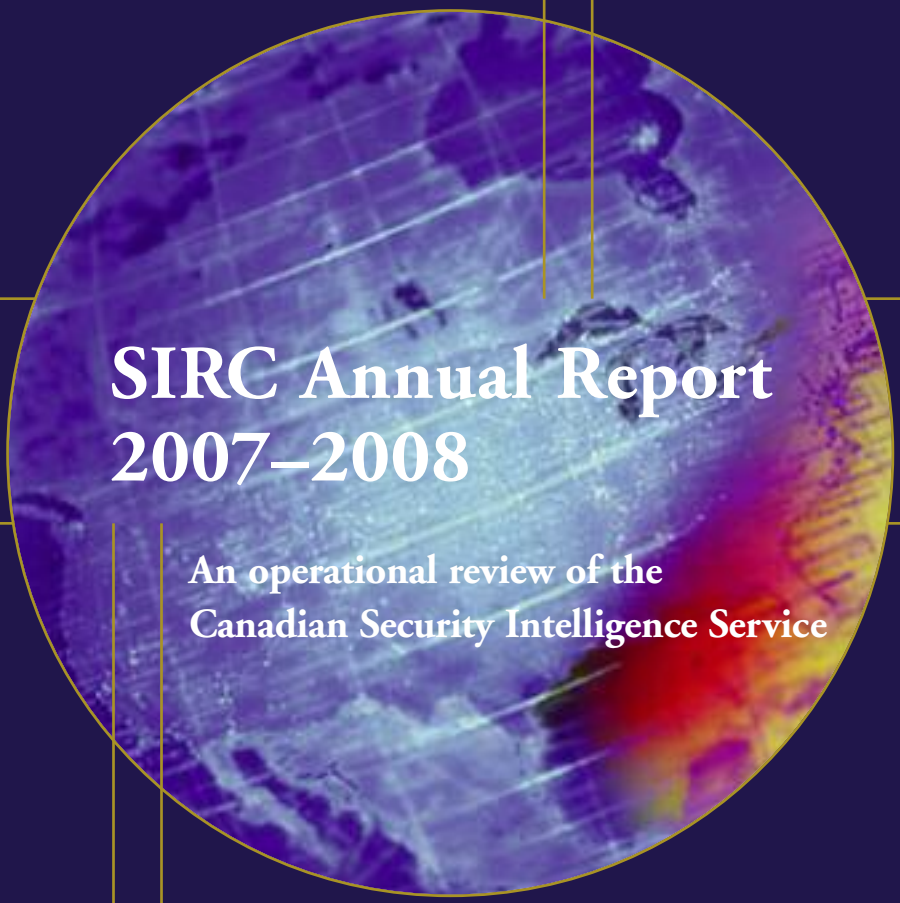
SECURITY INTELLIGENCE
REVIEW COMMITTEE



SIRC Annual Report 2007–2008

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
www.sirc-csars.gc.ca
Collect calls are accepted between 8:00 AM and 5:00 PM, EST

Cat. No. PS105-2008
ISBN 978-0-662-05944-8

SECURITY INTELLIGENCE
REVIEW COMMITTEE

SIRC Annual Report 2007–2008

An operational review of the Canadian Security Intelligence Service

Canad

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 30, 2008

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 2007–08, for your submission to Parliament.

Yours sincerely,

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

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

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

Table of contents

Members' Statement

For more than two decades, the Security Intelligence Review Committee (SIRC) has served to reassure Parliament and through it, Canadians, that the Canadian Security Intelligence Service (CSIS) is exercising its mandate to protect Canada's national security effectively and appropriately. In recent years, amidst dramatic changes to the nature and scope of the security intelligence landscape, SIRC's accountability function has taken on increasing significance. Unlike the Cold War era when there was a clear demarcation of interests between Western and Communist states, threats to national security today are much more diffuse and complex—transcending traditional state, political and geographic boundaries. The phenomena of transnational and homegrown terrorism are two such examples of this changing security environment. In response to this still-evolving context, most western nations, including Canada, have implemented fundamental changes to the ways in which they approach terrorism issues.

This transition has underscored the importance of independent, expert and informed review of CSIS. Whether in response to new legislative measures, changes to the security certificate process, various court decisions, findings from public inquiries or increased demands from government for security intelligence assessments, CSIS has implemented significant adjustments to its intelligence collection priorities and methods. SIRC has worked diligently to understand and evaluate these transformations, while ensuring that CSIS acts appropriately, effectively and in accordance with the law. Our reviews and complaint decisions provide an important means to reassure Canadians that CSIS continues to investigate new and evolving threats to national security in a manner that respects Canada's core democratic values. We accept this responsibility with an enormous sense of pride and probity.

With virtually unlimited access to all information under the control of CSIS—Cabinet confidences being the sole exception—SIRC is also uniquely situated to provide context to the debates about the nature and scope of the threat environment, and how these are addressed. Although SIRC does not promote any particular viewpoint or policy perspective, our reviews and complaint decisions provide important snapshots of CSIS's work—offering examinations of the nature and extent of the threat environment, and whether the Service addresses these threats appropriately and effectively and in a manner that respects its powers and authorities.

It is our hope that the declassified review summaries and complaints decisions that are published in our annual reports can help to inform ongoing public debate about the role of CSIS in protecting Canada's national security.

"With the *Canadian Charter of Rights and Freedoms* coming into play more often in matters of national security, and the advent of the newly created special advocate process, the guidance of the courts is both important and necessary if we, as a nation, are to find and preserve the right balance between national security and individual rights."

Readers of this year's annual report will note that in two of SIRC's decisions in complaints during 2007–08, SIRC recommended that CSIS amend its policy of destroying operational notes and, instead, retain those notes. These recommendations echoed our earlier recommendations and were aimed at ensuring that complainants and SIRC, as a quasi-judicial body, would have full access to all information relevant to matters brought before the Committee for a determination.

We are pleased that the Supreme Court of Canada's recent decision in *Charkaoui vs. Canada (Citizenship and Immigration)*, 2008 SCC 38, has brought clarity to this issue and that the court's decision reflects SIRC's oft-stated views on the matter. With the *Canadian Charter of Rights and Freedoms* coming into play more often in matters of national security, and the advent of the newly created special advocate process, the guidance of the courts is both important and necessary if we, as a nation, are to find and preserve the right balance between national security and individual rights.

SIRC strives to bring a fair and balanced perspective to our examinations of CSIS's performance. Although the Committee recognizes the increasing complexity and challenges in CSIS's work, we are always mindful of the high standards of accountability that are

essential for the legitimacy of a security intelligence agency in a democratic society. This means that, at times, SIRC will be critical of how CSIS performs, but it also means we will applaud, when warranted, the Service's contributions to protecting Canada's security. At all times we will endeavour to stay true to our commitment to earn and maintain the trust of the Canadian public in fulfilling the role that Parliament has entrusted to us.

How this report is organized

The Security Intelligence Review Committee's annual report has three sections.

Section 1: A year in review 2007–08
This section summarizes the reviews completed by SIRC as well as the complaint reports issued by SIRC during the period covered by this report.

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

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 2007–08

A. Review of CSIS security intelligence activities

HOW SIRC CARRIES OUT ITS REVIEW FUNCTION

The Security Intelligence Review Committee (SIRC) was created in 1984 as the only body with a mandate to carry out ongoing, independent review of the activities of CSIS.

Established under the *CSIS Act*, SIRC provides assurance to Parliament—and through it, to Canadians—that CSIS performs its duties and functions appropriately and effectively and in accordance with legislation, policy and Ministerial Direction. In doing so, SIRC seeks to ensure that CSIS both protects and 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 right to have access to any information under the control of the Service, no matter how highly classified that information may be.

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 reviews include findings and, where applicable, recommendations. Upon completion, the report is forwarded to both 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.

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 represent threats to the security of Canada;
- particular activities by CSIS 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. For more than twenty years, SIRC's reviews have provided Parliament and Canadians with a comprehensive picture of the Service's operational activities, and assurance that CSIS is performing its duties and functions appropriately, effectively and in accordance with the law.

For each review, SIRC's researchers will consult multiple information sources to examine specific aspects of the Service's work. For example, in addition to consulting the academic literature and arranging briefings with CSIS employees, researchers will spend considerable time reviewing various documents at CSIS headquarters. As part of this process, researchers may look at individual- and group-targeting files, human source files, operational messages and other relevant correspondence, documents relating to cooperation between CSIS and foreign and domestic agencies and partners, intelligence assessments and warrant documents, among other sources that vary between reviews. The goal is to create a diverse pool of information so SIRC can ensure that it has thoroughly reviewed, and completely understood, the issues at hand. SIRC is pleased that CSIS has made every effort to facilitate and improve SIRC's access to these information sources, and we appreciate their efforts in this regard.

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 2007–08

Review of CSIS's cooperation with and investigation of the intelligence agencies of a foreign country

Review 2007-01

Background

Traditionally, counter-intelligence investigations conducted by CSIS have focused on countries operating covertly in Canada. In this case the Service both cooperated with and investigated the intelligence agencies of a foreign country. SIRC was interested in examining the challenges faced by CSIS in managing these relationships, while also guarding against suspected threat-related activities. SIRC also examined whether the information exchanged and the cooperation undertaken with these agencies were within the scope of the relevant foreign arrangements, as well as whether there were any problems or issues that arose from this situation.

Findings

SIRC found that, despite greater cooperation between CSIS and the targeted agencies, the Service clearly had a legitimate interest in investigating the covert activities of those agencies. Although any relationship in these circumstances has the potential to become conflicted, SIRC assessed that CSIS handled its investigation in an effective manner. At the same time, SIRC confirmed that the Service needed to continue to exercise both caution and balance in maintaining this relationship to ensure the protection of Canada's security interests. SIRC also found that CSIS employees did not always submit a contact or visit form, as required by operational policy, following contact with a foreign agency representative.

SIRC made two recommendations arising from this review.

First, SIRC recommended that CSIS employees submit a standard, written record of non-operational information exchanged with foreign agencies. This would be placed in both the relevant "cooperation with" file and operational database. The written record of non-operational information exchanged should also cross-reference the operational information exchanged with those foreign agencies. SIRC believes that as the number of visits with foreign agency representatives increases, it is important that CSIS employees be kept abreast of information exchanged with foreign agencies, so that they can get quick, comprehensive snapshots of these interactions.

Second, Section 17(1)(b) of the *CSIS Act* states that the Service may, with the approval of the Minister, "enter into an arrangement or otherwise cooperate" with foreign security or intelligence organizations, which is reiterated in Ministerial Direction and operational policy. During its review, SIRC found documents indicating that the Service was cooperating with a foreign agency with which it did not have a Section 17 arrangement. CSIS maintained that the information exchanged with that agency was covered by existing arrangements with other agencies in that country. Nevertheless, SIRC recommended that CSIS establish a separate Section 17 foreign arrangement with that agency to conform with the *CSIS Act*, Ministerial Direction and operational policy.

Review of a counter-intelligence investigation

Review 2007-02

Background

In this study, SIRC reviewed one of CSIS's highest priority counter-intelligence investigations. This foreign intelligence service has conducted aggressive operations in Canada, targeting economic, political, scientific and technical information. It also has conducted operations against Canadian diplomatic premises and Canadian staff working overseas.

The objective of SIRC's review was to assess CSIS's performance in countering the foreign intelligence service's attempts to cultivate sources of information within the Government of Canada, as well as its attempts to obtain surreptitiously economic intelligence and controlled technologies from Canadian businesses.

Findings

SIRC concluded that CSIS's investigation was run professionally and was indicative of both strong operational planning and extensive experience with the investigation. The Service showed itself to be well positioned to identify and counter new threats posed by this foreign intelligence service. SIRC noted that CSIS had recently reconsidered and refocused its intelligence efforts to respond to a detected shift in practices by the foreign service in question. The Service must continue to shape its investigation to offset the challenges identified in this study and to close existing intelligence gaps.

SIRC also noted an inconsistent application of procedures for secure meetings with human sources, and expressed concern that certain practices could risk the security of CSIS's operations and increase the chance of exposing the source's relationship with the Service. As a result, SIRC suggested that CSIS review its practices and implement a consistent approach to all domestic human source operations.

An investigation of security concerns reported under the Government Security Policy

As part of this review, SIRC identified and reviewed CSIS's role in the investigation of security concerns that arose during the construction of the Department of National Defence's Above Ground Complex in North Bay, Ontario, as part of its North American Aerospace Defense Command (NORAD) modernization program. Although these issues were the subject of two reports by the Office of the Auditor General of Canada (May and October 2007), neither report discussed CSIS's role in the matter.

The Department of National Defence is responsible for meeting its security obligations under the Government Security Policy as they relate to the construction of this facility, and must report any concerns to CSIS when they arise. Further, CSIS is responsible for investigating national security concerns when they are reported. In this case, DND reported its security concerns to CSIS, and the Service responded in due course. SIRC noted, however, that CSIS did not receive sufficient information from the Department of National Defence to investigate various security concerns related to the NORAD facility fully and proactively.

SIRC also identified a gap in Canada's national security policy. The Government Security Policy requires all departments to request and receive security clearances from CSIS for individuals who require site access to secure facilities. The two reports issued by the Auditor General in 2007 indicated that departments and agencies often do not obtain the necessary security assessments for contractors. Yet there is no mechanism to alert CSIS when a department or agency has failed to meet these requirements.

SIRC believes that the failure of a department to request and receive appropriate security clearances could create a situation that could be exploited by a foreign intelligence service. Therefore, SIRC suggested that CSIS make every effort to be aware of construction projects involving secure locations and to develop a standardized procedure for CSIS to advise departments concerning the necessity of site access or security clearances.

SIRC recommended that CSIS consult with the Treasury Board Secretariat to clarify its responsibility to investigate incidents reported under the Government Security Policy, and to explore the value of enhancing interdepartmental liaison in order to advise departments of their security screening responsibilities under the policy. SIRC encourages CSIS to consider this recommendation as part of its future planning, and to include it in any discussions with the Treasury Board Secretariat about CSIS's responsibilities under the Government Security Policy.

Review of CSIS's Intelligence Assessments Branch

Review 2007-03

Background

CSIS's Intelligence Assessments Branch (IAB), formerly Research, Analysis and Production, plays an important role in providing timely and relevant strategic and tactical advice to the federal government concerning threats to national security. The IAB develops strategic analyses that examine current and emerging trends or issues that might affect national security in the future. The analyses are done for government or in support of Service investigations. It also prepares tactical analyses that support operational needs, including information about particular individuals, targets or other immediately pressing issues.

SIRC chose to review the IAB to enhance its understanding of the nature, scope and effectiveness of the branch's work. In addition to analyzing the strategic and tactical intelligence analyses produced by the branch, SIRC explored the nature and extent of the IAB's integration and cooperation with the wider Canadian security intelligence community and examined how the branch disseminated timely and relevant intelligence products.

Findings

Overall, SIRC found the IAB to be an effective and professionally organized group that has worked diligently in recent years to respond to growing demands—both within the Service and across government—for intelligence assessments and products. At the same time, considerable work remains for the IAB to adjust to the complex and changing security intelligence environment. This was recognized by IAB management and was demonstrated in ongoing work to improve and expand the branch's role. SIRC's review provided several insights into this ongoing transition.

First, recent organizational changes within the IAB should help to enhance the branch's capacity to produce strategic and tactical intelligence analyses for government or in support of Service investigations. In particular, SIRC believes that these changes represent an important step towards addressing the need for more long-term strategic analysis, especially since previous SIRC studies noted that frequent restructuring and insufficient resources had limited the Service's strategic intelligence assessment capabilities. For this reason, SIRC encourages CSIS's senior management to provide the necessary leadership and resources to ensure that the branch has the organizational stability to complete its important initiatives and objectives.

Second, SIRC believes that there will be increased pressure from across the security intelligence community for the IAB's assessments and related products. The challenge will be for the Service, and the IAB in particular, to continue to develop the capacity to meet those needs.

Third, SIRC found that the IAB has had a growing and important role collaborating with others in the Canadian intelligence community. For example, at an informal level, IAB analysts maintain contact across the intelligence community on a regular basis to share ideas and intelligence information. At a more formal level, these analysts and senior management participate in various interdepartmental working groups. SIRC believes that the branch's ongoing participation in such initiatives is essential in today's complex and evolving security environment.

SIRC's review also highlighted various challenges for the IAB in disseminating products and collecting client feedback. SIRC recognizes the Service's efforts to improve its methods of liaising with clients, to ensure that they receive relevant and timely analysis and commentary.

Review of CSIS's support for Canadian operations abroad

Review 2007-04

Background

The Director of CSIS noted in his 2006 speech to the Canadian Association for Security and Intelligence Studies that Canada's borders cannot protect the country from many of the threats it now faces. Canadian lives and property are at risk from the actions of individuals and groups residing in foreign countries—as are Canadians working or travelling abroad. In view of this, the Director maintained that one of CSIS's top challenges is "to strengthen (its) capacity to operate effectively outside of Canada in support of (its) core national security mandate."

SIRC's review sought to examine the Service's efforts to increase its capacity to operate outside Canada. SIRC therefore analyzed, as a case study, CSIS's role in interdepartmental efforts abroad to rescue members of a group known as the Christian Peacemakers, who were kidnapped in Iraq in 2005.

The following questions guided SIRC's research:

- Is existing Ministerial Direction and policy guidance adequate in light of the changing nature of CSIS operations?
- Are there any specific lessons that CSIS can draw from its participation in interdepartmental initiatives abroad?
- As CSIS expands its capacity to operate abroad, how is it interacting with federal departments and agencies that also have an international presence?

Findings

SIRC found that CSIS officers increased in two ways the effectiveness of interdepartmental efforts to rescue the kidnapped members of the Christian Peacemakers. First, the officers provided access to information and priorities of other intelligence agencies operating in Iraq. Second, they provided information collected by human sources operating in the region.

At the same time, SIRC found that the Christian Peacemakers example illustrated the challenges that CSIS will face as it increases its activities abroad:

- Existing Ministerial Direction may need to be updated to provide CSIS with appropriate guidance.
- The speed with which the Christian Peacemakers crisis developed demonstrated the importance of advance preparations in terms of materiel and logistics as well as applicable policy guidance. CSIS's International Region has started work on developing a materiel and policy infrastructure to respond to such crises.
- The rescue operation demonstrated a need to conduct operational assessments, including communications, on a regular basis. SIRC noted two instances in which information was not communicated effectively, although there was no evidence that this affected the overall quality of the operation. CSIS informed SIRC that based on lessons learned overseas, changes were recommended to existing policies and that new procedures are being developed and implemented on an ongoing basis.
- The operation revealed the challenges that CSIS may face in conducting human source operations overseas. SIRC does understand that an assessment of risk may change with time, and that an operation may appear more or less risky in hindsight. Nonetheless, given the probability that the Service may be involved in the type of human source operations examined in this review, SIRC recommended that CSIS review the criteria used to conduct risk assessments, and that the Service define more precisely the high-risk situations for which it is necessary to consult with the Minister of Public Safety.

Review of CSIS human source operations outside Canada

Review 2007-05

Background

The complexities of dealing with human beings, and human relations, make human sources a unique and challenging line of intelligence collection. Nevertheless, human sources remain an essential tool in security intelligence for understanding both threat environments and the intentions of targets—information that is not always evident from technical sources such as photographs or intercepted communications.

SIRC examined the challenges of conducting human source operations overseas, including operations in war zones. SIRC assessed the Service's actions against the *CSIS Act* and Ministerial Direction, as well as relevant operational policies and guidelines. Special attention was given to whether current Ministerial Direction was sufficient to accommodate the Service's foreign collection activities and support for military operations.

Findings

SIRC believes that the expansion of CSIS's foreign intelligence collection program will entail challenges as the organization adapts to new operational environments. SIRC recognizes the Service's efforts to work effectively in this still-evolving context, evidenced by the creation of the International Region, which includes the transition from Security Liaison Officer to Foreign Officer, and the approval of Executive Directives to guide certain operations. However, further work remains to be done.

SIRC therefore made two recommendations. First, SIRC's analysis suggests that the Service should reconsider its policy structure to accommodate its increasing activities outside Canada. Although the Committee found that CSIS had revised its practices to meet the challenges identified in the study, corresponding Service policy has yet to be adjusted. SIRC believes it appropriate for the Service to extract common principles and themes from its current practices to develop new policy to govern overseas source operations. To be effective, these changes in policy should be led by the Minister of Public Safety by way of clear Ministerial Direction. SIRC therefore recommended that CSIS prioritize the development of these policies upon receipt of the new Ministerial Direction.

SIRC's second recommendation concerned the assessment of risk for source operations. When risk assessments were reported in the planning documentation reviewed, there was little detail as to how these assessments were calculated, and

little consistency in the language used. As a result, it was often unclear what factors motivated the assessment of a particular risk level. CSIS policy has neither a standardized scale establishing thresholds between different levels of risk, nor consistent terminology when assessing risk.

SIRC concluded that CSIS should rationalize its risk assessment procedures and its reporting of risk in operational plans. Clearly described standards would provide operational staff with a tool to measure and assess risk, and ensure that all factors are considered. SIRC therefore recommended that CSIS standardize its risk assessments with detailed and consistent terminology that is reflected in operational policy.

Review of a counter-terrorism investigation

Review 2007-06

Background

This review examined one of CSIS's largest and highest-priority investigations. Operational activity undertaken within this investigation had taken place both in Canada and abroad, and the Service had cooperated with allied intelligence agencies to disrupt certain threat-related activities.

In the period under review, SIRC examined the nature and extent of the activities of a sample of group and individual targets, including how these targets constituted a threat to the security of Canada, as well as the effectiveness and appropriateness of the Service's investigation.

Findings

Two findings and one recommendation resulted from this review.

One of the groups reviewed was approved as a target in 2004, and again in 2006. SIRC found that the Service had no indication that members of the targeted group had been directly involved in any terror-related acts. According to CSIS, its main concern was that these individuals could be regarded as ideal recruits by terrorist groups.

Although there is evidence to suggest that this group is a terrorist organization—for example, some of its members are thought to have participated in terrorist activities outside of Canada—there is also a wide body of academic literature that suggests it is non-violent, and has been targeted by a number of foreign governments because it is considered a political threat. Although SIRC's review noted that the Service, in its investigation, was aware of the debate regarding the group's status as a terrorist organization, there was no reference to that debate in the targeting approval

process. Therefore, SIRC's first finding was that this debate should have been included in the targeting approval process.

SIRC therefore recommended that the debate about whether the targeted group is in fact a terrorist organization should be included in future targeting discussions. Although the ensuing discussion might not alter the final decision, the targeting approval process would nonetheless be better informed.

Another aspect of the review included an examination of the Service's investigation of targets in sensitive Canadian institutions, which includes academic, political, media, religious and trade union fields. Ministerial Direction and operational policy require that CSIS obtain a higher level of approval prior to undertaking investigative activities that have an impact, or appear to have an impact, on these institutions. SIRC's second finding was that CSIS may be required to undertake certain types of investigative activities that could have an impact on a sensitive sector institution. SIRC therefore believes the Service should re-examine existing policies to ensure that these activities are suitably covered.

Review of a Foreign Office

Review 2007-07

Background

Because the vast majority of threats that CSIS must contend with arise beyond Canada's borders, the Service has taken steps to strengthen its capacity to operate effectively abroad. CSIS has for many years operated Foreign Offices around the world—the number and locations of which are classified, except for those in London, Paris and Washington. Service representatives working at these posts are designated Foreign Officers (FO), formerly Security Liaison Officers (SLO).

SIRC's review of one such Foreign Office was designed:

- to examine the nature and volume of the Foreign Office's immigration-related work and how other responsibilities (i.e., intelligence gathering and liaison) were balanced;
- to study the office's relationships with other Canadian agencies located in the host country;
- to analyze the office's liaison relationships with foreign agencies to ensure that CSIS was prudent in its dealings with those intelligence entities with questionable human rights practices; and
- to inquire how CSIS's 2006 reorganization affected work at the office.

Findings

SIRC's examination of this Foreign Office illustrated the challenges facing CSIS in an immigration-generating, geo-politically complex and threat-diverse region. The Service places high expectations on Foreign Officers to address these competing demands, requiring solid time management and the effective development of diverse information sources. SIRC noted the Foreign Officer's capable handling of these divergent expectations at the office.

From SIRC's perspective, two overlapping issues converged at this office: strategic restructuring challenges and tactical workload expectations. These issues will become particularly relevant for this Foreign Office as the region's security intelligence demands continue to evolve. The challenge for CSIS will be to balance expanding collection demands with resource realities.

SIRC offered three concluding observations for the Service to consider as it attempts to address these competing priorities. First, CSIS will need to acknowledge and address ongoing human resource capacity issues, particularly in relation to the increased workload demands related to the transition from Service Liaison Officer to Foreign Officer. Efforts at addressing this challenge will depend on the extent to which the Service perceives the need to bolster collection capabilities at the office. Second, SIRC encouraged the Service to continue with efforts to increase liaisons with partner agencies, a strategy that SIRC believes will offset the over-reliance on particular information sources. Third, SIRC encouraged CSIS to continue refining its plans and priorities that focus on threats originating outside Canada.

Considering that the Service's reorganization remains a work in progress, there were no recommendations arising from this review.

Review of a counter-terrorism investigation*

Review 2006-08

Note:
This review was not finalized until after the 2006–07 annual report went to print.

Background

Western-based intelligence agencies have noted in recent years the activities of certain Islamist-based movements around the world whose adherents employ violence against those declared to be "enemies of Islam." In Canada, there are increasing concerns about the emergence of "homegrown" terrorist threats posed by so-called second generation Islamists—individuals born or raised in Canada who subsequently espouse radical beliefs, as well as converts who espouse extremist interpretations of Islam. CSIS has identified al Qaida-inspired threats as prominent, and particularly the threat posed by individuals who may, to all appearances, have blended into society.

To understand better why some who are born and raised in Canada might turn to extremism, and to prevent those who do so from engaging in threat-related activities, CSIS assigns priority to identifying the factors that may lead to radicalization.

SIRC reviewed the Service's investigation of certain individuals believed to be second-generation terrorists or recent converts to extremist interpretations of Islam. SIRC also reviewed CSIS's execution of warrant powers and its use of human sources.

Findings

SIRC found that the Service complied with the *CSIS Act*, as well as applicable Ministerial Direction and operational policies in this investigation. Specifically, SIRC found no issues of concern in CSIS's examination of individual targets, the development and execution of a warrant, and the management and control of most of the human sources associated with this investigation.

Concerning CSIS's direction of human sources, SIRC noted that appropriate authorization had not been provided by CSIS's executive for operations conducted within sensitive institutions, as required by its sensitive-sector policy.[1] For instance, SIRC found that a regional investigator had directed a human source to collect information within a sensitive institution without first obtaining executive approval.

[1] Sensitive institutions include those in the academic, political, media, religious and trade union fields.

SIRC also found that the investigation's targeting-approval documentation did not provide a sufficiently thorough overview of the issue, group, organization or individual targeted or a description of the activities of the proposed target, as per operational policy. In particular, SIRC believes the documentation could have included more detail regarding how the investigation would focus on issues of new, evolving or increasing concern. In the absence of this information, the investigation has served as a general operational file for the broader investigation of Islamist extremism. SIRC believes that clarifying and limiting this issue-based investigation could assist CSIS in more effectively identifying issues of developing concern and isolating them for analysis.

Therefore, the Committee recommended that CSIS clearly define this issue-based investigation when it is next renewed and determine whether it should focus on issues of increasing concern.

B. Investigation of complaints

HOW SIRC INVESTIGATES COMPLAINTS

In addition to its review function, SIRC is responsible for investigating complaints about CSIS. SIRC is committed to listening and responding to Canadians, as this is one of the key roles entrusted to SIRC by Parliament. The Committee considers complaints made by citizens concerning any activity of CSIS, or in cases where a security clearance necessary to obtain or maintain federal government employment or contracts has either been denied or revoked. Almost all complaint cases begin as inquiries to SIRC, and SIRC staff make every effort to respond promptly to such inquiries, and inform prospective complainants about what the *CSIS Act* requires to pursue a 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.

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*.

SIRC's legal team provides 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.

COMPLAINTS CAN TAKE SEVERAL FORMS

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, SIRC 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.[2] 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).

---

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

Table 1
Resolution of complaints

	2005–06	2006–07	2007–08
Carried over	18	24	20
New	45	37	32
Total	**63**	**61**	**52**
Closed	39	41	37
Carried forward to subsequent year	24	20	15
Reports issued	4	5	6

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.

C. SIRC complaint decisions 2007–08

Alleged intimidation

Report 2007-01

SIRC reported a decision made under Section 41 of the *CSIS Act* about a complaint concerning the conduct of three male CSIS officers during their interaction with the complainant, a female lawyer. She alleged that the three men had addressed her in a physically threatening manner and intimidated her in the presence of her clients at an office of Citizenship and Immigration Canada (CIC). The complainant's clients, a husband and wife, required a security screening interview by CSIS for purposes of their application for permanent residence.

Without notice to the complainant, CIC scheduled the clients to each be interviewed by CSIS officers separately and simultaneously. According to the complainant, this scheduling meant that she could not be present with her clients at both interviews. A conflict arose between the complainant and the three CSIS officers over the scheduling of the interviews and the complainant's role during the interview. The complainant stated that she felt physically threatened by the CSIS officers and was shaking. She also found their behaviour and comments to be rude and sexist. Furthermore, she alleged that the CSIS officers were racist.

As part of SIRC's investigation, a hearing was held. The complainant did not offer an independent third party to testify about the alleged conduct of the CSIS officers. SIRC was left with two different but equally plausible interpretations of how the events transpired.

SIRC found that the three CSIS officers reacted reasonably under the circumstances. They were following CSIS policy concerning the conduct of immigration interviews. The three CSIS officers maintained that their conduct was not intended to intimidate, but rather to find out what the problem was regarding the scheduled interviews. The prospect of simultaneous interviews caused conflict for the complainant, while the prospect of re-scheduling consecutive interviews caused conflict for CSIS.

SIRC found that, given the circumstances of this case, both sides would have been agitated by the conflict, and their behaviour would have been affected accordingly. Nevertheless, SIRC did not find evidence that either the complainant's behaviour

in serving as counsel to her clients, or the CSIS officers' behaviour was unreasonable, threatening or intimidating.

As with all complaints, the complainant had the burden of proof. SIRC concluded that the complainant did not present sufficient evidence to prove the alleged intimidation and misconduct.

Nevertheless, SIRC concluded that the conflict between the two parties might have been avoided if CSIS policies permitted an individual not only to have counsel or another representative attend a security screening interview, but also to advocate for that individual during the interview process with CSIS.

SIRC recommended that the Service's policies be amended so that individuals are permitted to be accompanied and fully represented by counsel or another representative during a security screening interview conducted by CSIS.

Alleged abuse of human rights and unfair treatment

Report 2007-02

In this complaint filed with SIRC under Section 41 of the *CSIS Act*, the complainant alleged that CSIS had abused his human rights and those of his family, and that the Service had treated him unfairly. SIRC investigated the complaint and concluded that there was no evidence of any abuse of human rights as alleged. While SIRC did find that the complainant had been treated unfairly, it was to a much lesser degree than had been alleged by the complainant.

Allegations concerning CSIS's handling of evidence obtained by torture

Report 2007-03

SIRC reported a decision concerning a complaint pursuant to Section 41 of the *CSIS Act*, in which the complainant, Paul Copeland, alleged a "total lack of concern" by CSIS regarding evidence obtained by torture.

Noteworthy in this case is that immediately after SIRC began its investigation, the Government of Canada implemented a key recommendation made by Justice O'Connor in his report on the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar. On December 12, 2006, the Honourable Frank Iacobucci

was appointed to undertake an inquiry into the actions of Canadian officials in relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin. Therefore, SIRC decided that it would be inappropriate for the Committee to include any findings in its report that could be the subject of this inquiry.

In investigating Mr. Copeland's complaint, SIRC had access to classified information relevant to the allegations, including a classified version of the report of Justice O'Connor (hereafter referred to as the "Arar Report"). After having reviewed all the documentation made available, as well as the representations of the parties, SIRC did not find evidence of a "total lack of concern."

In its decision, SIRC noted that on June 29, 2005, CSIS had implemented two relevant recommendations contained in SIRC's review of the role of CSIS in the matter of Maher Arar.[3] The first recommendation was to change CSIS operational policies so that it must consider the human rights record of a foreign state or agency when information received from those sources will be used in an application for targeting approval. The second recommendation was to amend a CSIS operational policy that governs the information included in a foreign-travel proposal so that it must consider the human rights records of foreign states or agencies regarding incoming visits or travel abroad.

Further, SIRC took into consideration Recommendation 14 made by Justice O'Connor in the Arar Report, which states:

> *"Information should never be provided to a foreign country where there is a credible risk that it will cause or contribute to the use of torture. Policies should include specific directions aimed at eliminating any possible Canadian complicity in torture, avoiding the risk of other human rights abuses and ensuring accountability."*

SIRC views this recommendation as the standard that CSIS should apply when exchanging information. As Justice O'Connor further stated:

> *"Domestically, the* Canadian Charter of Rights and Freedoms *confirms the absolute rejection of the use of torture."*

Although SIRC did not find evidence of a "total lack of concern" on the part of CSIS regarding evidence obtained by torture, it did find that at the time the complaint was made, CSIS lacked specific policies aimed at eliminating any possible Canadian com-

---

[3] A complete list of SIRC reviews is available on SIRC's website (www.sirc-csars.gc.ca).

plicity in torture. As noted in the Arar Report, CSIS had no personnel with expertise in recognizing intelligence that may have been the product of torture, but "[r]ather, CSIS's assessment focuse[d] on whether the Service can corroborate the information."

SIRC found this lack of expertise hampered the Service in exercising due diligence, not only in assessing the reliability of information—particularly whether the information was obtained by torture—but also in assessing whether there was a credible risk that the exchange of information would cause or contribute to the use of torture.

SIRC noted the following advice provided by Justice O'Connor in his report:

> *"Canadian officials must be more sophisticated in their assessments, taking into consideration all of the available information in order to draw reasonable inferences about what may have happened. The Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (Convention against Torture) provides that the human rights record of a country must be considered in assessing the risk of torture."*

During its investigation, SIRC was informed that CSIS has personnel with the expertise to assess the reliability of information. However, SIRC was neither informed nor could it determine whether CSIS has personnel with the expertise to make sophisticated assessments as to whether exchanges of information will create a risk of causing or contributing to any possible Canadian complicity in torture, or the risk of other human rights abuses.

In SIRC Review 2005-02 (CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post),[4] SIRC had found a lack of any written documentation about possible human rights concerns cited by organizations such as Amnesty International and Human Rights Watch. The concerns related to the Service's documentation of a separate and relatively new foreign arrangement with a particular intelligence agency. SIRC found that this lack of written documentation would not meet the standard of assessment as contemplated by Justice O'Connor in ensuring Canada's non-complicity with human rights abuses.

With respect to arrangements with foreign states or agencies to collect and share information and intelligence, both Ministerial Direction and operational policy require that CSIS address a country's human rights record. This includes any possible abuses by the security or intelligence organizations. Further, arrangements with

[4] A complete list of SIRC reviews is available on SIRC's website (www.sirc-csars.gc.ca).

countries that do not share Canada's respect for democratic or human rights will only be considered where contact is required to protect the security of Canada.

CSIS's policy requires that all applications for any targeting submission take into consideration the human rights record of any foreign state or agency whose information may be used to support the submission.

Based on these facts, SIRC found CSIS is concerned with human rights, but nevertheless may use information obtained by torture. Although it did not find a "total lack of concern" for evidence obtained by torture, SIRC did find that CSIS focused on the impact that torture might have on the reliability of information used in carrying out its responsibilities under the *CSIS Act*, rather than on its obligations domestically under the *Canadian Charter of Rights and Freedoms* and the *Criminal Code of Canada*, as well as internationally under the treaties signed by Canada that absolutely reject torture.

For purposes of this investigation, SIRC found that Justice O'Connor's findings and recommendations—as well as any future findings and recommendations by the Honourable Iacobucci's inquiry—will ensure that the use of information obtained through exchanges with foreign agencies is done in such a way that protects Canadians from threats to their security. These efforts will also respect the values of Canada's free and democratic society as reflected in the *Charter*, the *Criminal Code*, and its treaty obligations regarding the abhorrence of torture.

SIRC recommended that CSIS implement the recommendations directed at the Service in the Arar Report.

A second recommendation made as a result of this investigation cannot be disclosed for reasons of national security.

Alleged discriminatory practice

Report 2007-04

SIRC reported a decision on a complaint pursuant to Section 45 of the *Canadian Human Rights Act*. The complainant alleged that Transport Canada had discriminated against him on the grounds of race, national or ethnic origin, and religion by treating him in an adverse differential manner.

The Minister of Transport asked the Canadian Human Rights Commission to refer the case to SIRC.

The alleged discrimination concerned Transport Canada:

- not issuing the complainant an Airport Restricted Area Access Clearance Pass on grounds of religion and ethnic origin; and
- pursuing a policy and/or practice of denying security clearance to individuals of the complainant's ethnic origin.

Under Transport Canada's Airport Restricted Area Access Clearance Program (hereafter "the Program"), the complainant (who was working for a private-sector employer) needed site-access clearance to be issued a pass by the Airport Pass Control Office. This would have provided the individual with access to restricted areas within an airport. The aim of the Program is to prevent unlawful acts of interference with civil aviation. It does so by issuing a site-access pass to persons who meet the standards set out in this Program. The objective is to prevent uncontrolled entry into a restricted area of a listed airport by a person who falls within one of the listed categories of threats to security.

As part of the complainant's application process for a pass, the Director of Preventive Security for Transport Canada was provided with information about the complainant resulting from a criminal record check, a credit check and a CSIS indices check. The Director of Preventive Security decided to convene an Access Clearance Review Board, which took into consideration the national security concerns communicated by CSIS and the results of the criminal record check. The Review Board decided to recommend to the Minister of Transport the denial of the clearance. Subsequently the Minister denied the complainant site-access clearance. Since restricted-area access at the airport was a condition of employment, the individual's job was terminated.

The Minister of Transport made the decision without providing the complainant with the opportunity "to know the case against him" or to respond to the adverse information. Nor was the complainant provided any reasons for the denial. The Minister informed the individual that there was a 30-day deadline within which to seek from the Federal Court a judicial review of the decision.

SIRC found that:

1. The complaint of discrimination pertained to a practice that was based on considerations relating to national security, and hence was properly referred to SIRC pursuant to Subsection 45 (2) of the *Canadian Human Rights Act*.
2. The Minister's decision not to grant the site-access clearance, which resulted in the Airport Restricted Area Access Clearance Pass not being granted, was made in accordance with the relevant program, and was done for security considerations—not on prohibited grounds of discrimination based on the complainant's race, national or ethnic origin or his religion.
3. The security assessments conducted by CSIS and Transport Canada were flawed for two reasons:
    a. the procedure relied on by the Review Board and the Minister of Transport under the Program was inherently unfair and breached the rules of natural justice, given the serious consequences of the Minister's decision—namely the loss of the complainant's employment; and
    b. CSIS did not comply fully with its own procedures.

More specifically, SIRC found the procedure under the Program was inherently unfair and breached the rules of natural justice by:

- not providing the complainant with an opportunity to respond to any adverse information prior to the decision being taken by the Minister;
- not providing the complainant with reasons for the Minister's decision according to which the complainant could have made an informed choice to seek judicial review;
- relying on an inadequate security assessment; and
- failing to answer the complainant's counsel's telephone inquiries on a timely basis which, in all likelihood, would have had an impact on the complainant making an informed decision to seek judicial review within the 30-day deadline.

Given the serious consequences of the Minister's decision, which resulted in the loss of the complainant's employment, the complainant should have been afforded a fair process which adhered to the rules of natural justice.

SIRC recommended that the Canadian Human Rights Commission not investigate this complaint in accordance with Subsection 46 (2) of the *Canadian Human Rights Act*. It maintained that the Minister did not make his decision to deny the complainant site-access clearance based on a prohibited ground of discrimination, nor was Transport Canada pursuing a policy and/or practice of denying site-access clearance to individuals of the same ethnic origin as the complainant.

SIRC further recommended that the Minister provide the complainant with the opportunity to re-apply for the security clearance under the new policy.

Finally, SIRC recommended that if the complainant were to re-apply, CSIS or Transport Canada should conduct an interview with the complainant in the presence of counsel or any other representative. In addition, the complainant should be made aware of the right to record the interview, and that CSIS or Transport Canada also record the interview and retain a copy of the recording until the complainant has had an opportunity to exhaust any review process or until the retention period under the *Privacy Act* has expired, whichever is later.

Alleged improper advice to the Minister of Citizenship and Immigration

Report 2007-05

SIRC reported an investigation of a complaint made under Section 41 of the *CSIS Act* alleging that CSIS had provided improper advice to Citizenship and Immigration (CIC) in 2001 and 2004 regarding a complainant's application for permanent resident status in Canada under the former *Immigration Act*.

In this case, the complainant was a refugee from Pakistan. In his immigration documents, he had declared that while he was in Pakistan from 1985 until he immigrated to Canada in 1996, he had been a member of an organization called the Muttahida Quami Movement (otherwise referred to as "MQM"). In 2000, he was interviewed by CSIS, at which time he provided details of his past involvement with the MQM. He told the CSIS interviewer that he had not been involved with the MQM since arriving in Canada.

Following the interview, CSIS provided an inadmissibility brief to CIC in 2001. In 2004, CSIS updated their advice to CIC. At the time of the second inadmissibility brief, the *Immigration Act* had been replaced by the *Immigration and Refugee Protection Act (IRPA)*. Section 19 of the former Act had been replaced with Section 34 of the IRPA.

Much of SIRC's investigation focused on whether, by law, there are reasonable grounds to believe the MQM is an organization that is or was engaged in terrorism. The investigation also focused on whether the advice from CSIS to CIC regarding this issue was proper. SIRC received evidence from both the Service and the complainant on this issue. SIRC considered the wording of the *Immigration Act* as it was applied by CSIS in the 2001 inadmissibility brief that was later confirmed by

the 2004 inadmissibility brief and found that the advice from CSIS to CIC on this issue was proper.

However, SIRC found other aspects of the advice from CSIS to CIC were wrong or inaccurate and therefore improper. SIRC found no evidence to support a bona fide belief that the complainant has been a member of the MQM since arriving in Canada. This advice was wrong and was perpetuated by the second inadmissibility brief in 2004. SIRC also found an inaccurate statement in the 2001 inadmissibility brief.

Additionally, SIRC considered the exception set out in Section 19 (1)(f)(iii)(B) of the former *Immigration Act* whereby an applicant could not fall within the inadmissible class as set out in paragraph (f) or be deemed inadmissible, where the applicant has satisfied the Minister of Citizenship and Immigration that his or her admission would not be detrimental to the national interest. From a review of the CSIS analyst's assessment, the analyst did not address the exception.

Finally, the 2004 inadmissibility brief did not address the fact that the *Immigration Act* had been replaced by the *Immigration and Refugee Protection Act* and that the exception embedded in Section 19 (1)(f)(iii)(B) of the former *Immigration Act* is currently found in a general exception in Section 34 (2) in the *IRPA*. Therefore, it was improper for CSIS not to have updated their advice by referring to the new legislation. SIRC found that the advice in the 2004 inadmissibility brief was wrong because it did not take the new legislation into account.

SIRC also made two findings regarding procedure.

The first finding concerned the production of documents. On four occasions during the investigation, SIRC requested a copy of the relevant security screening guidelines or procedures relied on by CSIS for the provision of their advice to CIC. After the hearing, counsel for CSIS provided SIRC, pursuant to an undertaking, a copy of the Security Screening Procedures Guidelines which, to the best of the Service's knowledge, were in effect at the time the first inadmissibility brief was prepared. Security screening procedures for the purpose of preparing the second inadmissibility brief in 2004 were never formally approved. Although a witness for CSIS testified that all the procedures and guidelines were complied with in the preparation of the inadmissibility briefs, SIRC could not give much weight to that testimony since the witness had no personal involvement in the preparation of the briefs. Moreover, CSIS could not tell SIRC with full certainty what documents were relied upon in the preparation of the briefs.

The second finding concerned the destruction of the CSIS interviewer's notes. SIRC was informed that the interviewer had destroyed the notes taken during the interview with the complainant in accordance with CSIS operational policy, identified as OPS-217 *Operational Notes* and thus the notes were not available to SIRC for purposes of the investigation. SIRC determined that the destruction of the notes did not hinder its investigation. However, SIRC found that the notes of a subject interview for immigration screening may be required as evidence or information for investigations or proceedings before the courts or administrative tribunals and therefore should be retained by the Service. SIRC has recommended on other occasions that notes of interviews not be destroyed.

Finally, SIRC recommended that CSIS prepare fresh advice to CIC, to satisfy the Minister of CIC that the presence of the complainant in Canada would not be detrimental to the national interest in accordance with Subsection 34(2) of the *IRPA*, or if required, could be used by the complainant to seek what is referred to as "Ministerial Relief" in respect of Subsection 34(2) under the *IRPA*.

Alleged unreasonable delay in processing a site-access clearance

Report 2007-06

SIRC reported on a complaint made pursuant to Section 41 of the *CSIS Act*, regarding the delay by CSIS in completing its security assessment for the purposes of the complainant's employment. The complainant had received an offer of employment that was conditional upon the complainant successfully obtaining a reliability and site-access clearance. The employer specified in the letter of offer the date by which the complainant was to obtain the reliability and site-access clearance, failing which the employer would have the option of either extending the time for the satisfaction of the condition of employment or of rescinding the offer. When SIRC began the hearing of this complaint, CSIS had not completed its security assessment. More than twenty months had elapsed since the complainant had received the offer of employment, and the complainant had been subjected to three subject interviews by CSIS.

SIRC concluded that when the complainant first wrote the Director of CSIS (approximately two months after the complainant had received the letter of offer) to complain about the time taken by CSIS to complete its security assessment, the complaint was premature, notwithstanding the date specified by the employer in the offer of employment. SIRC also found that although there was an accumulation of moderate delays, the overall time taken by CSIS to complete its security assessment

during the first seven months was reasonable. However, SIRC found that after the first seven months, although the delays were not deliberate, the time taken by CSIS to conduct its security enquiries was not reasonable and the delays could have been avoided.

SIRC made four recommendations:

- that CSIS take all necessary steps to ensure the adoption of its *Security Screening Procedures Manual* and *Security Screening Investigator's Guidebook* before June 30, 2008;
- that CSIS adopt guidelines to ensure that the information recorded and contained in the security screening database accurately reflect the status of the file to enable all users of the system to be as fully aware as possible of the file without having to review the hard-copy file and that appropriate diary dates be included in its security screening database;
- that CSIS policy be revised as expeditiously as possible to prevent the destruction of recorded or written notes which may be required as evidence in proceedings before the courts or administrative tribunals; and
- that CSIS provide its advice forthwith with regard to the complainant's security assessment.

Section 2

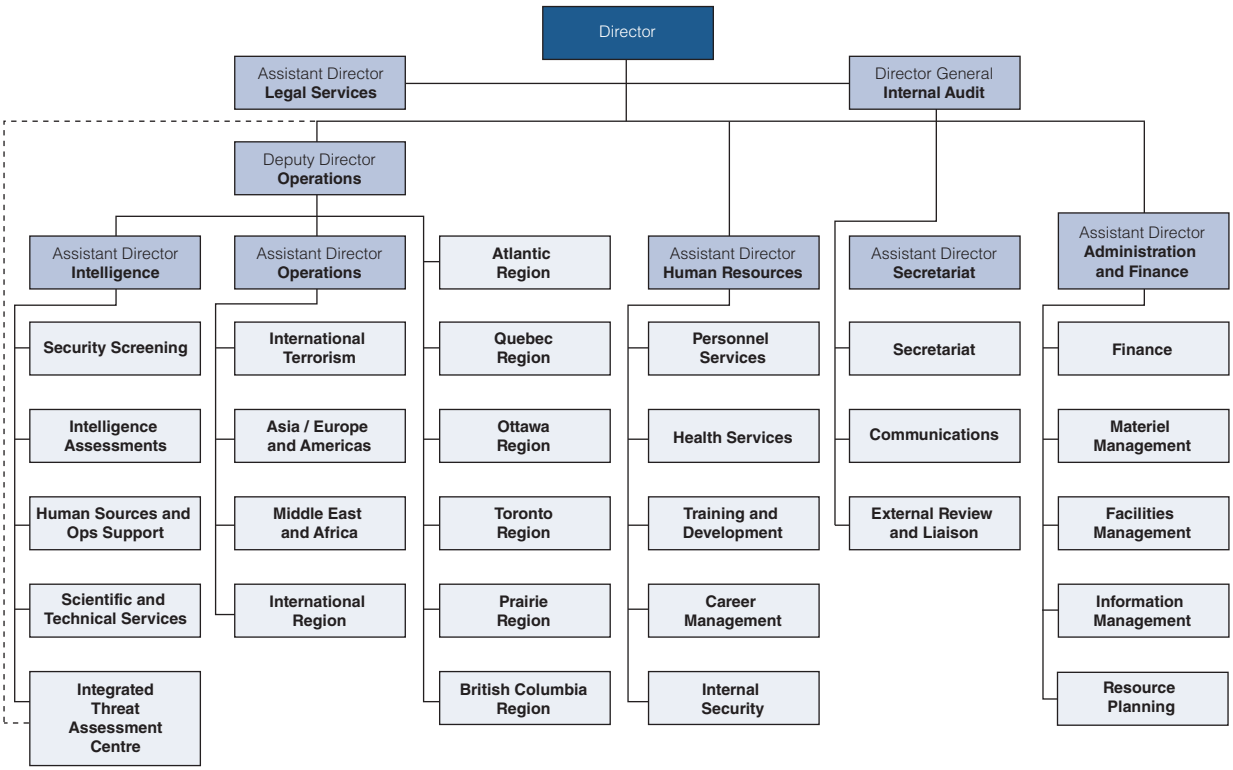
CSIS operational activities and accountability mechanisms

A. CSIS operational activities

The Deputy Director Operations, who reports to CSIS's Director, is responsible for three groups:

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

Canadian Security Intelligence Service



i. Intelligence

SECURITY SCREENING BRANCH

As a key component of Canada's national security framework, security screening provides one of the Service's most visible functions.

The Security Screening Branch has two program streams: government screening and immigration screening. In response to an increasing number of screening requests over the past several years, the branch has attempted to improve its technical and case management functions to ensure that they continue to provide timely, relevant and accurate assessments that meet client expectations. The branch has also consulted with government clients to guide them through new rules concerning the security screening process.

Government screening provides security assessments—an appraisal of an individual's loyalty to Canada and, so far as it relates thereto, the reliability of the individual—for all government departments and institutions, except the Royal Canadian

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

1. **Notices of assessment** (NOA) 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.

Mounted Police (RCMP), for which CSIS performs indices and Out-of-Country (OCC) checks, including joint subject interviews for cause. It is also involved in a site-access program for airports, port and marine facilities, the parliamentary precinct and nuclear power facilities, as well as providing assessments to provincial departments. These programs are meant to enhance security and reduce the potential threat from terrorist groups and foreign governments that seek to gain advantage by obtaining authorized access to classified information or other assets, materials and sensitive sites.

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 30 percent and 16 percent respectively of all requests in 2007–08.

As indicated in Table 2, in 2007–08, CSIS received 50,300 requests for new or updated security clearances and provided 48,800 security assessments to federal departments. The volume of requests was down slightly from the previous fiscal year, as was the number of security assessments. The biggest change was a decrease in the number of requests from DND.

Table 2
CSIS government security screening*

	2005-06	2006-07	2007-08
Requests from DND	9,200	13,100	8,800
Requests from other departments or agencies	32,900	38,100	41,500
Total	**42,100**	**51,200**	**50,300**
Assessments issued to DND	8,900	13,100	8,300
Assessments issued to other departments or agencies†	28,900	41,800	40,500
Total	**37,800**	**55,000**	**48,800**

* Figures have been rounded to the nearest 100.

† This number includes assessments performed for provincial governments and for access to nuclear facilities.

As part of its efforts to track efficiency in responding to security screening requests, CSIS calculates its turnaround times using a median number of calendar days. As indicated in Table 3, the median turnaround times decreased compared to the previous year's levels, the exception being an increase for Level III (Top Secret) assessments.

However, the median times for this category were calculated differently in 2007–08, which resulted in a rise in the median time in comparison to previous years. For 2007–08, median times for Level III clearances exclude updates for those who already have this clearance, a process that takes considerably less time than requests for new or upgrade assessments.[5] For example, while the median turnaround time for new and upgrade Level III assessments for DND is 164 days, the median time for updates is 29 days. Similarly, for non-DND clients the median turnaround time is 186 days for new or upgrade Level III assessments, compared to four days for updates.

Table 3
Median turnaround time (in calendar days)

		2005–06	2006–07	2007–08
DND	Level I (Confidential)	24	40	23
	Level II (Secret)	19	40	28
	Level III (Top Secret)	39	82	164 (new) 29 (updates)
Non-DND	Level I (Confidential)	15	32	17
	Level II (Secret)	13	21	13
	Level III (Top Secret)	60	47	186 (new) 4 (updates)

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 indicate to a requesting agency that the Government Security Policy threshold for denying clearance has been met. However, it is the responsibility of the requesting agency to grant, revoke or deny a clearance. In 2007–08, the Service issued eight information briefs reporting information of an adverse nature. Two denial briefs were issued.

[5] Individuals with a Level III (Top Secret) clearance must renew/update their clearance level every five years. New and upgrade assessments include those who are applying for a clearance and those who are applying for a higher-level clearance (e.g., someone with a Level I clearance who applies for a Level III clearance).

CSIS also provides site-access screening (see Table 4). Unlike a government security clearance, a site-access clearance only gives an individual access to certain secure areas or provides accreditation for special events. In 2007–08, CSIS received over 67,500 requests for this type of screening and provided no information briefs to requesting agencies. The increase in requests for access to nuclear facilities in 2006–07 was a result of a five-year renewal cycle for pre-existing clearances. The number of these requests therefore dropped in 2007–08. There was also a decrease in the number of requests associated with the Free and Secure Trade (FAST) program.

The Service provided over 1,300 assessments for special events in 2007–08.

Table 4
Site-access screening*

	2005–06	2006–07	2007–08
Parliamentary precinct	1,000	1,100	1,100
Airport restricted-access area	37,600	39,300	36,800
Nuclear facilities	10,600	17,900	9,200
Free and Secure Trade (FAST)	3,100	23,100	10,700
Special events accreditation	5,600	0	1,300
Marine Transportation Security Clearance Program†	N/A	N/A	6,300
Other government departments	2,400	2,500	2,100
Total	**60,300**	**83,900**	**67,500**

* Figures have been rounded to the nearest 100.

† The Marine Transportation Security Clearance Program, which provides security assessments in relation to the security of Canada's ports, became operational in December 2007.

Immigration screening helps to ensure that individuals who pose a threat to security and/or are inadmissible under the *IRPA* do not gain entry or obtain status in Canada. This program provides security advice to:

a) identify whether or not citizenship applicants will engage in activities that constitute a threat to the security of Canada;
b) identify individuals who are inadmissible on security grounds under Section 34(1) of the *IRPA*;
c) identify visitor and refugee claimants at Canadian ports of entry who are inadmissible for security reasons; and
d) screen those requesting visitor visas from countries that pose a terrorist, espionage and transnational criminal activity threat.

In 2007–08, the branch received 94,400 requests under various immigration screening programs (see Table 5). The number of requests received within and from outside Canada was similar to the previous year, while the number of refugee determination requests decreased. The number of front-end screening requests increased from the previous year.

Table 5
Immigration security screening

	Requests*			Briefs		
	2005–06	2006–07	2007–08	2005–06	2006–07	2007–08
Within and outside Canada†	63,200	62,800	66,000	133	201	195
Front-end Screening††	17,100	17,900	21,800	89	143	117
Refugee determination†††	11,700	11,600	6,600	127	153	142
Subtotal	**92,000**	**92,300**	**94,400**	**349**	**497**	**454**
Citizenship applications	308,000	227,300	190,000	120	155	109
Total	**400,000**	**319,600**	**284,400**	**469**	**652**	**563**

* Figures have been rounded to the nearest 100.

† 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.

†† Individuals claiming refugee status in Canada or at ports of entry.

††† Refugees, as defined by the *IRPA*, who apply from within Canada for permanent resident status.

CSIS finds no adverse information in the majority of its screening investigations of refugee claimants or immigration/citizenship candidates. In 2007–08, the Service issued 325 information briefs, 129 inadmissibility briefs and one incidental letter related to immigration cases.

In recent years, the Service's turnaround times for providing information or inadmissibility briefs were generally quite lengthy. In 2007–08, information briefs related to immigration cases took a median of 508 calendar days for an application filed in Canada, 620 days for those filed from the United States and 150 days for those filed abroad. Information briefs related to permanent resident applicants who are refugees in Canada had a median turnaround time of 497 days, and those for files subject to the Front-End Screening Program had a turnaround time of 339 days.

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

Table 6
Turnaround time (in days) for notices of assessment

	2005–06	2006–07	2007–08
Citizenship	1	1	1
Immigration (Canada)†	70	78	59
Immigration (USA)††	62	29	45
Overseas immigration	16	14	20
Refugee determination	96	98	64
Front-end screening	23	19	28

† This includes certain classes of individuals who apply for permanent resident status within Canada.

†† 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.

Other screening activities

In 2007–08, the Security Screening Branch also vetted 111,300 visa applications for foreign programs. In addition, the branch was involved in the following two programs:

- **The Trusted Traveller Program** — a pre-clearance program for individuals who travel frequently to the United States. This program is currently under development; and
- **Passenger Protect** — the branch worked with other government departments in developing airline passenger screening programs, in particular the domestic "no-fly" program, which became operational on June 18, 2007.

INTELLIGENCE ASSESSMENTS BRANCH

The Intelligence Assessments Branch 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 Assessments*, *Threat and Risk Assessments* and *Perspectives*.

In recent years, the branch has undergone a series of changes in an attempt to respond to the growing demand within the Service and across government for strategic and operational assessments. As part of this process, the branch has engaged in dialogue with federal partners and clients to ensure that CSIS continues to provide relevant and timely assessments that meet the needs of clients. The branch has sought opportunities to coordinate with partners within the assessment community to identify common areas of interest and produce community assessments. Likewise, it has created internal mechanisms to promote an ongoing dialogue with collectors within the Service to ensure that analytical support is provided in a timely fashion to assist in investigations.

This branch also has a role in the Terrorist Entity Listing process both in regards to listing new entities and renewing those already listed. The Service prepares Security Intelligence Reports (SIRs) on groups that are believed to be, or act on behalf of, a terrorist entity. This report outlines the Service's findings and forms the basis for consideration by the Governor-in-Council on whether to approve that a group be listed under Section 83.05 of the *Criminal Code of Canada*. 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 still reasonable grounds for an entity to be listed and make a recommendation to the Governor-in-Council accordingly.

The Minister's most recent review of the listing commenced in February 2008 and is to be completed this fall.

HUMAN SOURCES AND OPERATIONS SUPPORT BRANCH

This branch provides a range of support and coordination services including risk management and analytical expertise 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 contains the Threat Management Centre, which provides 24/7 support to operational staff at headquarters and regional and Foreign Offices, and it provides support to the Service's involvement in major special events such as last year's North American Leaders' Summit and the upcoming 2010 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.

During the period under review, ITAC issued 348 threat assessments and redistributed over 1,300 others produced by allied fusion centres. ITAC also published *Media Watch* each business day for distribution to clients. Further, ITAC provided over 120 briefings to its domestic clients, including the Petroleum Industry Annual Safety Seminar, the Canadian Association of Chiefs of Police Liaison Conference, the Cyber Security Task Force and a critical infrastructure conference in the United States.

During the period under review, ITAC assumed responsibility for the Threat Assessment Unit, which provides time-sensitive evaluations of potential threats to Canadians and Canadian interests in Canada or abroad, or to foreign interests or nationals in Canada. ITAC provided assessments of key issues for the Government of Canada and in relation to the North America Leaders' Summit at Montebello, Quebec in August 2007. Also of note, ITAC produced three papers in collaboration with the Canadian Centre of Intelligence and Security Studies at Carleton University.

ITAC continued its planning work regarding a 24/7 centre with an integrated analytical capacity.

ii. Operations

Under Operations, four branches are 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.

Middle East and Africa Branch

This branch concentrates its investigative effort on threats that emanate from, or have as their major focus in, countries in the Middle East and Africa. 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 Terrorism Branch

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

International Region

This branch 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 intelligence or enforcement agencies, as well as the operation of the Service's Foreign Offices abroad. The Service relies on these offices 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.

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 examine all aspects of warrants granted to the Service, particularly since this is part of the vital accountability function provided by the Federal Court. However, as part of its review activities, SIRC does consider whether the Service adheres to the warrant approved by the Federal Court (i.e., how the warrant powers were used by CSIS).

In 2007–08, the Federal Court approved 71 new warrants—a notable increase from the previous year. The Federal Court also approved the replacement or renewal of 182 warrants, which is also an increase from the previous year's levels. During the same period, 56 warrants were either terminated or expired without being renewed. No warrant applications were denied by the Federal Court. In one instance, the Federal Court denied the Service's request for a foreign telecommunications warrant authorizing the interception, outside Canada, of the communications of subjects under investigation. In its decision, the court ruled that it had no jurisdiction to issue the warrant sought under the *CSIS Act*.

Table 7
Warrant statistics

	2004–05	2005–06	2006–07	2007–08
New warrants	40	24	42	71
Replaced or renewed	207	203	134	182
Total	**247**	**227**	**176†**	**253††**

† Included in this number were 25 urgent warrants.
†† Included in this number were 19 urgent warrants.

B. Reporting requirements

CSIS DIRECTOR'S ANNUAL REPORT (2006–07)

Every year, the Director of CSIS submits a classified report to the Minister of Public Safety. It describes in detail the priorities and operational activities of the Service. The Inspector General of CSIS examines this report and submits to the Minister a certificate that attests the extent to which she or he is satisfied with its contents. Next, the Minister sends a copy of both documents to SIRC for its review, as required by Section 38(a) of the *CSIS Act*.

In the 2006–07 edition of the report—the first one to be issued following the realignment of operational resources within CSIS—the Director noted that the realignment provides the Service with a flexible organizational structure that can be easily modified to future operational needs.

In addition to summarizing the Service's use of human sources during the year, the report identified the activities of each operational branch and specialized group within CSIS, as well as all domestic and foreign arrangements, as provided under Section 17 of the *CSIS Act*.

The Director reported that CSIS had suspended its relationships with five human sources because of criminal activity. He further noted that CSIS had not directed the sources to undertake this activity and that the Service immediately took corrective measures upon learning about the incidents. The Director highlighted CSIS's role in identifying suspected Russian spy Paul William Hampel, and of the Service's role in expelling this individual from Canada. The Director also reported that the Service's Middle East and Africa Branch terminated an investigation because of a lack of reporting of threat-related activities.

Of particular note, the Director drew the Minister of Public Safety's attention to the challenges that CSIS faces with the rapid growth and changes to Internet-related technologies. He indicated that a remedy for these challenges would be for Parliament to pass legislation, such as the *Technical Assistance to Law Enforcement Agencies Act*. The legislation was tabled in November 2005 but was not passed because of the federal election that was called immediately afterwards.

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

CERTIFICATE OF THE INSPECTOR GENERAL OF CSIS (2006–07)

Established in 1984 under the *CSIS Act*, the Inspector General of CSIS functions as the "eyes and ears" of the Minister of Public Safety, reviewing the Service's operations and providing assurance that CSIS is complying with Ministerial Direction, operational policy and the *CSIS Act*.

Every year, the Inspector General submits a certificate to the Minister stating the extent to which he or she is satisfied with the CSIS Director's Annual Report. This certificate informs the Minister of any unreasonable or unnecessary exercise of CSIS powers, as well as any instances of the Service failing to comply with either the *CSIS Act* or Ministerial Direction.

In the latest certificate, the Inspector General was satisfied with the CSIS Director's 2006–07 Annual Report, stating that the Service has not acted beyond the framework of its statutory authority, had not contravened any Ministerial Directions, and had not exercised its powers unreasonably or unnecessarily.

However, the Inspector General expressed concern that there had been an increasing number of instances of non-compliance with CSIS operational policy, as well as a greater number of transcription errors in documents. Most of the instances of non-compliance were administrative errors. She also remarked on the length of time required to develop or update operational policies in response to changing requirements and activities.

For more information about the Certificate of the Inspector General (CSIS), please refer to the Public Safety website (www.publicsafety.gc.ca).

UNLAWFUL CONDUCT BY CSIS

Under Section 20(2) of the *CSIS Act*, the Director of CSIS must submit a report to the Minister when, in the Director's opinion, a CSIS employee may have acted unlawfully in performing his or her duties 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 2007–08, no CSIS employee acted unlawfully, and no such reports were issued.

DISCLOSURE OF INFORMATION

Section 19 of the *CSIS Act* prohibits the disclosure of information obtained by the Service in the course of its investigations 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, or to 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 and International Trade 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 90 disclosure letters during fiscal year 2007–08.

C. 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, 2008, CSIS had 39 MOUs with domestic partners: 29 with federal departments or agencies and 10 with provincial and municipal entities.

In 2007–08, SIRC examined the Service's arrangement with Transport Canada, focusing on the Service's contribution of security screening information in support of two of that department's programs: the Marine Transportation Security Clearance Program and the Passenger Protect Program. Transport Canada is responsible for ensuring that Canadian aviation, marine, railway and road transportation systems are safe, efficient and accessible.

With respect to the Marine Transportation Security Clearance Program, SIRC found that, although this program is not yet fully operational, CSIS has worked collaboratively with Transport Canada to reduce the risk of security threats by conducting background checks on marine workers who have access to certain areas or perform certain duties. In terms of the Passenger Protect Program, SIRC found that CSIS has worked effectively with Transport Canada (along with the RCMP, which also contributes to the program) to ensure that individuals placed on the so-called "no-fly list" do pose a demonstrable threat to aviation security, and that decisions to place individuals on this list are based on clearly defined criteria.

More information about these programs can be found on Transport Canada's website (www.tc.gc.ca).

ARRANGEMENTS WITH FOREIGN AGENCIES

As of March 31, 2008, CSIS had 276 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 five new arrangements in 2007–08 and expanded three existing ones.

In 2007–08, SIRC examined foreign arrangements that had been restricted by the Service because of concerns relating to a country's or agency's human rights record, reliability, or ability to protect information provided by the Service. In general, restricted arrangements prevent CSIS from sharing operational information with an agency, although this does not prevent the Service from receiving unsolicited information concerning Canada's safety and security from a restricted agency.

SIRC found that CSIS adhered to its self-imposed restrictions with the agencies in question. SIRC also found that the Service performed well in terms of balancing the need to collect vital security intelligence information, while remaining aware of the potential problems of dealing with a restricted agency.

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

For 2006–08, the Minister 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 July 2008, however, SIRC received the latest Ministerial Direction for 2008–2009.

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.

In 2007–08, CSIS revised and/or published over 140 policies. Also, more than 70 additional policies were initiated or under development during the same period. Many revisions were administrative in nature. The remainder were operational and pertained to, among others things, targeting levels and approvals process, as well as security screening and warrant powers. In addition, as part of a project launched by the Director in 2006–07, the Service continued its efforts to review all operational policies to determine where executive and management responsibilities must be delegated.

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 2007–08.

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., and the Honourable Roy Romanow, P.C., O.C., Q.C.

The term of the Honourable Baljit S. Chadha, P.C. ended on February 20, 2008. On April 22, 2008, the Honourable Aldéa Landry, P.C., C.M., Q.C. tendered her resignation from SIRC.

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.

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

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 a 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.

Committee activities

May 23–25, 2007: The Honourable Roy Romanow and Senior Counsel were speakers at a symposium marking the 25th anniversary of the *Canadian Charter of Rights and Freedoms* entitled "A Living Tree: The Legacy of 1982 in Canada's Political Evolution," hosted by the Saskatchewan Institute of Public Policy.

June 7–8, 2007: The Chair, the Executive Director and a Member of SIRC attended the International Intelligence Review Agencies symposium on accountability of intelligence and security agencies and human rights. The Chair delivered a speech to participants at this event, which was hosted by the Review Committee on the Intelligence and Security Services and the Faculty of Law at Radboud University (Netherlands).

June 10–12, 2007: The Chair, Members, the Executive Director and selected staff attended the International Conference on the Administration of Justice and National Security in Democracies, hosted in Ottawa by the Federal Court of Canada.

June 14, 2007: The Executive Director and senior staff met with the Australian Inspector General.

June 18, 2007: The Executive Director, accompanied by senior staff, appeared before the Senate Standing Committee to describe SIRC's role and powers as a review body and quasi-judicial complaints tribunal.

Continued on page 56

Committee activities
(continued)

September 20–21, 2007: The Executive Director attended a conference in Ottawa, entitled "Protecting Security and Human Rights: The Case of Migration in Canada," hosted by the Institute for Research on Public Policy.

November 13, 2007 and March 31, 2008: At Carleton University, the Executive Director lectured on SIRC's role and mandate to students of a course on National Security and Intelligence in the Modern State.

November 28, 2007: The Executive Director and senior staff met with officials from the Norwegian Parliamentary Intelligence Oversight Committee.

November 30–December 2, 2007: The Executive Director was a panellist at a conference hosted by the Justice Institute of British Columbia's Committee on Diversity and Policing. The conference was entitled "Balance between Security, Human Rights and Accountability."

January 23, 2008: The Senior Counsel was a guest lecturer on National Security Law at the Faculty of Law, University of Ottawa.

As part of their ongoing work, the Chair of SIRC, Committee Members and senior staff participate in regular discussions with CSIS executive and staff, and other senior members of the security intelligence community.

These exchanges are supplemented by discussions with academics, security and intelligence experts and other relevant organizations. These activities enrich SIRC's knowledge about issues and opinions affecting national security intelligence.

SIRC staff also visits CSIS regional offices on a rotating basis to examine how Ministerial Direction and CSIS policy affect the day-to-day work of investigators in the field. These visits give Committee Members an opportunity to be briefed by regional CSIS staff on local issues, challenges and priorities. It is also an opportunity to communicate SIRC's focus and concerns.

During the 2007–08 fiscal year, SIRC staff 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 hearings, briefings and review activities represent its chief expenditures. Table 8 below presents a breakdown of estimated and actual expenditures.

Table 8
SIRC expenditures 2007–08

	Estimates	Actual
Personnel	$1,900,000	$1,844,000
Goods and Services	$1,000,000	$781,000
Total	**$2,900,000**	**$2,626,000**

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

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.

Table 9
Requests for release of information

	2005–06	2006–07	2007–08
Access to Information Act	17	12	15
Privacy Act	5	2	2

Recommendations

Summary of SIRC recommendations concerning reviews

	SIRC recommended that…
Review 2007-01	• CSIS employees submit a standard, written record of non-operational information exchanged with foreign partners. This would be placed in both the relevant "cooperation with" file and operational database. The written record of non-operational information exchanged should also cross-reference the operational information exchanged with those foreign partners. • When CSIS is cooperating with a foreign agency, the Service should establish a separate Section 17 foreign arrangement with that agency to conform with the *CSIS Act*, Ministerial Direction and operational policy.
Review 2007-02	• CSIS consult with the Treasury Board Secretariat to clarify its responsibility to investigate incidents reported under the Government Security Policy, and to explore the value of enhancing interdepartmental liaison in order to advise departments of their security screening responsibilities under the policy.
Review 2007-04	• CSIS review the criteria used to conduct risk assessments, and that the Service define more precisely the high-risk situations for which it is necessary to consult with the Minister of Public Safety.
Review 2007-05	• CSIS should reconsider its policy structure to accommodate its increasing activities outside Canada. • CSIS standardize its risk assessments with detailed and consistent terminology that is reflected in operational policy.

	SIRC recommended that…
Review 2007-06	• Debates about whether a targeted group is in fact a terrorist organization should be included in future targeting discussions by CSIS.
Review 2006-08* ** Note: This review was not finalized until after the 2006–07 annual report went to print.*	• With respect to the Service's investigation of certain individuals believed to be second-generation terrorists, or recent converts to extremist interpretations of Islam, CSIS should clearly define this issue-based investigation when it is next renewed and determine whether it should focus on issues of increasing concern.

Summary of SIRC recommendations concerning complaints

	SIRC recommended that…
Report 2007-01	• CSIS policies be amended so that individuals are permitted to be accompanied and fully represented by counsel or another representative during a security screening interview conducted by the Service.
Review 2007-03	• CSIS implement the recommendations directed at the Service in the *Arar Report*.
Review 2007-04	• The Canadian Human Rights Commission not investigate this complaint in accordance with Subsection 46 (2) of the *Canadian Human Rights Act*. • The Minister provide the complainant with the opportunity to re-apply for the security clearance under the new policy. • If the complainant were to re-apply, CSIS or Transport Canada should conduct an interview with the complainant in the presence of counsel or other representative. In addition, the complainant should be made aware of the right to record the interview, and that CSIS or Transport Canada also record the interview and retain a copy of the recording until the complainant has had an opportunity to exhaust any review process or until the retention period under the *Privacy Act* has expired, whichever is later.

	SIRC recommended that…
Report 2007-05	• CSIS prepare fresh advice to Citizenship and Immigration Canada that the presence of the complainant in Canada would not be detrimental to the national interest in accordance with Subsection 34(2) of the *Immigration and Refugee Protection Act*, or if required, could be used by the complainant to seek what is referred to as "Ministerial Relief."
Report 2007-06	• CSIS take all necessary steps to ensure the adoption of its *Security Screening Procedures Manual* and *Security Screening Investigator's Guidebook* before June 30, 2008. • CSIS adopt guidelines to ensure that the information recorded and contained in the security screening database accurately reflect the status of the file to enable all users of the system to be as fully aware as possible of the file without having to review the hard-copy file, and that appropriate diary dates be included in its security screening database. • CSIS policy be revised as expeditiously as possible to prevent the destruction of recorded or written notes which may be required as evidence in proceedings before the courts or administrative tribunals. • CSIS provide its advice forthwith with regard to the complainant's security assessment.